Protection des données personnelles
Référentiel légal et réglementaire

Tome 4

Autres textes réglementaires européens
Déclaration des droits numériques
DMA - DSA - DGA - DA - AIA

-

Complément

du Règlement (UE) 2016/679

du Parlement européen et du Conseil

du 27 avril 2016

AFCDP
Association Française des Correspondants à la protection des Données à caractère Personnel

Chers amis, chers adhérents,

Depuis 2004, l'AFCDP soutient les professionnels de la conformité à la loi Informatique et Libertés - et au RGPD désormais. Cela se traduit, entre autres, par la production de livrables conçus par les membres de l'association - comme une FAQ pour gérer les demandes de droit d'accès ou un livre blanc pour « survivre » à un contrôle sur place de la CNIL.

Voici le tome 4.

Après :
- le tome 1 qui propose le texte du RGPD annoté et indexé ;
- le tome 2 qui compile les principales lignes directrices du CEPD ;
- le tome 3 qui regroupe la loi Informatique et Libertés dans sa nouvelle mouture issue de la loi du 20 juin 2018 et de l'ordonnance de réécriture du 12 décembre 2018, et les principaux décrets associés ;
ce quatrième volume regroupe de nouveaux textes européens qui constituent un ensemble de règlementations du marché du numérique, ainsi que le projet de « Déclaration européenne sur les droits et principes numériques pour la décennie numérique », sorte de préambule à ce corpus législatif européen.

Nous ne doutons pas que ce nouveau tome aura autant de succès que les trois précédents.

Les fautes sont nôtres mais merci d'avance de nous aider à les corriger en nous les signalant par simple courriel.

Confraternellement,

Patrick Blum
Délégué Général de l'AFCDP

Commentaires

Dès juin 2016, l'AFCDP a mis à disposition une version annotée, commentée et indexée du RGPD (le tome 1).

En novembre 2018, l'association qui regroupe les DPO et tous les professionnels de la conformité au RGPD a publié un recueil des principales lignes directrices du CEPD (le tome 2).

Le tome 3 publié en 2019 regroupe la loi Informatique et Libertés, dans sa dernière version, et les principaux décrets d'application. Les textes sont complétés en marge par des annotations et commentaires, ainsi que des sous-titres destinés à en améliorer la lecture.

Le présent document réunit d'autres textes règlementaires européens qui peuvent avoir des impacts sur la protection des données personnelles, comme le DMA, le DSA, le DGA, le Data Act et le règlement sur l'intelligence artificielle.

Ce document est un guide pratique destiné aux adhérents de l'AFCDP. Il ne constitue pas une référence légale.

Vous avez remarqué une erreur ou une correction à apporter ? Merci de nous aider à améliorer ce document, par courriel adressé à delegue.general@afcdp.net.

Les autres ressources de l'AFCDP

L'AFCDP met également diverses ressources à la disposition des professionnels :

- un « job board » dédié aux professionnels de la conformité au RGPD ;
- un modèle de fiche de poste de DPD ;
- un modèle de lettre de mission de DPD ;
- une Charte de déontologie du DPD ;
- une place de marché RGPD ;
- une lettre de veille mensuelle et gratuite, « L'Actualité des données personnelles ».

Ces ressources sont accessibles sur le site Web de l'AFCDP : www.afcdp.net

Les membres de l'AFCDP bénéficient de livrables qui leur sont réservés et bénéficient d'un jeu d'illustrations RGPD qu'ils peuvent utiliser librement, par exemple dans le cadre de leurs actions de sensibilisation (ci-dessous, un exemple).

Des textes pour un avenir numérique pour l'Europe

C'est en octobre 2020, lors d'une réunion spécifique du Conseil, que les dirigeants européens ont tracé les grandes lignes de la transformation numérique de l'Europe, et invité la Commission à définir une stratégie numérique complète fixant les ambitions numériques concrètes de l'Union Européenne pour 2030.

Pour adapter la société et les économies européennes à l'ère numérique, l'UE a annoncé s'engager à créer « un espace numérique sûr pour les citoyens et les entreprises, d'une manière inclusive et accessible à tous », en permettant une transformation numérique qui préserve les valeurs de l'UE et protège les droits fondamentaux et la sécurité des citoyens, tout en renforçant la souveraineté numérique de l'Europe

La Commission européenne a proposé une stratégie sous la forme d'une « boussole numérique » qui fixe des objectifs et des jalons numériques spécifiques à atteindre d'ici 2030, en plaçant les compétences numériques et l'éducation au premier plan et en s'articulant autour de quatre domaines : compétences, entreprises, gouvernement et infrastructure. En mars 2021, les dirigeants de l'UE ont souligné la nécessité de renforcer la souveraineté numérique de l'Europe et ont identifié la boussole numérique comme un pas en avant.

Comme première étape de sa boussole numérique, la Commission a proposé le « **Parcours vers la décennie numérique** », programme politique qui définit le cadre de gouvernance pour atteindre les objectifs numériques 2030.

La Commission a également conduit le processus d'adoption en 2023 de la **Déclaration européenne sur les droits et principes numériques**, qui défini les droits des citoyens dans l'espace numérique et le développement d'un cadre de principes que l'UE et les États membres conviennent de respecter dans la transformation numérique.

Dans le cadre de sa boussole numérique, la Commission a ensuite proposé un « paquet » sur les services numériques, réponse au besoin de réguler l'espace numérique. Il comporte deux textes spécifiques : le règlement sur les services numériques (DSA) et le règlement sur les marchés numériques (DMA).

Le règlement sur les services numériques (DSA) part du constat que les plateformes en ligne constituent une partie importante du marché et de l'économie numériques de l'UE, et qu'il convient de renforcer, de moderniser et de clarifier les règles relatives aux services numériques pour assurer la sécurité des utilisateurs en ligne, et permettre aux entreprises numériques innovantes de se développer.

Le règlement sur les marchés numériques (DMA) vise à créer des conditions équitables pour les entreprises de l'UE en règlementant les grandes technologies.

L'économie des données est au cœur du deuxième volet de la stratégie numérique européenne. Pour accompagner le développement de la technologie, qui produit de plus en plus de données, l'Union européenne souhaite créer un marché unique pour les données conforme à ses valeurs, permettant plus de partage et de réutilisation des données entre les secteurs et les frontières.

Cette stratégie européenne pour les données proposée par la Commission devrait faciliter la transformation numérique au cours de la décennie 2022-2030 en construisant une économie européenne des données compétitive, tout en garantissant les valeurs européennes et un niveau élevé de sécurité, de protection des données et de respect de la vie privée.

Le premier élément de cette stratégie est le **Règlement sur la gouvernance des données (DGA)**, qui vise à promouvoir la disponibilité des données pour une réutilisation à travers les secteurs et les frontières, avec

des mécanismes solides pour accroitre la confiance dans les services d'intermédiation de données et favoriser l'altruisme des données dans toute l'UE, tout en jouant un rôle central pour permettre et guider la création d'espaces de données interopérables communs à l'échelle de l'UE dans des secteurs stratégiques tels que l'énergie, la mobilité et santé.

La Commission a également proposé un règlement concernant des règles harmonisées en matière d'accès et d'utilisation équitables des données. Ce **Règlement sur les données (DA)** vise à assurer l'équité dans la répartition de la valeur des données entre les acteurs de l'économie des données et de favoriser l'accès aux données et leur utilisation.

Enfin, la Commission a observé que l'intelligence artificielle peut contribuer à une économie plus innovante, efficace, durable et compétitive, tout en améliorant la sécurité, l'éducation et les soins de santé pour les citoyens, et en contribuant à la lutte contre le changement climatique. Mais le développement de la technologie IA, présente aussi des risques et demande une approche éthique et centrée sur l'humain.

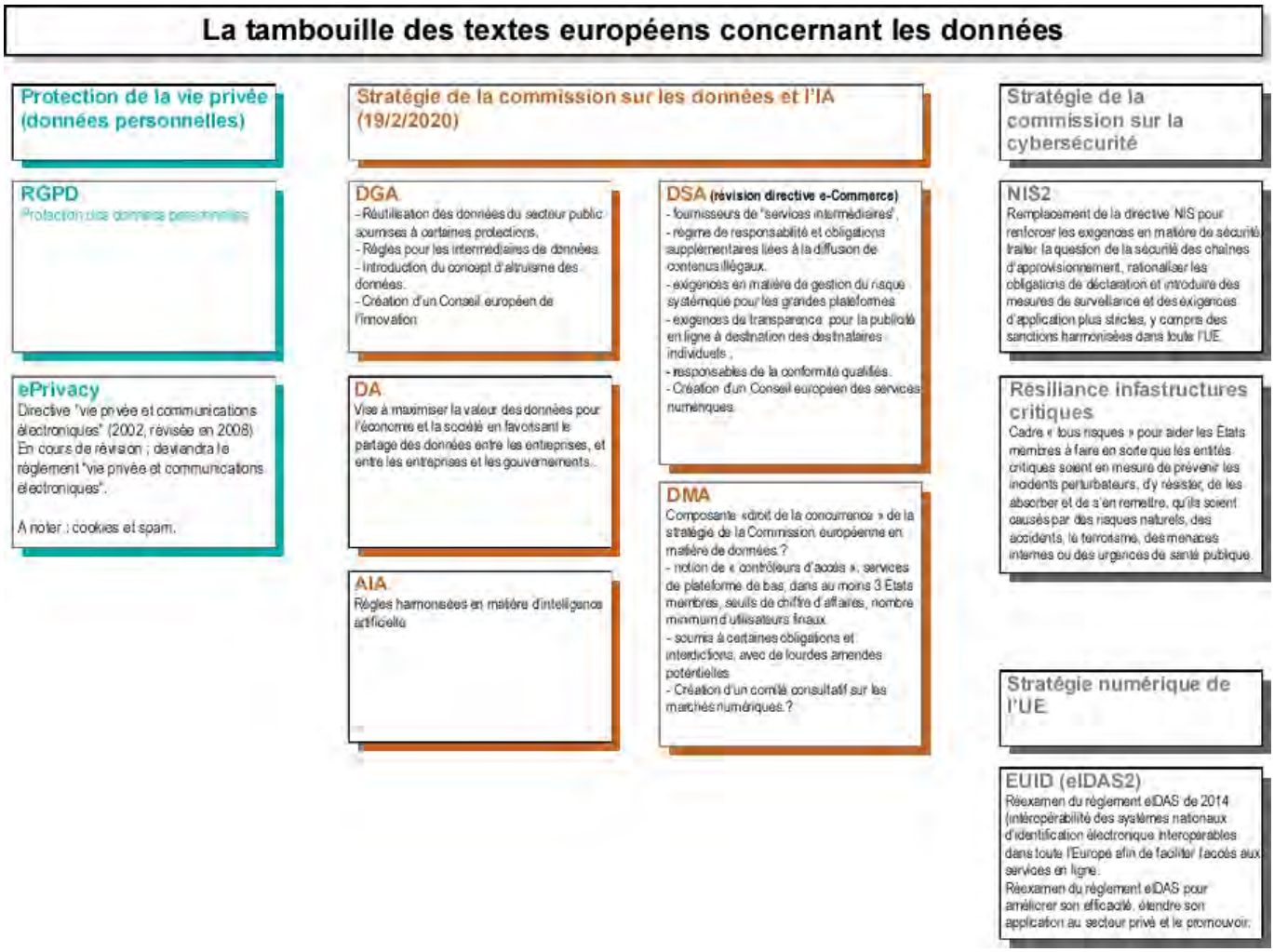
Elle a ainsi proposé un règlement visant à harmoniser les règles sur l'intelligence artificielle avec le **Règlement sur l'intelligence artificielle (AIA)** et un plan coordonné qui comprend un ensemble d'actions conjointes pour la Commission et les États membres dans le but d'améliorer la confiance dans l'intelligence artificielle et de favoriser le développement et la mise à jour de la technologie de l'IA.

En marge des textes concernant directement les données présentés dans ce volume, d'autres textes présentent un intérêt pour les professionnels de la protection des données, et pourront être consultés par ailleurs. Ainsi, la Commisison a proposé une révision de la directive NIS. La proposition de **directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS2)** fait partie d'un ensemble de mesures visant à améliorer encore les capacités de résilience et de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'UE dans son ensemble. Elle couvre le domaine de la cybersécurité et de la protection des infrastructures critiques. La proposition est conforme aux priorités de la Commission visant à rendre l'Europe adaptée à l'ère numérique et à construire une économie prête pour un avenir qui fonctionne pour les citoyens.

Cette directive s'appuie sur la directive NIS qu'elle abroge. Elle modernise le cadre juridique antérieur en tenant compte de la numérisation accrue du marché intérieur ces dernières années et de l'évolution du paysage des menaces en matière de cybersécurité.

D'autre part, le corpus réglementaire unique, qui englobe l'ensemble de la législation de l'Union européenne relative aux établissements financiers, ne faisant que survoler les risques opérationnels liés aux technologies de l'information et de la communication, en septembre 2020, la Commission a présenté une proposition de **règlement sur la résilience opérationnelle numérique du secteur financier (DORA)**, afin d'introduire et d'harmoniser les principales exigences opérationnelles numériques dans l'ensemble de l'Union, de manière à rendre les opérations informatiques résilientes face à des perturbations opérationnelles et à des cyberattaques de grande ampleur.

D'autres textes complètent ce corpus, en particulier en ce qui concerne les règles sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur, le règlement eIDAS de 2014, qui vise à rendre les systèmes nationaux d'identité électronique interopérables dans toute l'Europe afin de faciliter l'accès aux services en ligne. Dans la stratégie numérique de l'UE "Façonner l'avenir numérique de l'Europe", la Commission a procédé au réexamen du règlement eIDAS afin d'améliorer son efficacité, d'étendre son application au secteur privé et de le promouvoir. L'initiative a conduit à l'adoption d'un nouveau **règlement concernant l'établissement du cadre européen relatif à une identité numérique (eIDAS2)**, révision de la version de 2014.


La tambouille des textes européens concernant les données
Protection de la vie privée (données personnelles)
RGPD
Protection des données personnelles
ePrivacy
Directive "vie privée et communications électroniques" (2002, révisée en 2008)
En cours de révision ; deviendra le règlement "vie privée et communications électroniques".
A noter : cookies et spam.
Stratégie de la commission sur les données et l'IA (19/2/2020)
DGA
- Réutilisation des données du secteur public soumises à certaines protections.
- Règles pour les intermédiaires de données
- Introduction du concept d'altruisme des données.
- Création d'un Conseil européen de l'innovation
DA
Vise à maximiser la valeur des données pour l'économie et la société en favorisant le partage des données entre les entreprises, et entre les entreprises et les gouvernements.
AIA
Règles harmonisées en matière d'intelligence artificielle
DSA (révision directive e-Commerce)
- fournisseurs de "services intermédiaires",
- régime de responsabilité et obligations supplémentaires liées à la diffusion de contenus illégaux.
- exigences en matière de gestion du risque systémique pour les grandes plateformes
- exigences de transparence pour la publicité en ligne à destination des destinataires individuels ;
- responsables de la conformité qualifiés.
- Création d'un Conseil européen des services numériques
DMA
Composante «droit de la concurrence » de la stratégie de la Commission européenne en matière de données.?
- notion de « contrôleurs d'accès », services de plateforme de base, dans au moins 3 États membres, seuils de chiffre d'affaires, nombre minimum d'utilisateurs finaux.
- soumis à certaines obligations et interdictions, avec de lourdes amendes potentielles
- Création d'un comité consultatif sur les marchés numériques.?
Stratégie de la commission sur la cybersécurité
NIS2
Remplacement de la directive NIS pour renforcer les exigences en matière de sécurité, traiter la question de la sécurité des chaînes d'approvisionnement, rationaliser les obligations de déclaration et introduire des mesures de surveillance et des exigences d'application plus strictes, y compris des sanctions harmonisées dans toute l'UE.
Résilience infrastructures critiques
Cadre « tous risques » pour aider les États membres à faire en sorte que les entités critiques soient en mesure de prévenir les incidents perturbateurs, d'y résister, de les absorber et de s'en remettre, qu'ils soient causés par des risques naturels, des accidents, le terrorisme, des menaces internes ou des urgences de santé publique.
Stratégie numérique de l'UE
EUID (eIDAS2)
Réexamen du règlement eIDAS de 2014 (interopérabilité des systèmes nationaux d'identification électronique interopérables dans toute l'Europe afin de faciliter l'accès aux services en ligne.
Réexamen du règlement eIDAS pour améliorer son efficacité, étendre son application au secteur privé et le promouvoir.

Les textes de ce volume

TABLE DES MATIÈRES

DSA

RÈGLEMENT (UE) 2022/2065 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 19 octobre 2022

relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) 117

AIA

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) 363

Déclaration européenne sur les droits et principes numériques pour la décennie numérique

Déclaration européenne sur les droits et principes numériques pour la décennie numérique

(2023/C 23/01)

Le Parlement européen, le Conseil et la Commission proclament solennellement la déclaration commune suivante sur les droits et principes numériques pour la décennie numérique.

Préambule

considérant ce qui suit:

(1) L'Union européenne (UE) est une «union de valeurs», comme l'établit l'article 2 du traité sur l'Union européenne, fondée sur le respect de la dignité humaine, la liberté, la démocratie, l'égalité, l'État de droit et le respect des droits de l'homme, y compris les droits des personnes appartenant à des minorités. De plus, aux termes de la charte des droits fondamentaux de l'Union européenne, l'UE se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité. La charte réaffirme en outre les droits qui résultent notamment des obligations internationales communes aux États membres.

(2) La transformation numérique touche tous les aspects de la vie des citoyens. Elle ouvre des possibilités considérables pour améliorer la qualité de la vie et en matière de croissance économique et de durabilité.

(3) La transformation numérique présente également des défis pour nos sociétés démocratiques, nos économies et les individus. Alors que la transformation numérique s'accélère, le moment est venu pour l'UE de préciser comment ses valeurs et ses droits fondamentaux applicables hors ligne devraient s'appliquer dans l'environnement numérique. La transformation numérique ne devrait pas entraîner de régression des droits. Ce qui est illégal hors ligne est illégal en ligne. La présente déclaration s'entend sans préjudice des «politiques hors ligne», comme celles liées à l'accès aux services publics essentiels hors ligne.

(4) Le Parlement a demandé à plusieurs reprises que soient établis des principes éthiques guidant la stratégie de l'UE en matière de transformation numérique, et que soit assuré le plein respect des droits fondamentaux tels que la protection des données, le droit à la vie privée, la non-discrimination et l'égalité de genre, ainsi que de principes comme la protection des consommateurs, la neutralité technologique et de l'internet, la fiabilité et l'inclusivité. Il a également appelé à une protection renforcée des droits des utilisateurs dans l'environnement numérique, ainsi que des droits des travailleurs et du droit à la déconnexion[1].

Protection des données

(5) S'inspirant d'initiatives antérieures telles que la «Déclaration de Tallinn sur l'administration en ligne» et la «Déclaration de Berlin sur la société numérique et l'administration numérique basée sur des valeurs», les États membres ont appelé, dans la «Déclaration de Lisbonne – La démocratie numérique dans un but précis», à adopter un modèle de transformation numérique qui renforce la dimension humaine de l'écosystème numérique et dont le marché unique numérique serait le cœur. Les États membres ont appelé à l'adoption d'un modèle de transformation numérique dans lequel la technologie contribuerait à répondre à la nécessité de lutter contre le changement climatique et de protéger l'environnement.

(6) La vision de l'UE en matière de transformation numérique est centrée sur les citoyens, leur donne les moyens d'agir et favorise les entreprises innovantes. La décision relative au «programme d'action pour la décennie numérique à l'horizon 2030» définit les objectifs numériques concrets, qui reposent sur quatre axes principaux (les compétences numériques, les infrastructures numériques, la transformation numérique des entreprises et la numérisation des services publics). La voie que l'UE doit suivre

1. 2020/2216(INI); 2020/2018(INL); 2020/2019(INL); 2020/2022(INI); 2020/2012(INL); 2020/2014(INL); 2020/2015(INI); 2020/2017(INI); 2019/2186(INI); 2019/2181(INL); 2022/2266(INI).

pour réaliser la transformation numérique de nos sociétés et de notre économie embrasse en particulier la souveraineté numérique de manière ouverte, le respect des droits fondamentaux, l'État de droit et la démocratie, l'inclusion, l'accessibilité, l'égalité, la durabilité, la résilience, la sécurité, l'amélioration de la qualité de vie, la disponibilité des services et le respect des droits et des aspirations de chacun. Elle devrait contribuer à une économie et une société dynamiques, équitables et efficaces dans l'utilisation des ressources.

(7) La présente déclaration énonce des intentions et des engagements politiques partagés et rappelle les droits les plus pertinents dans le contexte de la transformation numérique. La déclaration devrait en outre guider les décideurs politiques lorsqu'ils réfléchissent à leur vision de la transformation numérique: une transformation numérique qui est centrée sur les citoyens; qui soutient la solidarité et l'inclusion, par la connectivité et par l'éducation, la formation et les compétences numériques, des conditions de travail justes et équitables ainsi que l'accès aux services publics numériques en ligne; qui rappelle l'importance de la liberté de choix dans les interactions avec les algorithmes et les systèmes d'intelligence artificielle et dans un environnement numérique équitable; qui encourage la participation à l'espace public numérique; qui accroît la sûreté, la sécurité et l'autonomisation dans l'environnement numérique, en particulier pour les enfants et les jeunes, tout en garantissant le droit à la vie privée et le contrôle des personnes sur leurs données; qui promeut la durabilité. Les différents chapitres de la présente déclaration devraient constituer un cadre de référence global, et non être lus isolément.

(8) La présente déclaration devrait également servir de référence aux entreprises et aux autres acteurs concernés qui élaborent et déploient de nouvelles technologies. Promouvoir la recherche et l'innovation est important à cet égard. Il convient par ailleurs d'accorder une attention particulière aux PME et aux jeunes pousses.

(9) Le fonctionnement démocratique de la société et de l'économie numériques devrait être encore renforcé, dans le plein respect de l'État de droit, des recours effectifs et de l'application des lois. La présente déclaration n'affecte pas les limites licites imposées à l'exercice de droits pour les rendre conciliables avec l'exercice d'autres droits, ni les restrictions nécessaires et proportionnées instaurées dans l'intérêt général.

(10) La présente déclaration repose notamment sur le droit primaire de l'UE, en particulier le traité sur l'Union européenne, le traité sur le fonctionnement de l'Union européenne et la charte des droits fondamentaux de l'Union européenne, ainsi que sur le droit dérivé et la jurisprudence de la Cour de justice de l'Union européenne. Elle s'appuie également sur le socle européen des droits sociaux, et le complète. Elle est de nature déclaratoire et, à ce titre, n'a aucune incidence sur le contenu des règles de droit ou leur application.

(11) L'UE devrait promouvoir la déclaration dans ses relations avec les autres organisations internationales et les pays tiers, y compris en prenant en considération ces droits et principes dans ses relations commerciales, afin que les principes qu'elle défend guident ses partenaires internationaux vers une transformation numérique centrée sur les citoyens et les droits fondamentaux partout dans le monde. La déclaration devrait notamment servir de référence pour les activités menées dans le cadre d'organisations internationales, telles que la réalisation du programme de développement durable à l'horizon 2030, ainsi que l'approche multipartite de la gouvernance de l'internet.

(12) La promotion et l'application de la déclaration constituent un engagement et une responsabilité politiques partagés de l'UE et de ses États membres dans le cadre de leurs compétences respectives et dans le plein respect du droit de l'UE. La Commission fera régulièrement rapport au Parlement et au Conseil sur les progrès accomplis. Les États membres et la Commission devraient tenir compte des principes et droits numériques définis dans la présente déclaration lorsqu'ils coopèrent en vue d'atteindre les objectifs généraux énoncés dans la décision relative au «programme d'action pour la décennie numérique à l'horizon 2030».

Déclaration sur les droits et principes numériques pour la décennie numérique

Notre objectif consiste à promouvoir une voie européenne de la transformation numérique, centrée sur les citoyens, qui repose sur les valeurs européennes et les droits fondamentaux de l'UE, qui réaffirme les droits de l'homme universels et qui profite à tous les citoyens et entreprises, et à la société dans son ensemble.

En conséquence, nous déclarons les droits et principes suivants:

CHAPITRE I
Mettre les citoyens au cœur de la transformation numérique

1. Les citoyens sont au cœur de la transformation numérique dans l'Union européenne. La technologie devrait servir et profiter à toutes les personnes vivant au sein de l'UE et leur donner les moyens de concrétiser leurs aspirations, en toute sécurité et dans le plein respect de leurs droits fondamentaux.

Nous nous engageons à:

a) renforcer le cadre démocratique pour une transformation numérique qui profite à tous et améliore la vie de toutes les personnes vivant au sein de l'UE;

b) prendre les mesures nécessaires pour que les valeurs de l'UE et les droits des personnes reconnus par le droit de l'UE soient respectés tant en ligne qu'hors ligne;

c) encourager une action responsable et diligente de tous les acteurs, publics et privés, dans l'environnement numérique, et à y veiller;

d) promouvoir activement cette vision de la transformation numérique, y compris dans nos relations internationales.

CHAPITRE II
Solidarité et inclusion

2. La technologie devrait servir à unir, et non à diviser. La transformation numérique devrait contribuer à l'équité et à l'inclusivité sociales et économiques dans l'UE.

Nous nous engageons à:

a) veiller à ce que la conception, la mise au point, le déploiement et l'utilisation de solutions technologiques respectent les droits fondamentaux, permettent leur exercice et favorisent la solidarité et l'inclusion;

b) faire en sorte que la transformation numérique ne laisse personne de côté. Elle devrait profiter à tous, assurer un équilibre de genre et inclure notamment les personnes âgées, les personnes vivant dans des zones rurales, les personnes handicapées ou les personnes marginalisées, vulnérables ou défavorisées et les personnes qui agissent en leur nom. Elle devrait également promouvoir la diversité culturelle et linguistique;

c) élaborer des cadres adéquats pour que tous les acteurs du marché bénéficiant de la transformation numérique assument leurs responsabilités sociales et participent de manière équitable et proportionnée aux coûts des biens, services et infrastructures publics, dans l'intérêt de toutes les personnes vivant au sein de l'UE.

Connectivité

3. Toute personne, où qu'elle se trouve dans l'UE, devrait avoir accès à une connexion numérique à haut débit et d'un prix abordable.

Nous nous engageons à:

a) garantir l'accès à une connectivité de haute qualité, et notamment un accès à internet, pour tous, où que ce soit dans l'UE, y compris pour les personnes à faible revenu;

b) protéger et promouvoir un internet neutre et ouvert dans lequel les contenus, les services et les applications ne sont pas bloqués ou dégradés de manière injustifiée.

Éducation, formation et compétences numériques

4. Toute personne a droit à l'éducation, à la formation et à l'apprentissage tout au long de la vie et devrait pouvoir acquérir toutes les compétences numériques de base et avancées.

Nous nous engageons à:

a) promouvoir une éducation et une formation numériques de qualité, notamment en vue de réduire l'écart numérique entre les hommes et les femmes;

b) soutenir les efforts qui permettent à tous les apprenants et les enseignants d'acquérir et de partager les aptitudes et compétences numériques nécessaires, y compris l'éducation aux médias et la pensée critique, pour participer activement à l'économie, à la société et aux processus démocratiques;

c) promouvoir et soutenir les efforts visant à doter tous les établissements d'enseignement et de formation de la connectivité, d'infrastructures et d'outils numériques;

d) donner à chacun, par le renforcement des compétences ou la reconversion, la possibilité de s'adapter aux changements induits par la numérisation du travail.

Conditions de travail justes et équitables

5. Toute personne a droit à des conditions de travail équitables, justes, saines et sûres et à une protection appropriée dans l'environnement numérique, ainsi que sur son lieu de travail physique, quels que soient le statut, les modalités ou la durée de son emploi.

6. Les syndicats et organisations patronales jouent un rôle important dans la transformation numérique, en particulier pour ce qui est de définir des conditions de travail justes et équitables, y compris en ce qui concerne l'utilisation d'outils numériques au travail.

Nous nous engageons à:

a) veiller à ce que chacun puisse se déconnecter et bénéficier de garanties qui lui assurent un équilibre entre vie professionnelle et vie privée dans un environnement numérique;

Equilibre entre vie privée et vie professionnelle.

b) veiller à ce que, dans l'environnement de travail, les outils numériques ne mettent aucunement en danger la santé physique et mentale des travailleurs;

c) veiller au respect des droits fondamentaux des travailleurs dans l'environnement numérique, y compris leur droit à la vie privée, le droit d'association et le droit de négociation et d'action collectives, ainsi qu'à la protection contre la surveillance illégale et injustifiée;

d) veiller à ce que l'utilisation de l'intelligence artificielle sur le lieu de travail soit transparente et suive une approche fondée sur les risques et à ce que des mesures de prévention adéquates soient prises pour préserver un environnement de travail sûr et sain;

e) veiller en particulier à ce que le contrôle humain soit garanti lors de décisions importantes affectant les travailleurs, et à ce que ceux-ci soient généralement informés qu'ils interagissent avec des systèmes d'intelligence artificielle.

Services publics numériques en ligne

7. Chacun devrait avoir accès en ligne aux services publics essentiels dans l'UE. Nul ne doit être invité à fournir des données, si cela n'est pas nécessaire, lors de l'accès aux services publics numériques et de leur utilisation.

Minimisation des données nécessaires.

Nous nous engageons à:

a) veiller à ce que les personnes vivant au sein de l'UE se voient offrir la possibilité d'utiliser une identité numérique accessible, facultative, sûre et fiable, qui donne accès à un large éventail de services en ligne;

b) assurer une large accessibilité et la réutilisation des informations du secteur public;

c) faciliter et encourager un accès continu, sécurisé et interopérable dans toute l'UE aux services publics numériques conçus pour répondre aux besoins des citoyens de manière efficace, y compris et surtout les services numériques de santé et de soins, notamment l'accès aux dossiers médicaux électroniques.

CHAPITRE III
Liberté de choix

Interactions avec les algorithmes et les systèmes d'intelligence artificielle

8. L'intelligence artificielle devrait servir d'outil pour les citoyens, afin d'accroître, en définitive, le bien-être de l'être humain.

9. Toute personne devrait être en mesure de bénéficier des avantages qu'offrent les systèmes algorithmiques et d'intelligence artificielle, y compris en faisant des choix libres et éclairés dans l'environnement numérique, tout en étant protégée contre les risques et les atteintes à sa santé, à sa sécurité et à ses droits fondamentaux.

Nous nous engageons à:

a) promouvoir des systèmes d'intelligence artificielle axés sur l'humain, fiables et éthiques tout au long de leur mise au point, de leur déploiement et de leur utilisation, conformément aux valeurs de l'UE;

b) assurer un niveau de transparence adéquat quant à l'utilisation des algorithmes et de l'intelligence artificielle, et à faire en sorte que les citoyens soient formés à les utiliser et qu'ils soient informés lorsqu'ils interagissent avec ces technologies;

c) veiller à ce que les systèmes algorithmiques reposent sur des ensembles de données appropriés, afin d'éviter toute discrimination et de permettre une surveillance humaine de tous les résultats qui affectent la sécurité et les droits fondamentaux des citoyens;

Contrôle des algorithmes vis-à-vis de la discrimination.

d) veiller à ce que les technologies telles que l'intelligence artificielle ne soient pas utilisées pour préjuger des choix des personnes, par exemple en matière de santé, d'éducation, d'emploi et de vie privée;

e) prévoir des garanties et prendre des mesures appropriées, y compris en promouvant des normes fiables, pour que l'intelligence artificielle et les systèmes numériques soient, en permanence, sûrs et utilisés dans le plein respect des droits fondamentaux;

f) prendre des mesures pour faire en sorte que la recherche en matière d'intelligence artificielle respecte les normes éthiques les plus élevées et la législation pertinente de l'UE.

Un environnement numérique loyal

10. Toute personne devrait pouvoir choisir en connaissance de cause et librement les services en ligne qu'elle utilisera, sur la base d'informations objectives, transparentes, facilement accessibles et fiables.

11. Toute personne devrait avoir la possibilité d'exercer une concurrence loyale et d'innover dans l'environnement numérique. Cela devrait également profiter aux entreprises, y compris aux PME.

Nous nous engageons à:

a) garantir un environnement numérique sûr et sécurisé fondé sur une concurrence loyale, où les droits fondamentaux sont protégés, où les droits des utilisateurs et la protection des consommateurs au sein du marché unique numérique sont assurés et où les responsabilités des plateformes, en particulier des grands acteurs et des contrôleurs d'accès, sont bien définies;

b) promouvoir l'interopérabilité, la transparence et les technologies et normes ouvertes comme moyen de renforcer encore la confiance dans les technologies ainsi que la capacité des consommateurs à faire des choix de manière autonome et en connaissance de cause.

CHAPITRE IV
Participation à l'espace public numérique

12. Toute personne devrait avoir accès à un environnement numérique fiable, diversifié et multilingue. L'accès à des contenus diversifiés contribue à un débat public pluraliste et à une participation effective à la démocratie de manière non discriminatoire.

13. Toute personne a droit à la liberté d'expression et d'information, ainsi qu'à la liberté de réunion et d'association dans l'environnement numérique.

14. Toute personne devrait pouvoir accéder à des informations permettant de savoir qui détient la propriété ou le contrôle des services de médias qu'elle utilise.

15. Les plateformes en ligne, en particulier les très grandes plateformes en ligne, devraient encourager un débat démocratique libre en ligne. Eu égard au rôle que jouent leurs services dans la formation de l'opinion et du discours publics, les très grandes plateformes en ligne devraient atténuer les risques découlant du fonctionnement et de l'utilisation de leurs services, y compris en ce qui concerne les campagnes de mésinformation et de désinformation, et protéger la liberté d'expression.

Nous nous engageons à:

a) continuer à protéger tous les droits fondamentaux en ligne, notamment la liberté d'expression et d'information, y compris la liberté et le pluralisme des médias;

b) favoriser le développement et l'utilisation optimale des technologies numériques pour stimuler l'engagement des citoyens et la participation démocratique;

c) prendre des mesures proportionnées pour lutter contre toute forme de contenu illicite, dans le plein respect des droits fondamentaux, y compris le droit à la liberté d'expression et d'information, et sans imposer d'obligations générales de surveillance ou de censure;

d) créer un environnement numérique dans lequel les personnes sont protégées contre la désinformation et la manipulation de l'information et contre d'autres formes de contenu préjudiciable, notamment le harcèlement et la violence à caractère sexiste;

e) soutenir un accès effectif aux contenus numériques reflétant la diversité culturelle et linguistique dans l'UE;

f) donner aux personnes les moyens de faire des choix libres et spécifiques, et à limiter l'exploitation des vulnérabilités et des biais, notamment par la publicité ciblée.

CHAPITRE V
Sûreté, sécurité et autonomisation

Un environnement numérique protégé, sûr et sécurisé

16. Tout le monde devrait avoir accès à des technologies, produits et services numériques qui sont, dès la conception, sûrs, sécurisés et respectueux de la vie privée, donnant ainsi lieu à un niveau élevé de confidentialité, d'intégrité, de disponibilité et d'authenticité des informations traitées.

Technologies respectueuses de la vie privée.

Nous nous engageons à:

a) prendre des mesures supplémentaires pour promouvoir la traçabilité des produits et veiller à ce que seuls des produits sûrs et conformes à la législation de l'UE soient proposés sur le marché unique numérique;

b) protéger les intérêts des citoyens, des entreprises et des institutions publiques contre les risques liés à la cybersécurité et la cybercriminalité, y compris les violations de données et l'usurpation ou la manipulation d'identité. Cela inclut des exigences en matière de cybersécurité pour les produits connectés mis sur le marché unique;

Protection contre les violations de données.

c) mettre en échec et traduire en justice les personnes qui cherchent à compromettre, au sein de l'UE, la sécurité en ligne et l'intégrité de l'environnement numérique ou qui encouragent la violence et la haine par des moyens numériques.

Droit à la vie privée et contrôle des personnes sur leurs données

17. Toute personne a droit au respect de sa vie privée et à la protection de ses données à caractère personnel. Ce dernier droit permet notamment à chacun de contrôler la manière dont ses données à caractère personnel sont utilisées et avec qui elles sont partagées.

Protection des données à caractère personnel.

18. Toute personne a droit à la confidentialité de ses communications et des informations figurant sur ses appareils électroniques, et a le droit de ne pas être soumise à une surveillance en ligne illicite, à un suivi omniprésent illicite ou à des mesures d'interception.

19. Toute personne devrait être en mesure de définir son patrimoine numérique et de décider du sort qui sera réservé, après son décès, à ses comptes personnels et aux informations qui la concernent.

Nous nous engageons à:

a) veiller à ce que chacun ait le contrôle effectif de ses données à caractère personnel et non personnel, conformément aux règles de l'UE en matière de protection des données et à la législation pertinente de l'UE;

b) garantir effectivement la possibilité pour une personne de transférer facilement ses données à caractère personnel et non personnel entre différents services numériques, dans le respect des droits en matière de portabilité;

Transfert de données entre services numériques.

c) protéger efficacement les communications contre tout accès non autorisé de tiers;

d) interdire l'identification illicite ainsi que la conservation illicite de relevés d'activité.

Protection et autonomisation des enfants et des jeunes dans l'environnement numérique

20. Les enfants et les jeunes devraient être formés à l'environnement numérique afin d'y faire des choix sûrs, en connaissance de cause, et d'y exprimer leur créativité.

21. Des contenus et services adaptés à chaque âge devraient améliorer l'expérience, le bien-être et la participation des enfants et des jeunes dans l'environnement numérique.

22. Il convient d'accorder une attention particulière au droit des enfants et des jeunes d'être protégés contre toute forme de criminalité, commise ou facilitée par les technologies numériques.

Nous nous engageons à:

a) offrir à tous les enfants et les jeunes la possibilité d'acquérir les aptitudes et les compétences nécessaires, y compris l'éducation aux médias et la pensée critique, afin de naviguer et de s'investir activement et en toute sécurité dans l'environnement numérique et d'y faire des choix en connaissance de cause;

b) promouvoir des expériences positives pour les enfants et les jeunes dans un environnement numérique adapté à l'âge et sûr;

c) protéger tous les enfants et les jeunes contre les contenus nuisibles et illicites, l'exploitation, la manipulation et les abus en ligne, et à empêcher l'utilisation de l'espace numérique pour commettre ou faciliter des actes criminels;

d) protéger tous les enfants et les jeunes contre le traçage, le profilage et le ciblage illégaux, en particulier à des fins commerciales;

e) associer les enfants et les jeunes à l'élaboration des politiques numériques qui les concernent.

CHAPITRE VI
Durabilité

23. En vue de prévenir tout préjudice important à l'environnement, et afin de promouvoir l'économie circulaire, les produits et services numériques devraient être conçus, produits, utilisés, réparés, recyclés et éliminés de manière à atténuer leur impact négatif sur l'environnement et la société et à éviter une obsolescence prématurée.

24. Pour être en mesure de faire des choix responsables, toute personne devrait avoir accès à des informations exactes et faciles à comprendre sur l'incidence environnementale et la consommation d'énergie des produits et services numériques, leur réparabilité et leur durée de vie.

Nous nous engageons à:

a) encourager le développement et l'utilisation de technologies numériques durables qui ont une incidence environnementale et sociale négative minimale;

b) inciter à des choix de consommation et à des modèles d'entreprise durables, et à encourager un comportement d'entreprise durable et responsable tout au long des chaînes de valeur mondiales des produits et services numériques, y compris en vue de lutter contre le travail forcé;

c) promouvoir la mise au point, le déploiement et l'utilisation active de technologies numériques innovantes ayant une incidence positive sur l'environnement et le climat, afin d'accélérer la transition écologique;

d) promouvoir des normes et des labels en matière de durabilité pour les produits et services numériques.

DMA

DMA

RÈGLEMENT (UE) 2022/1925 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 septembre 2022

relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

statuant conformément à la procédure législative ordinaire[3],

considérant ce qui suit:

(1) Les services numériques en général et les plateformes en ligne en particulier jouent un rôle toujours plus important au sein de l'économie, notamment sur le marché intérieur, en permettant aux entreprises d'atteindre les utilisateurs dans l'ensemble de l'Union, en facilitant le commerce transfrontière et en ouvrant des débouchés commerciaux entièrement nouveaux à un grand nombre d'entreprises dans l'Union, au profit des consommateurs dans l'Union.

Services de plateforme essentiels

(2) Parallèlement, parmi ces services numériques, les services de plateforme essentiels présentent un certain nombre de caractéristiques qui peuvent être exploitées par les entreprises qui les fournissent. Parmi les caractéristiques de ces services de plateforme essentiels figurent par exemple des économies d'échelle extrêmes, qui résultent souvent de coûts marginaux presque nuls pour ajouter des entreprises utilisatrices ou des utilisateurs finaux. Les services de plateforme essentiels se caractérisent en outre par des effets de réseau très importants, leur capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce à leur caractère multiface, un degré considérable de dépendance des entreprises utilisatrices et des utilisateurs finaux, des effets de verrouillage, l'absence de multihébergement aux mêmes fins par les utilisateurs finaux, l'intégration verticale et les avantages liés aux données. Toutes ces caractéristiques, combinées à des pratiques déloyales de la part des entreprises fournissant ces services de plateforme essentiels, peuvent sensiblement compromettre la contestabilité des services de plateforme essentiels, ainsi que nuire à l'équité de la relation commerciale entre les entreprises fournissant ces services et leurs entreprises utilisatrices et utilisateurs finaux. En pratique, cela conduit à une diminution rapide et potentiellement considérable du choix des entreprises utilisatrices

1. JO C 286 du 16.7.2021, p. 64.
2. JO C 440 du 29.10.2021, p. 67.
3. Position du Parlement européen du 5 juillet 2022 (non encore parue au Journal officiel) et décision du Conseil du 18 juillet 2022.

et utilisateurs finaux, et peut donc conférer au fournisseur de ces services la position de « contrôleurs d'accès ». Dans le même temps, il convient de reconnaître que les services qui ne poursuivent pas d'objectif commercial, comme les projets collaboratifs, ne devraient pas être considérés comme des services de plateforme essentiels aux fins du présent règlement.

(3) Un petit nombre de grandes entreprises fournissant des services de plateforme essentiels ont vu le jour et disposent d'un pouvoir économique considérable qui pourrait faire d'elles des contrôleurs d'accès au sens du présent règlement. En règle générale, elles sont en mesure de relier de nombreuses entreprises utilisatrices à de nombreux utilisateurs finaux à travers leurs services, ce qui, en retour, leur permet de tirer profit de leurs avantages, tels qu'un accès à de vastes quantités de données, d'un domaine d'activité à un autre. Certaines de ces entreprises exercent un contrôle sur des écosystèmes de plateformes entiers au sein de l'économie numérique et sont structurellement extrêmement difficiles à concurrencer ou à contester par des opérateurs du marché existants ou nouveaux, indépendamment du degré d'innovation et d'efficacité de ces opérateurs du marché. La contestabilité est réduite en particulier du fait de l'existence de barrières très hautes à l'entrée ou à la sortie, y compris des coûts d'investissement élevés qui, en cas de sortie, ne sont pas récupérables, ou le sont difficilement, et l'absence d'intrants clés de l'économie numérique, tels que les données, ou l'accès limité à ces derniers. Le mauvais fonctionnement des marchés sous-jacents, ou leur mauvais fonctionnement futur, est par conséquent plus probable.

(4) Dans de nombreux cas, cette combinaison de caractéristiques des contrôleurs d'accès est susceptible de mener à de graves déséquilibres en matière de pouvoir de négociation, et donc à des pratiques et conditions déloyales à l'égard tant des entreprises utilisatrices que des utilisateurs finaux de services de plateforme essentiels fournis par ces contrôleurs d'accès, au détriment des prix, de la qualité, de la concurrence loyale, du choix et de l'innovation dans le secteur numérique.

(5) Il s'ensuit que les processus du marché sont souvent incapables de garantir des résultats économiques équitables en ce qui concerne les services de plateforme essentiels. Si les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne s'appliquent au comportement des contrôleurs d'accès, le champ d'application de ces dispositions se limite à certains cas de pouvoir de marché, par exemple la position dominante sur certains marchés et le comportement anticoncurrentiel, et l'application intervient ex post et requiert une enquête approfondie, au cas par cas, sur des faits souvent très complexes. En outre, le droit existant de l'Union ne répond pas, ou pas efficacement, aux entraves au bon fonctionnement du marché intérieur dues au comportement de contrôleurs d'accès qui n'occupent pas nécessairement de position dominante au sens du droit de la concurrence.

(6) En offrant des points d'accès à un grand nombre d'entreprises utilisatrices pour atteindre leurs utilisateurs finaux, partout dans l'Union et sur différents marchés, les contrôleurs d'accès ont un poids important sur le marché intérieur. L'incidence néfaste des pratiques déloyales sur le marché intérieur, et en particulier la faible contestabilité des services de plateforme essentiels, y compris les conséquences sociétales et économiques négatives de ces pratiques déloyales, a conduit les législateurs nationaux et les organismes de réglementation sectoriels à agir. Un certain nombre de solutions réglementaires ont déjà été adoptées au niveau national ou proposées en réponse aux questions liées aux pratiques déloyales et à la contestabilité des services numériques, ou à certaines d'entre elles au moins. Il en a résulté des divergences entre les solutions réglementaires, qui entraînent une fragmentation du marché intérieur, augmentant en conséquence le risque de voir croître les coûts de mise en conformité, en raison des différents dispositifs réglementaires nationaux.

(7) Par conséquent, l'objectif du présent règlement est de contribuer au bon fonctionnement du marché intérieur en établissant des règles visant à garantir la contestabilité et l'équité des marchés dans le secteur numérique en général et pour les entreprises utilisatrices et les utilisateurs finaux des services de plateforme essentiels fournis par les contrôleurs d'accès en particulier. Les entreprises utilisatrices et les utilisateurs finaux de services de plateforme essentiels fournis par des contrôleurs d'accès devraient bénéficier de garanties réglementaires contre les pratiques déloyales des contrôleurs d'accès dans l'ensemble de l'Union, afin de faciliter les échanges transfrontières au sein de l'Union et, partant, le bon fonctionnement du marché intérieur, et d'éliminer la fragmentation existante ou éviter qu'elle apparaisse dans les domaines

spécifiques régis par le présent règlement. De plus, si les contrôleurs d'accès adoptent généralement des modèles commerciaux et des structures algorithmiques mondiaux, ou du moins paneuropéens, ils peuvent adopter, et, dans certains cas, ont adopté, des conditions et pratiques commerciales différentes dans les divers États membres, qui sont susceptibles de créer des disparités entre les conditions de concurrence pour les utilisateurs de services de plateforme essentiels fournis par les contrôleurs d'accès, aux dépens de l'intégration du marché intérieur.

(8) En rapprochant les législations nationales divergentes, il est possible d'éliminer les obstacles à la liberté de fournir et recevoir des services, y compris les services de vente au détail, au sein du marché intérieur. Un ensemble ciblé d'obligations légales harmonisées devrait par conséquent être établi à l'échelon de l'Union afin de garantir la contestabilité et l'équité des marchés numériques sur lesquels les contrôleurs d'accès opèrent au sein du marché intérieur, dans l'intérêt de l'économie de l'Union dans son ensemble et, en définitive, des consommateurs de l'Union.

(9) Il n'est possible d'éviter effectivement une fragmentation du marché intérieur qu'en interdisant aux États membres d'appliquer des règles nationales qui relèvent du même champ d'application et poursuivent les mêmes objectifs que le présent règlement. Cela ne fait pas obstacle à la possibilité d'appliquer aux contrôleurs d'accès, au sens du présent règlement, d'autres règles nationales qui poursuivent d'autres objectifs d'intérêt public légitimes énoncés dans le traité sur le fonctionnement de l'Union européenne ou qui se justifient pour des raisons impérieuses d'intérêt général reconnues par la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de justice »).

(10) Dans le même temps, puisque le présent règlement vise à compléter l'application du droit de la concurrence, il devrait s'appliquer, sans préjudice des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne, aux règles de concurrence nationales correspondantes et aux autres règles de concurrence nationales relatives au comportement unilatéral, qui reposent sur une évaluation individualisée des positions et du comportement sur le marché, y compris les effets réels ou éventuels ainsi que la portée précise du comportement interdit, et qui prévoient la possibilité pour les entreprises de justifier objectivement le comportement en question par des motifs d'efficience, ainsi qu'aux règles nationales concernant le contrôle des concentrations. Toutefois, l'application de ces règles ne devrait pas porter atteinte aux obligations imposées aux contrôleurs d'accès au titre du présent règlement ni à leur application uniforme et effective sur le marché intérieur.

(11) Les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne et les règles de concurrence nationales correspondantes relatives aux comportements anticoncurrentiels multilatéraux et unilatéraux ainsi que le contrôle des concentrations ont pour objectif la protection d'une concurrence non faussée sur le marché. Le présent règlement poursuit un objectif complémentaire, mais différent de la protection d'une concurrence non faussée sur tout marché, au sens du droit de la concurrence, qui est de veiller à ce que les marchés sur lesquels les contrôleurs d'accès opèrent sont et restent contestables et équitables, indépendamment des effets réels, éventuels ou présumés sur la concurrence sur un marché donné du comportement d'un contrôleur d'accès couvert par ce règlement. Le présent règlement vise par conséquent à protéger un intérêt juridique différent de celui qui est protégé par lesdites règles et il devrait s'appliquer sans préjudice de leur application.

(12) Le présent règlement devrait également s'appliquer sans préjudice des règles qui découlent d'autres actes du droit de l'Union régissant certains aspects de la fourniture de services couverts par le présent règlement, en particulier les règlements (UE) 2016/679[4] et (UE) 2019/1150[5] du Parlement européen et du Conseil et le règlement relatif à un marché intérieur des services numériques, les directives 2002/58/CE[6], 2005/29/CE[7], 2010/13/UE[8], (UE) 2015/2366[9], (UE) 2019/790[10]et (UE) 2019/882[11] du Parle-

cf. RGPD

4. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).
5. Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).

ment européen et du Conseil et la directive 93/13/CEE du Conseil[12], ainsi que les règles nationales visant à mettre en œuvre ou à transposer ces actes juridiques de l'Union.

(13) La faible contestabilité et les pratiques déloyales dans le secteur numérique sont plus fréquentes et prononcées pour certains services numériques que pour d'autres. C'est le cas en particulier pour les services numériques répandus et couramment utilisés, qui servent, pour la plupart, d'intermédiaires directs entre les entreprises utilisatrices et les utilisateurs finaux, et qui se caractérisent principalement par des économies d'échelle extrêmes, des effets de réseau très importants, la capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce au caractère multiface de ces services, des effets de verrouillage, l'absence de multihébergement ou l'intégration verticale. Il n'existe souvent qu'une seule grande entreprise ou très peu de grandes entreprises fournissant ces services numériques. Le plus souvent, ces entreprises sont devenues des contrôleurs d'accès pour les entreprises utilisatrices et les utilisateurs finaux, avec de profondes répercussions. En particulier, elles ont acquis la capacité de fixer facilement des conditions générales commerciales de manière unilatérale et préjudiciable pour leurs entreprises utilisatrices et utilisateurs finaux. Par conséquent, il est nécessaire de se concentrer uniquement sur les services numériques les plus largement utilisés par les entreprises utilisatrices et les utilisateurs finaux et pour lesquels les préoccupations relatives à la faible contestabilité et aux pratiques déloyales des contrôleurs d'accès sont plus apparentes et urgentes du point de vue du marché intérieur.

(14) En particulier, les services d'intermédiation en ligne, les moteurs de recherche en ligne, les systèmes d'exploitation, les réseaux sociaux en ligne, les services de plateformes de partage de vidéos, les services de communications interpersonnelles non fondés sur la numérotation, les services d'informatique en nuage, les assistants virtuels, les navigateurs internet et les services de publicité en ligne, y compris les services d'intermédiation publicitaire, sont tous capables de toucher un grand nombre d'utilisateurs finaux comme d'entreprises, ce qui comporte un risque de pratiques commerciales déloyales. Ils devraient donc être inclus dans la définition des services de plateforme essentiels et relever du champ d'application du présent règlement. Les services d'intermédiation en ligne peuvent également opérer dans le domaine des services financiers, et ils peuvent agir en tant qu'intermédiaires ou être utilisés pour fournir des services tels que ceux énumérés de manière non exhaustive à l'annexe II de la directive (UE) 2015/1535 du Parlement européen et du Conseil[13]. Aux fins du présent règlement, la définition des services de plateforme essentiels devrait être neutre sur le plan technologique et devrait s'entendre comme englobant ceux qui sont proposés par différents moyens ou sur différents dispositifs, tels que la télévision connectée ou les services numériques embarqués dans les véhicules. Dans certaines circonstances, la

6. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).
7. Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales ») (JO L 149 du 11.6.2005, p. 22).
8. Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels ») (JO L 95 du 15.4.2010, p. 1).
9. Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).
10. Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).
11. Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).
12. Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).
13. Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

notion d'utilisateurs finaux devrait inclure les utilisateurs qui sont habituellement considérés comme des entreprises utilisatrices, mais qui, dans une situation donnée, n'utilisent pas les services de plateforme essentiels dans le but de fournir des biens ou des services à d'autres utilisateurs finaux, telles que, à titre d'exemple, les entreprises qui dépendent des services d'informatique en nuage pour leurs propres besoins

(15) Qu'un service numérique puisse être qualifié de service de plateforme essentiel ne suscite pas en soi de préoccupations suffisamment sérieuses en matière de contestabilité ou de pratiques déloyales. De telles préoccupations apparaissent seulement lorsqu'un service de plateforme essentiel constitue un point d'accès majeur et est exploité par une entreprise ayant un poids important sur le marché intérieur et jouissant d'une position solide et durable, ou par une entreprise susceptible de jouir d'une telle position dans un avenir proche. En conséquence, l'ensemble ciblé de règles harmonisées prévues dans le présent règlement ne devrait s'appliquer qu'aux entreprises désignées sur la base de ces trois critères objectifs, et ne devrait s'appliquer qu'aux services de plateforme essentiels qui représentent, individuellement, un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux. Le fait qu'une entreprise fournissant des services de plateforme essentiels puisse jouer un rôle d'intermédiaire non seulement entre les entreprises utilisatrices et les utilisateurs finaux, mais aussi entre utilisateurs finaux, par exemple dans le cas de services de communications interpersonnelles non fondés sur la numérotation, ne devrait pas empêcher de conclure qu'une telle entreprise constitue ou pourrait constituer un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre des utilisateurs finaux.

(16) Dans le but de garantir l'application effective du présent règlement aux entreprises fournissant des services de plateforme essentiels qui sont les plus susceptibles de remplir ces critères objectifs, et pour lesquels les pratiques déloyales affaiblissant la contestabilité sont les plus fréquentes et ont le plus de répercussions, la Commission devrait être en mesure de désigner directement comme contrôleurs d'accès les entreprises fournissant des services de plateforme essentiels qui répondent à certains seuils quantitatifs. Ces entreprises devraient en tout état de cause faire l'objet d'un processus de désignation rapide qui devrait commencer dès que le présent règlement devient applicable.

(17) Le fait qu'une entreprise ait un chiffre d'affaires très élevé dans l'Union et fournisse un service de plateforme essentiel dans au moins trois États membres constitue un indice probant indiquant que cette entreprise a un impact significatif sur le marché intérieur. Il en va de même lorsqu'une entreprise fournissant un service de plateforme essentiel dans au moins trois États membres a une capitalisation boursière très importante ou une juste valeur marchande équivalente. Par conséquent, il convient que l'entreprise fournissant un service de plateforme essentiel soit présumée avoir un poids important sur le marché intérieur lorsqu'elle fournit ce service dans au moins trois États membres et lorsque soit le chiffre d'affaires de son groupe réalisé dans l'Union est égal ou supérieur à un seuil élevé spécifique, soit la capitalisation boursière de son groupe est égale ou supérieure à une valeur absolue élevée déterminée. En ce qui concerne les entreprises fournissant des services de plateforme essentiels appartenant à des entreprises qui ne sont pas cotées en Bourse, il convient de se référer à la juste valeur marchande équivalente. Il devrait être possible pour la Commission d'utiliser son pouvoir d'adopter des actes délégués afin de mettre au point une méthode objective pour calculer cette valeur.

Un chiffre d'affaires élevé du groupe, réalisé dans l'Union, associé au nombre seuil d'utilisateurs de services de plateforme essentiels dans l'Union témoigne d'une capacité relativement forte de monétiser ces utilisateurs. Une capitalisation boursière élevée par rapport au même nombre seuil d'utilisateurs dans l'Union traduit un potentiel relativement important de monétisation de ces utilisateurs dans un avenir proche. Ce potentiel de monétisation marque à son tour, en principe, la position de point d'accès des entreprises concernées. Ces deux indicateurs reflètent en outre la capacité financière des entreprises concernées, y compris leur faculté de tirer profit de leur accès aux marchés financiers dans le but de renforcer leur position. Cela peut notamment être le cas lorsque cet accès supérieur est utilisé pour acquérir d'autres entreprises, cette capacité s'étant à son tour avérée avoir des répercussions néfastes potentielles sur l'innovation. La capitalisation boursière peut également refléter la position future attendue et les effets sur le marché intérieur des entreprises concernées, en dépit d'un chiffre d'affaires actuel potentiellement relativement faible. La valeur de la capitalisation

boursière devrait reposer sur un niveau qui représente la capitalisation boursière moyenne des plus grandes entreprises cotées en Bourse de l'Union sur une période appropriée.

(18) Alors qu'une capitalisation boursière égale ou supérieure au seuil au cours de l'exercice précédent devrait donner lieu à une présomption selon laquelle une entreprise fournissant des services de plateforme essentiels a un poids important sur le marché intérieur, une capitalisation boursière durable de l'entreprise fournissant des services de plateforme essentiels égale ou supérieure au seuil pendant trois ans ou plus devrait renforcer encore cette présomption.

(19) En revanche, un certain nombre de facteurs relatifs à la capitalisation boursière pourraient nécessiter une évaluation approfondie pour déterminer s'il faut considérer qu'une entreprise fournissant des services de plateforme essentiels a un impact significatif sur le marché intérieur. Cela pourrait être le cas lorsque la capitalisation boursière de l'entreprise fournissant des services de plateforme essentiels au cours des exercices précédents était considérablement inférieure au seuil et que la volatilité de sa capitalisation boursière sur la période étudiée était disproportionnée par rapport à la volatilité globale du marché des actions, ou que sa trajectoire de capitalisation boursière par rapport aux tendances du marché était incompatible avec une croissance rapide et unidirectionnelle.

(20) Disposer d'un nombre très important d'entreprises utilisatrices qui dépendent d'un service de plateforme essentiel pour atteindre un très grand nombre d'utilisateurs finaux actifs chaque mois permet à l'entreprise fournissant ce service d'exercer à son avantage une influence sur les activités d'une large part des entreprises utilisatrices et révèle, en principe, que cette entreprise est un point d'accès majeur. Il convient de fixer les niveaux respectifs pertinents de ces chiffres de manière à représenter un pourcentage substantiel de la population totale de l'Union en ce qui concerne les utilisateurs finaux et de la population totale des entreprises utilisant des services de plateforme essentiels pour déterminer le seuil relatif aux entreprises utilisatrices. Les utilisateurs finaux actifs et les entreprises utilisatrices actives devraient faire l'objet d'une identification et d'un calcul qui permettent de représenter correctement le rôle et la portée du service de plateforme essentiel spécifique en question. Afin d'apporter une sécurité juridique aux contrôleurs d'accès, les éléments permettant de déterminer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives par service de plateforme essentiel devraient être énoncés dans une annexe du présent règlement. Les évolutions technologiques et autres peuvent avoir une influence sur ces éléments. Il convient dès lors d'habiliter la Commission à adopter des actes délégués pour modifier le présent règlement en actualisant la méthodologie et la liste d'indicateurs utilisés afin de déterminer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives.

(21) Une entreprise bénéficie ou bénéficiera probablement dans le futur d'une position solide et durable dans ses activités notamment lorsque la contestabilité de la position de l'entreprise fournissant le service de plateforme essentiel est limitée. Tel est probablement le cas si cette entreprise a fourni un service de plateforme essentiel dans au moins trois États membres à un très grand nombre d'entreprises utilisatrices et d'utilisateurs finaux pendant une période d'au moins trois ans.

(22) Les évolutions du marché et de la technologie peuvent influer sur de tels seuils. La Commission devrait donc être habilitée à adopter des actes délégués visant à préciser la méthode utilisée pour déterminer si les seuils quantitatifs sont atteints, et à l'adapter régulièrement aux évolutions du marché et de la technologie, le cas échéant. Ces actes délégués ne devraient pas modifier les seuils quantitatifs fixés dans le présent règlement.

(23) Une entreprise fournissant des services de plateforme essentiels devrait pouvoir, dans des circonstances exceptionnelles, renverser la présomption selon laquelle elle a un poids important sur le marché intérieur en démontrant que, même si elle atteint les seuils quantitatifs fixés dans le présent règlement, elle ne remplit pas les exigences nécessaires pour être désignée comme contrôleur d'accès. La charge de la preuve que la présomption découlant du respect de seuils quantitatifs ne devrait pas s'appliquer incombe à cette entreprise. La Commission ne devrait prendre en considération, dans son évaluation des preuves et des arguments présentés, que les éléments directement liés aux critères quantitatifs, à savoir le poids de l'entreprise fournissant des services

de plateforme essentiels sur le marché intérieur, au-delà des recettes ou de la capitalisation boursière, par exemple sa taille en termes absolus ainsi que le nombre d'États membres dans lesquels elle est présente; la mesure dans laquelle le nombre d'entreprises utilisatrices et d'utilisateurs finaux réels dépasse les seuils ainsi que l'importance du service de plateforme essentiel de l'entreprise, compte tenu de l'échelle globale des activités du service de plateforme essentiel concerné; et le nombre d'années pendant lesquelles les seuils ont été atteints.

Toute justification reposant sur des motifs économiques, en rapport avec la définition du marché ou visant à démontrer des gains d'efficience découlant d'un type particulier de comportement de l'entreprise fournissant des services de plateforme essentiels, devrait être rejetée, car elle n'est pas pertinente pour la désignation d'un contrôleur d'accès. Si les arguments présentés ne sont pas suffisamment étayés et ne remettent manifestement pas en cause la présomption, la Commission devrait pouvoir les rejeter dans le délai de 45 jours ouvrables prévu pour la désignation. La Commission devrait être en mesure de prendre une décision en se fondant sur les informations disponibles en ce qui concerne les seuils quantitatifs lorsque l'entreprise fournissant les services de plateforme essentiels entrave l'enquête de manière significative en ne se conformant pas aux mesures d'enquête prises par la Commission.

(24) Il convient également de prévoir l'évaluation du rôle de contrôleur d'accès que jouent les entreprises fournissant des services de plateforme essentiels qui n'atteignent pas tous les seuils quantitatifs, à la lumière des exigences objectives globales selon lesquelles elles ont un poids important sur le marché intérieur, servent de points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux et bénéficient d'une position solide et durable dans leurs activités, ou sont susceptibles d'en bénéficier dans un avenir proche. Lorsque l'entreprise qui fournit des services de plateforme essentiels est une moyenne, une petite ou une microentreprise, l'évaluation devrait soigneusement examiner si une telle entreprise serait en mesure de compromettre substantiellement la contestabilité des services de plateforme essentiels, étant donné que le présent règlement vise principalement les grandes entreprises disposant d'un pouvoir économique considérable plutôt que les moyennes, les petites ou les microentreprises.

(25) Une telle évaluation ne peut être effectuée qu'à la lumière d'une enquête de marché, tout en tenant compte des seuils quantitatifs. Dans son évaluation, la Commission devrait prendre en compte les objectifs consistant à préserver et à promouvoir l'innovation et la qualité des produits et services numériques ainsi que l'équité et la compétitivité des prix, et veiller à ce que les niveaux de qualité et de choix offerts aux entreprises utilisatrices et aux utilisateurs finaux soient ou restent élevés. Des éléments spécifiques aux entreprises fournissant des services de plateforme essentiels concernées peuvent être pris en considération, tels que des économies d'échelle ou de gamme extrêmes, des effets de réseau très importants, des avantages fondés sur les données, leur capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce à leur caractère multiface, les effets de verrouillage, l'absence de multihébergement, une structure d'entreprise conglomérale ou l'intégration verticale. En outre, une capitalisation boursière très importante, un ratio de valeur de fonds propres par rapport au bénéfice très élevé ou un chiffre d'affaires très important tiré des utilisateurs finaux d'un seul service de plateforme essentiel peuvent être utilisés comme indicateurs du potentiel d'utilisation d'un effet de levier par ces entreprises et du basculement du marché en leur faveur. Avec la capitalisation boursière, les taux de croissance relatifs élevés sont des exemples de paramètres dynamiques particulièrement pertinents pour identifier les entreprises fournissant des services de plateforme essentiels dont on peut prévoir qu'elles acquerront une position solide et durable. La Commission devrait être en mesure de prendre une décision en tirant des conclusions défavorables à partir des données disponibles lorsque l'entreprise fournissant des services de plateforme essentiels entrave l'enquête de manière significative en refusant de se conformer aux mesures d'enquête prises par la Commission.

(26) Un sous-ensemble de règles particulier devrait s'appliquer aux entreprises fournissant des services de plateforme essentiels dont on peut prévoir qu'elles bénéficieront d'une position solide et durable dans un avenir proche. Les mêmes caractéristiques spécifiques des services de plateforme essentiels les rendent susceptibles de basculer: dès qu'une entreprise fournissant le service de plateforme essentiel a obtenu un certain avantage par rapport à ses concurrentes ou à des concurrentes potentielles en termes de taille ou de pouvoir d'intermédiation, sa position pourrait

devenir inattaquable et évoluer au point de devenir solide et durable dans un avenir proche. Les entreprises peuvent tenter de provoquer ce basculement et devenir des contrôleurs d'accès en recourant à certaines des conditions et pratiques déloyales régies par le présent règlement. Il semble adéquat d'intervenir dans une telle situation, avant que le marché ne bascule de manière irréversible.

(27) Cependant, une telle intervention précoce devrait se limiter à imposer uniquement les obligations nécessaires et appropriées pour veiller à ce que les services concernés restent contestables et permettre que le risque qualifié de conditions et pratiques déloyales soit évité. Les obligations empêchant l'entreprise fournissant des services de plateforme essentiels concernée de bénéficier d'une position solide et durable dans ses activités, telles que les obligations visant à empêcher l'utilisation d'un effet de levier et celles facilitant le changement de plateforme et le multihébergement, visent plus directement cet objectif. Dans le but de garantir la proportionnalité, la Commission devrait également appliquer, parmi ce sous-ensemble d'obligations, uniquement celles qui sont nécessaires et proportionnées pour atteindre les objectifs du présent règlement, et devrait régulièrement réexaminer ces obligations afin de déterminer si elles doivent être maintenues, supprimées ou adaptées.

(28) Appliquer uniquement les obligations qui sont nécessaires et proportionnées pour atteindre les objectifs du présent règlement devrait permettre à la Commission d'intervenir efficacement et en temps opportun, tout en respectant pleinement la proportionnalité des mesures envisagées. Cela devrait en outre rassurer les acteurs actuels ou potentiels du marché quant à la contestabilité et à l'équité des services visés.

(29) Les contrôleurs d'accès devraient respecter les obligations énoncées dans le présent règlement en ce qui concerne chacun des services de plateforme essentiels énumérés dans la décision de désignation correspondante. Le cas échéant, les obligations devraient s'appliquer tout en tenant compte de la situation de conglomérat des contrôleurs d'accès. En outre, la Commission devrait pouvoir, par voie de décision, imposer des mesures d'exécution au contrôleur d'accès. Ces mesures d'exécution devraient être conçues efficacement, eu égard aux caractéristiques des services de plateforme essentiels ainsi qu'aux risques éventuels de contournement, et dans le respect du principe de proportionnalité et des droits fondamentaux des entreprises visées et des tiers.

(30) La nature technologique complexe et en très rapide évolution des services de plateforme essentiels nécessite un réexamen régulier du statut des contrôleurs d'accès, y compris ceux dont on peut prévoir qu'ils bénéficieront, dans un avenir proche, d'une position solide et durable dans leurs activités. Afin de fournir à tous les acteurs du marché, y compris les contrôleurs d'accès, la sécurité requise en ce qui concerne les obligations juridiques applicables, il convient de fixer un délai pour ces réexamens réguliers. Il importe également de mener ces réexamens à intervalles réguliers et au moins tous les trois ans. En outre, il importe de préciser que tout changement des éléments de fait sur la base desquels une entreprise fournissant des services de plateforme essentiels a été désignée comme contrôleur d'accès ne devrait pas nécessiter que la décision de désignation soit modifiée. Une modification ne sera nécessaire que si le changement des éléments de fait entraîne également une modification de l'évaluation. Pour décider s'il en va ainsi ou pas, il convient de se fonder sur une évaluation au cas par cas des faits et circonstances.

(31) Pour préserver la contestabilité et l'équité des services de plateforme essentiels fournis par les contrôleurs d'accès, il est important de prévoir de manière claire et non équivoque un ensemble de règles harmonisées relatives à ces services. De telles règles sont nécessaires face au risque que représentent les effets néfastes des pratiques des contrôleurs d'accès, et sont bénéfiques pour l'environnement commercial des services concernés, les utilisateurs et, en fin de compte, la société dans son ensemble. Les obligations correspondent aux pratiques qui sont considérées comme compromettant la contestabilité ou comme déloyales, ou les deux, compte tenu des caractéristiques du secteur numérique, et qui ont une incidence directe particulièrement négative sur les entreprises utilisatrices et les utilisateurs finaux. Les obligations énoncées dans le présent règlement devraient pouvoir prendre spécifiquement en considération la nature des services de plateforme essentiels fournis. Les obligations prévues par le présent règlement devraient non seulement garantir la contestabilité et l'équité en ce qui concerne les services de plateforme essentiels énumérés dans la décision de désignation, mais aussi en ce qui concerne d'autres produits et services numériques grâce auxquels les contrôleurs d'accès tirent parti de leur position de point d'accès et qui sont

souvent fournis en accompagnement ou à l'appui des services de plateforme essentiels.

(32) Aux fins du présent règlement, la contestabilité devrait se rapporter à la capacité des entreprises à surmonter efficacement les barrières à l'entrée et à l'expansion, et à faire concurrence au contrôleur d'accès sur la base des mérites de leurs produits et services. Les caractéristiques des services de plateforme essentiels dans le secteur numérique, telles que les effets de réseau, les importantes économies d'échelle et les avantages tirés des données, limitent la contestabilité de ces services et des écosystèmes connexes. Cette faible contestabilité réduit les incitations à innover et à améliorer les produits et services pour le contrôleur d'accès, ses entreprises utilisatrices, ses concurrents et ses clients, et a donc une incidence négative sur le potentiel d'innovation de l'économie des plateformes en ligne au sens large. La contestabilité des services dans le secteur numérique peut également être limitée s'il y a plus d'un contrôleur d'accès pour un service de plateforme essentiel. Le présent règlement devrait donc interdire certaines pratiques des contrôleurs d'accès qui sont susceptibles de renforcer les barrières à l'entrée ou à l'expansion, et imposer aux contrôleurs d'accès certaines obligations qui tendent à abaisser ces barrières. Les obligations devraient également porter sur les situations dans lesquelles la position du contrôleur d'accès peut être tellement solide que la concurrence interplateformes n'est pas effective à court terme, ce qui signifie que la concurrence interplateformes doit être créée ou renforcée.

(33) Aux fins du présent règlement, l'iniquité devrait être liée à un déséquilibre entre les droits et obligations des entreprises utilisatrices lorsque le contrôleur d'accès obtient un avantage disproportionné. Les acteurs du marché, y compris les entreprises utilisatrices de services de plateforme essentiels et les autres fournisseurs de services fournis en accompagnement ou à l'appui de ces services de plateforme essentiels, devraient être en mesure de tirer adéquatement parti des avantages découlant de leurs efforts d'innovation ou autres. En raison de leur position de point d'accès et de leur pouvoir de négociation supérieur, il se peut que les contrôleurs d'accès aient des comportements qui ne permettent pas à d'autres de tirer pleinement parti des avantages de leurs propres contributions et qu'ils fixent unilatéralement des conditions déséquilibrées pour l'utilisation de leurs services de plateforme essentiels ou des services fournis en accompagnement ou à l'appui de leurs services de plateforme essentiels. Ce déséquilibre n'est pas exclu du simple fait que le contrôleur d'accès offre gratuitement un service particulier à un groupe spécifique d'utilisateurs, et il peut également consister à écarter ou à défavoriser les entreprises utilisatrices, en particulier si ces dernières sont en concurrence avec les services fournis par le contrôleur d'accès. Le présent règlement devrait donc imposer des obligations aux contrôleurs d'accès pour ce qui est de ce type de comportements.

(34) La contestabilité et l'équité sont étroitement liées. L'absence de contestabilité ou la faible contestabilité d'un service donné peut permettre à un contrôleur d'accès de se livrer à des pratiques déloyales. De même, les pratiques déloyales d'un contrôleur d'accès peuvent réduire la possibilité pour les entreprises utilisatrices ou autres de contester sa position. Une obligation spécifique prévue par le présent règlement peut donc porter sur ces deux éléments.

(35) Dans la mesure où il n'existe pas de mesures alternatives moins restrictives qui conduiraient au même résultat, eu égard au besoin de protéger l'ordre public et la vie privée, et de lutter contre les pratiques commerciales frauduleuses et trompeuses, les obligations énoncées dans le présent règlement sont donc nécessaires pour répondre aux questions d'intérêt général soulevées.

Traitement de données à caractère personnel

(36) Les contrôleurs d'accès collectent souvent directement les données à caractère personnel des utilisateurs finaux aux fins de la fourniture de services de publicité en ligne lorsque les utilisateurs finaux utilisent des sites internet et des applications logicielles de tiers. Les tiers fournissent en outre aux contrôleurs d'accès les données à caractère personnel de leurs utilisateurs finaux aux fins de l'utilisation de certains services fournis par les contrôleurs d'accès dans le cadre de leurs services de plateforme essentiels, par exemple des audiences personnalisées. Le traitement, aux fins de la fourniture de services de publicité en ligne, de données à caractère personnel de tiers utilisant des services de plateforme essentiels offre aux contrôleurs d'accès des avantages potentiels en ce qui concerne l'accumulation de données, érigeant de ce fait des barrières à l'entrée. En effet, les contrôleurs d'accès traitent des données à caractère

personnel d'un nombre nettement plus élevé de tiers que d'autres entreprises. Des avantages similaires résultent des pratiques consistant i) à combiner les données à caractère personnel des utilisateurs finaux collectées auprès d'un service de plateforme essentiel avec les données collectées auprès d'autres services, ii) à recourir à l'utilisation croisée de données à caractère personnel provenant d'un service de plateforme essentiel dans d'autres services proposés séparément par le contrôleur d'accès, notamment ceux qui ne sont pas fournis en accompagnement ou à l'appui du service de plateforme essentiel concerné, et vice versa, ou iii) à connecter des utilisateurs finaux à différents services de contrôleurs d'accès afin de combiner des données à caractère personnel. Afin d'éviter que la contestabilité des services de plateforme essentiels ne soit injustement compromise par les contrôleurs d'accès, ceux-ci devraient permettre aux utilisateurs finaux de choisir librement d'adhérer à de telles pratiques de traitement de données et de connexion en proposant une autre possibilité moins personnalisée, mais équivalente, et sans subordonner l'utilisation du service de plateforme essentiel ou certaines de ses fonctionnalités au consentement de l'utilisateur final. Cela devrait être sans préjudice du fait que le contrôleur d'accès traite des données à caractère personnel ou connecte des utilisateurs finaux à un service, en invoquant comme base juridique l'article 6, paragraphe 1, points c),
d) et e), du règlement (UE) 2016/679, mais pas l'article 6, paragraphe 1, points b) et f), dudit règlement.

cf. RGPD

(37) L'autre possibilité moins personnalisée ne devrait pas être différente ou de qualité moindre par rapport au service offert aux utilisateurs finaux qui donnent leur consentement, sauf si une baisse de la qualité résulte directement du fait que le contrôleur d'accès n'est pas en mesure de traiter ces données à caractère personnel ou de connecter les utilisateurs finaux à un service. Il ne devrait pas être plus difficile de ne pas donner son consentement que de le donner. Lorsque le contrôleur d'accès demande le consentement, il devrait prendre les devants et présenter une solution conviviale à l'utilisateur final pour que celui-ci puisse donner, modifier ou retirer son consentement de façon explicite, claire et simple. En particulier, le consentement devrait être donné par une déclaration ou un acte positif clair par lequel l'utilisateur final manifeste de façon libre, spécifique, éclairée et univoque son accord, au sens du règlement (UE) 2016/679. Au moment de donner son consentement, et uniquement lorsqu'il y a lieu, l'utilisateur final devrait être informé que le fait de ne pas donner son consentement peut se traduire par une offre moins personnalisée, mais que, à tous autres égards, le service de plateforme essentiel restera inchangé et qu'aucune fonctionnalité ne sera supprimée. À titre exceptionnel, si le consentement ne peut être donné directement au service de plateforme essentiel du contrôleur d'accès, les utilisateurs finaux devraient être en mesure de donner leur consentement par l'intermédiaire de chaque service tiers qui utilise ce service de plateforme essentiel, pour permettre au contrôleur d'accès de traiter des données à caractère personnel aux fins de la fourniture de services de publicité en ligne.

cf. RGPD

Enfin, il devrait être aussi simple de retirer son consentement que de le donner. Les contrôleurs d'accès ne devraient pas concevoir, organiser ou exploiter leurs interfaces en ligne de façon à tromper ou à manipuler les utilisateurs finaux ou, de toute autre manière, à altérer ou à limiter substantiellement la capacité des utilisateurs finaux de donner librement leur consentement. En particulier, les contrôleurs d'accès ne devraient pas être autorisés à demander plus d'une fois par an aux utilisateurs finaux de donner leur consentement pour une finalité de traitement identique à celle pour laquelle ils n'ont initialement pas donné leur consentement ou ont retiré leur consentement. Le présent règlement est sans préjudice du règlement (UE) 2016/679, y compris son cadre d'application, qui reste pleinement applicable en ce qui concerne toute réclamation introduite par des personnes concernées en rapport avec une infraction aux droits que leur confère ledit règlement.

cf. RGPD

(38) Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel, notamment pour ce qui est de l'utilisation de leurs données à caractère personnel à des fins de communication commerciale ou de création de profils d'utilisateurs. La protection des enfants en ligne est un objectif important de l'Union, qui devrait être pris en compte dans le droit applicable de l'Union. Dans ce contexte, il convient de prendre dûment en considération le règlement relatif au marché intérieur des services numériques. Aucune disposition du présent règlement ne dispense les contrôleurs d'accès de l'obligation de protéger les enfants prévue dans le droit applicable de l'Union.

Cas des enfants

Liberté de choix

(39) Dans certains cas, par exemple lorsqu'ils imposent des conditions contractuelles, les contrôleurs d'accès peuvent restreindre la capacité des entreprises utilisatrices de leurs services d'intermédiation en ligne de proposer des produits ou des services aux utilisateurs finaux à des conditions plus favorables, notamment en matière de prix, par le biais d'autres services d'intermédiation en ligne ou de canaux de vente directe en ligne. Lorsque de telles restrictions concernent des services d'intermédiation en ligne de tiers, elles limitent la contestabilité interplateformes, et donc le choix des utilisateurs finaux pour ce qui est des autres services d'intermédiation en ligne. Lorsque ces restrictions concernent des canaux de vente directe en ligne, elles limitent injustement la liberté des entreprises utilisatrices d'utiliser ces canaux. Pour que les entreprises utilisatrices des services d'intermédiation en ligne des contrôleurs d'accès puissent librement choisir d'autres services d'intermédiation en ligne ou d'autres canaux de vente directe en ligne, et différencier les conditions dans lesquelles elles proposent leurs produits ou services aux utilisateurs finaux, les contrôleurs d'accès ne devraient pas être autorisés à limiter les entreprises utilisatrices dans leur choix de différencier les conditions commerciales, y compris les prix. Une telle restriction devrait s'appliquer à toute mesure dont les effets sont équivalents, telle que l'augmentation des taux de commission ou le déréférencement des offres des entreprises utilisatrices.

(40) Afin d'éviter une aggravation de leur dépendance à l'égard des services de plateforme essentiels des contrôleurs d'accès et de promouvoir le multihébergement, les entreprises utilisatrices de ces contrôleurs d'accès devraient être libres de promouvoir et de choisir le canal de distribution qu'elles jugent le plus approprié pour interagir avec les utilisateurs finaux qu'elles ont déjà acquis par l'intermédiaire des services de plateforme essentiels fournis par les contrôleurs d'accès ou d'autres canaux. Cela devrait être valable pour la promotion des offres, y compris au moyen d'une application logicielle de l'entreprise utilisatrice, ainsi que pour toute forme de communication et de conclusion de contrats entre les entreprises utilisatrices et les utilisateurs finaux. Un utilisateur final est un utilisateur final acquis s'il a déjà établi une relation commerciale avec l'entreprise utilisatrice et que, le cas échéant, le contrôleur d'accès a été rémunéré directement ou indirectement par l'entreprise utilisatrice pour faciliter l'acquisition initiale de l'utilisateur final par l'entreprise utilisatrice. De telles relations commerciales peuvent être payantes ou gratuites, par exemple, des essais gratuits, des niveaux de service gratuits, et peuvent avoir été établies soit via le service de plateforme essentiel du contrôleur d'accès, soit par tout autre canal. Inversement, les utilisateurs finaux devraient également être libres de choisir les offres de ces entreprises utilisatrices et de conclure des contrats avec elles, soit, le cas échéant, par l'intermédiaire des services de plateforme essentiels du contrôleur d'accès, soit à partir d'un canal de distribution direct de l'entreprise utilisatrice ou d'un autre canal indirect auquel l'entreprise utilisatrice a recours.

(41) La capacité des utilisateurs finaux d'acheter du contenu, des abonnements, des fonctionnalités ou autres en dehors des services de plateforme essentiels des contrôleurs d'accès ne devrait être ni compromise ni restreinte. Il convient particulièrement d'éviter une situation dans laquelle les contrôleurs d'accès restreignent l'utilisation de ces services et l'accès à ces services par les utilisateurs finaux au moyen d'une application logicielle fonctionnant sur leur service de plateforme essentiel. Par exemple, les abonnés à un contenu en ligne acheté sans passer par une application logicielle, une boutique d'applications logicielles ou un assistant virtuel ne devraient pas être empêchés d'accéder à ce contenu en ligne sur une application logicielle du service de plateforme essentiel du contrôleur d'accès au seul motif que l'achat s'est fait sans passer par cette application logicielle, cette boutique d'applications logicielles ou cet assistant virtuel.

Signalement

(42) Garantir le droit des entreprises utilisatrices et utilisateurs finaux, y compris les lanceurs d'alerte, de faire part de préoccupations quant aux pratiques déloyales des contrôleurs d'accès en signalant tout problème lié au non-respect du droit de l'Union ou national pertinent à toute autorité administrative ou autre autorité publique compétente, y compris les juridictions nationales, est essentiel à la préservation d'un environnement commercial équitable et à la protection de la contestabilité du secteur numérique. Par exemple, il se peut que des entreprises utilisatrices ou des utilisateurs finaux veuillent se plaindre de différents types de pratiques déloyales, tels que des conditions d'accès discriminatoires, la clôture injustifiée de comptes d'entreprises utilisatrices ou la motivation peu claire de déréférencements de produits. Par conséquent, toute pratique qui constituerait un obstacle pour ces utilisateurs ou qui les empêcherait de quelque manière que ce soit de faire part de leurs préoccupations ou de demander

réparation, au moyen par exemple de clauses de confidentialité dans les accords ou d'autres conditions écrites, devrait être interdite. Cette interdiction devrait être sans préjudice du droit des entreprises utilisatrices et des contrôleurs d'accès d'établir, dans leurs accords, les conditions d'utilisation, y compris le recours à des mécanismes légaux de traitement des plaintes, notamment à tout mécanisme de règlement extrajudiciaire des litiges, ou le recours à la compétence de tribunaux spécifiques dans le respect du droit de l'Union et du droit national applicable. Cela devrait également être sans préjudice du rôle que jouent les contrôleurs d'accès dans la lutte contre la présence de contenus illicites en ligne.

Procédés illicites

(43) Certains services fournis en accompagnement ou à l'appui des services de plateforme essentiels pertinents du contrôleur d'accès, par exemple les services d'identification, les moteurs de navigateurs internet, les services de paiement ou les services techniques qui soutiennent la fourniture de services de paiement, tels que les systèmes de paiement pour les achats intégrés dans des applications, sont essentiels pour que les entreprises utilisatrices puissent mener leurs activités et pour leur permettre d'optimiser leurs services. En particulier, chaque navigateur est construit sur un moteur de navigateur internet, qui est responsable des principales fonctionnalités du navigateur, telles que la vitesse, la fiabilité et la compatibilité internet. Lorsque les contrôleurs d'accès exploitent et imposent des moteurs de navigateurs internet, ils sont en mesure de déterminer quelles fonctionnalités et quelles normes s'appliqueront non seulement à leurs propres navigateurs internet, mais aussi aux navigateurs internet concurrents et, en aval, aux applications logicielles internet. Les contrôleurs d'accès ne devraient donc pas tirer parti de leur position pour exiger des entreprises utilisatrices qui dépendent d'eux qu'elles recourent à l'un quelconque des services fournis en accompagnement ou à l'appui des services de plateforme essentiels par le contrôleur d'accès lui-même dans le cadre de la fourniture de services ou de produits par ces entreprises utilisatrices. Pour éviter une situation dans laquelle les contrôleurs d'accès imposent indirectement aux entreprises utilisatrices leurs propres services fournis en accompagnement ou à l'appui des services de plateforme essentiels, il devrait en outre être interdit aux contrôleurs d'accès d'exiger des utilisateurs finaux qu'ils recourent à ces services lorsque cette exigence serait imposée dans le contexte du service fourni aux utilisateurs finaux par l'entreprise utilisatrice qui recourt au service de plateforme essentiel du contrôleur d'accès. Cette interdiction vise à protéger la liberté de l'entreprise utilisatrice de choisir d'autres services que ceux du contrôleur d'accès et ne devrait pas être interprétée comme obligeant l'entreprise utilisatrice à proposer de telles alternatives à ses utilisateurs finaux.

(44) Le procédé consistant à exiger des entreprises utilisatrices ou des utilisateurs finaux qu'ils s'abonnent ou s'enregistrent auprès de tout autre service de plateforme essentiel d'un contrôleur d'accès énuméré dans la décision de désignation ou qu'ils atteignent les seuils quantitatifs concernant les utilisateurs finaux actifs et les entreprises utilisatrices actives fixés dans le présent règlement, comme condition d'utilisation, d'accès, d'inscription ou d'enregistrement pour un service de plateforme essentiel, donne aux contrôleurs d'accès un moyen de capter ou de rendre captifs de nouvelles entreprises utilisatrices et de nouveaux utilisateurs finaux pour ses services de plateforme essentiels en faisant en sorte que les entreprises utilisatrices ne puissent accéder à un service de plateforme essentiel sans s'enregistrer ou créer un compte dans le but de recevoir un deuxième service de plateforme essentiel. Ce procédé confère également aux contrôleurs d'accès un avantage potentiel en ce qui concerne l'accumulation de données. En tant que tel, il est donc susceptible d'ériger des barrières à l'entrée et devrait être interdit.

Publicité en ligne

(45) Les conditions dans lesquelles les contrôleurs d'accès fournissent des services de publicité en ligne aux entreprises utilisatrices, dont les annonceurs et les éditeurs, manquent souvent de transparence et sont opaques. Cette opacité est en partie liée aux pratiques de quelques plateformes, mais elle résulte aussi de la complexité même de la publicité programmatique moderne. On estime que ce secteur est devenu moins transparent après l'introduction de la nouvelle législation portant sur la vie privée. Pour les annonceurs et les éditeurs, cela conduit souvent à un manque d'informations et de connaissances quant aux conditions des services de publicité en ligne qu'ils achètent et compromet leur capacité à changer d'entreprise fournissant des services de publicité en ligne. En outre, les coûts des services de publicité en ligne dans ces conditions sont susceptibles d'être plus élevés que dans un environnement de plateforme plus équitable, plus transparent et contestable. Ces coûts plus élevés se répercuteront vraisemblablement sur les prix que paieront les utilisateurs finaux pour de nombreux produits

et services quotidiens qui reposent sur l'utilisation des services de publicité en ligne. Les obligations de transparence devraient donc exiger des contrôleurs d'accès qu'ils communiquent gratuitement aux annonceurs et éditeurs à qui ils fournissent des services de publicité en ligne, sur demande, les informations nécessaires aux deux parties pour comprendre le prix payé pour chacun des différents services de publicité en ligne fournis dans le cadre de la chaîne de valeur publicitaire correspondante.

Ces informations devraient être fournies, sur demande, à un annonceur au niveau d'une publicité individuelle en ce qui concerne le prix et les honoraires facturés à cet annonceur et, sous réserve de l'accord de l'éditeur propriétaire de l'inventaire dans lequel la publicité est affichée, la rémunération perçue par cet éditeur consentant. La fourniture quotidienne de ces informations permettra aux annonceurs de recevoir des informations présentant un niveau de granularité suffisant pour comparer les coûts d'utilisation des services de publicité en ligne des contrôleurs d'accès aux coûts liés à l'utilisation des services de publicité en ligne d'autres entreprises. Si certains éditeurs ne donnent pas leur consentement au partage des informations pertinentes avec l'annonceur, le contrôleur d'accès devrait fournir à l'annonceur les informations relatives à la rémunération moyenne journalière perçue par ces éditeurs pour les publicités concernées. La même obligation et les mêmes principes de partage des informations pertinentes concernant la fourniture de services de publicité en ligne devraient s'appliquer aux demandes des éditeurs. Étant donné que les contrôleurs d'accès peuvent utiliser différents modèles de tarification pour la fourniture de services de publicité en ligne aux annonceurs et aux éditeurs, par exemple un prix par impression, par vue ou tout autre critère, les contrôleurs d'accès devraient également indiquer la méthode de calcul de chacun des prix et de chacune des rémunérations.

Double rôle du contrôleur d'accès

(46) Dans certaines circonstances, un contrôleur d'accès joue un double rôle lorsque, en tant qu'entreprise fournissant des services de plateforme essentiels, il fournit à ses entreprises utilisatrices un service de plateforme essentiel et éventuellement d'autres services fournis en accompagnement ou à l'appui de ce service de plateforme essentiel, et que, parallèlement, il se trouve ou compte se trouver en concurrence avec ces mêmes entreprises pour la fourniture aux mêmes utilisateurs finaux de services ou de produits identiques ou similaires. Dans de telles circonstances, un contrôleur d'accès peut profiter de son double rôle pour utiliser des données générées ou fournies par ses entreprises utilisatrices dans le cadre des activités qu'elles exercent lorsqu'elles ont recours aux services de plateforme essentiels ou aux services fournis en accompagnement ou à l'appui de ces services de plateforme essentiels, aux fins de ses propres services ou produits. Les données de l'entreprise utilisatrice peuvent également inclure toutes données générées par les activités de ses utilisateurs finaux ou fournies au cours de ces activités. Tel peut être le cas lorsqu'un contrôleur d'accès fournit aux entreprises utilisatrices une place de marché en ligne ou une boutique d'applications logicielles, et que, parallèlement, il fournit des services en tant qu'entreprise fournissant des services de détail en ligne ou des applications logicielles. Afin d'empêcher les contrôleurs d'accès de tirer injustement profit de leur double rôle, il est nécessaire de veiller à ce qu'ils n'utilisent pas les données agrégées ou non agrégées, qui pourraient comprendre les données anonymisées et les données à caractère personnel qui ne sont pas accessibles au grand public, dans le but de fournir des services similaires à ceux de leurs entreprises utilisatrices. Cette obligation devrait s'appliquer au contrôleur d'accès dans son ensemble, et notamment mais pas exclusivement, à son unité opérationnelle qui est en concurrence avec les entreprises utilisatrices d'un service de plateforme essentiel.

(47) Les entreprises utilisatrices peuvent également acheter des services de publicité en ligne à une entreprise fournissant des services de plateforme essentiels dans le but de fournir des biens et des services aux utilisateurs finaux. Dans ces circonstances, il peut arriver que les données ne soient pas générées dans le service de plateforme essentiel, mais soient fournies à ce service par l'entreprise utilisatrice, ou soient générées à partir des opérations qu'elle effectue par l'intermédiaire du service de plateforme essentiel concerné. Dans certains cas, ce service de plateforme essentiel fournissant de la publicité peut jouer un double rôle en tant qu'entreprise fournissant des services de publicité en ligne et en tant qu'entreprise fournissant des services entrant en concurrence avec ceux des entreprises utilisatrices. En conséquence, l'interdiction imposée à un contrôleur d'accès jouant un double rôle d'utiliser les données des entreprises utilisatrices devrait également s'appliquer aux données qu'un service de plateforme essentiel a reçues des entreprises aux fins de la fourniture de services de publicité en ligne liés à ce service de plateforme essentiel.

(48) En ce qui concerne les services d'informatique en nuage, l'obligation de ne pas utiliser les données des entreprises utilisatrices devrait s'étendre aux données fournies ou générées par les entreprises utilisatrices dans le cadre de leur utilisation du service d'informatique en nuage du contrôleur d'accès, ou par l'intermédiaire de sa boutique d'applications logicielles qui permet aux utilisateurs finaux des services d'informatique en nuage d'accéder aux applications logicielles. Cette obligation ne devrait pas porter atteinte au droit du contrôleur d'accès d'utiliser des données agrégées pour la fourniture d'autres services fournis en accompagnement ou à l'appui de son service de plateforme essentiel, par exemple des services d'analyse de données, dans le respect du règlement (UE) 2016/679 et de la directive 2002/58/CE, ainsi que des obligations pertinentes du présent règlement relatives à ces services.

cf. RGPD

(49) Un contrôleur d'accès peut recourir à divers moyens pour favoriser ses propres services ou produits ou ceux d'un tiers sur son système d'exploitation, son assistant virtuel ou son navigateur internet au détriment de services identiques ou similaires que les utilisateurs finaux pourraient obtenir par l'intermédiaire d'autres tiers. Cela peut notamment se produire lorsque certaines applications logicielles ou certains services sont préinstallés par le contrôleur d'accès. Pour permettre aux utilisateurs finaux de choisir, les contrôleurs d'accès ne devraient pas les empêcher de désinstaller toute application logicielle sur leur système d'exploitation. Il ne devrait être possible pour le contrôleur d'accès de restreindre cette désinstallation que lorsque ces applications logicielles sont essentielles au fonctionnement du système d'exploitation ou de l'appareil. Les contrôleurs d'accès devraient par ailleurs permettre aux utilisateurs finaux de modifier facilement les paramètres par défaut du système d'exploitation, de l'assistant virtuel et du navigateur internet lorsque ces paramètres par défaut favorisent leurs propres applications logicielles et services. Cela peut se faire notamment en présentant un choix à l'écran, lorsque l'utilisateur recourt pour la première fois à un moteur de recherche en ligne, à un assistant virtuel ou à un navigateur internet du contrôleur d'accès énuméré dans la décision de désignation, permettant aux utilisateurs finaux de sélectionner un autre service par défaut lorsque le système d'exploitation du contrôleur d'accès oriente les utilisateurs finaux vers ce moteur de recherche en ligne, cet assistant virtuel ou ce navigateur internet et lorsque l'assistant virtuel ou le navigateur internet du contrôleur d'accès oriente l'utilisateur vers le moteur de recherche en ligne énuméré dans la décision de désignation.

Préinstallation/désinstallation

(50) Les règles fixées par un contrôleur d'accès pour la distribution d'applications logicielles peuvent, dans certaines circonstances, restreindre la capacité des utilisateurs finaux d'installer et d'utiliser effectivement les applications logicielles ou les boutiques d'applications logicielles de tiers sur le matériel informatique ou les systèmes d'exploitation de ce contrôleur d'accès, et restreindre également la capacité des utilisateurs finaux d'accéder à de telles applications logicielles ou boutiques d'applications logicielles sans passer par les services de plateforme essentiels de ce contrôleur d'accès. De telles restrictions peuvent limiter la capacité des développeurs d'applications logicielles d'utiliser d'autres canaux de distribution et la capacité des utilisateurs finaux de choisir entre les différentes applications logicielles de différents canaux de distribution, et devraient être interdites comme étant déloyales et susceptibles d'affaiblir la contestabilité des services de plateforme essentiels. Afin de garantir la contestabilité, le contrôleur d'accès devrait en outre permettre aux applications logicielles ou boutiques d'applications logicielles de tiers de demander à l'utilisateur final de décider si ce service devrait devenir le service par défaut et de permettre que le changement soit effectué facilement.

Applications par défaut

Le contrôleur d'accès concerné devrait pouvoir mettre en œuvre des mesures techniques ou contractuelles proportionnées dans le but d'éviter que les applications logicielles ou les boutiques d'applications logicielles de tiers ne compromettent l'intégrité du matériel informatique ou du système d'exploitation qu'il fournit, s'il démontre que ces mesures sont nécessaires et justifiées et qu'il n'existe aucun moyen moins restrictif de préserver cette intégrité. L'intégrité du matériel informatique ou du système d'exploitation devrait inclure tous les choix de conception qui doivent être mis en œuvre et faire l'objet d'une maintenance pour protéger le matériel informatique ou le système d'exploitation contre tout accès non autorisé, en veillant à ce que les contrôles de sécurité spécifiés pour le matériel informatique ou le système d'exploitation concerné ne puissent être compromis. En outre, afin de garantir que les applications logicielles ou boutiques d'applications logicielles de tiers ne compromettent pas la sécurité des utilisateurs finaux, le contrôleur d'accès devrait pouvoir mettre en œuvre

des mesures et des paramètres strictement nécessaires et proportionnés, autres que les paramètres par défaut, permettant aux utilisateurs finaux de garantir efficacement la sécurité, pour ce qui concerne les applications logicielles ou boutiques d'applications logicielles de tiers, si le contrôleur d'accès démontre que de telles mesures et de tels paramètres sont strictement nécessaires et justifiés et qu'il n'existe pas de moyens moins restrictifs d'atteindre cet objectif. Le contrôleur d'accès devrait être empêché de mettre en œuvre de telles mesures en tant que paramètres par défaut ou fonctionnalités préinstallées.

Intégration verticale

(51) Les contrôleurs d'accès sont souvent verticalement intégrés et proposent certains produits ou services aux utilisateurs finaux par l'intermédiaire de leurs propres services de plateforme essentiels ou d'une entreprise utilisatrice sur laquelle ils exercent un contrôle, ce qui entraîne fréquemment des conflits d'intérêts. Cette situation se présente notamment lorsqu'un contrôleur d'accès fournit ses propres services d'intermédiation en ligne au travers d'un moteur de recherche en ligne. Lorsqu'ils proposent ces produits ou services dans le service de plateforme essentiel, les contrôleurs d'accès peuvent assurer une meilleure position, en termes de classement, ainsi que pour l'indexation et l'exploration qui y sont liées, à leur propre offre par rapport à celle des produits ou services des tiers également actifs dans ce service de plateforme essentiel. Cela peut notamment se produire avec des produits ou des services, y compris d'autres services de plateforme essentiels, qui sont classés parmi les résultats communiqués par des moteurs de recherche en ligne ou qui sont partiellement ou entièrement intégrés dans les résultats de moteurs de recherche en ligne, les groupes de résultats spécialisés dans un domaine défini, ou affichés avec les résultats d'un moteur de recherche en ligne, qui sont considérés ou utilisés par certains utilisateurs finaux comme un service distinct du moteur de recherche en ligne ou additionnel.

Les applications logicielles distribuées par l'intermédiaire de boutiques d'applications logicielles, ou les vidéos distribuées par l'intermédiaire de plateformes de partage de vidéos, ou les produits ou services mis en avant et affichés dans le fil d'actualité d'un service de réseau social en ligne, ou les produits ou services classés parmi des résultats de recherche ou affichés sur une place de marché en ligne, ou encore des produits ou services offerts par l'intermédiaire d'un assistant virtuel constituent d'autres exemples. Cette phase dans laquelle une position privilégiée est réservée à l'offre du contrôleur d'accès lui-même peut avoir lieu avant même qu'intervienne le classement à la suite d'une recherche, par exemple lors de l'exploration et de l'indexation. Par exemple, dès l'étape de l'exploration, un processus de découverte permettant de trouver des contenus nouveaux et mis à jour, ainsi que celle de l'indexation, qui implique le stockage et l'organisation des contenus trouvés au cours du processus d'exploration, le contrôleur d'accès peut favoriser son propre contenu par rapport à celui de tiers. Dans ces circonstances, le contrôleur d'accès joue un double rôle, en tant qu'intermédiaire vis-à-vis des entreprises tierces et en tant qu'entreprise fournissant directement des produits ou services. En conséquence, de tels contrôleurs d'accès sont en mesure de compromettre directement la contestabilité de ces produits ou services dans ces services de plateforme essentiels, au détriment des entreprises utilisatrices qui ne sont pas sous leur contrôle.

(52) Dans ces circonstances, le contrôleur d'accès ne devrait accorder aux produits ou aux services qu'il fournit soit lui- même soit à travers une entreprise utilisatrice qu'il contrôle aucune forme de traitement différencié ou préférentiel en matière de classement, ainsi que pour l'indexation et l'exploration qui y sont liées, dans le service de plateforme essentiel, que ce soit par des moyens juridiques, commerciaux ou techniques. Afin que cette obligation soit effective, les conditions s'appliquant à un tel classement devraient être généralement équitables et transparentes. Dans ce contexte, le classement devrait couvrir toutes les formes de priorité relative, dont l'affichage, la notation, la création de liens hypertextes ou les résultats vocaux, et devrait également inclure les cas où un service de plateforme essentiel ne présente ou ne communique qu'un seul résultat à l'utilisateur final. Afin que cette obligation soit effective et ne puisse pas être contournée, il convient de l'appliquer également à toute mesure qui a un effet équivalent à un traitement différencié ou préférentiel en matière de classement. Les lignes directrices adoptées en vertu de l'article 5 du règlement (UE) 2019/1150 devraient également faciliter la mise en œuvre et le contrôle du respect de cette obligation.

(53) Les contrôleurs d'accès ne devraient pas restreindre ou entraver le libre choix des utilisateurs finaux en empêchant techniquement ou de toute autre manière le change-

ment vers d'autres applications logicielles ou services ou l'abonnement à d'autres applications logicielles ou services. Cela permettrait à un plus grand nombre d'entreprises de proposer leurs services, ce qui, en définitive, élargirait le choix offert aux utilisateurs finaux. Les contrôleurs d'accès devraient garantir ce libre choix, qu'ils soient ou non les fabricants du matériel informatique au moyen duquel se fait l'accès aux applications logicielles ou aux services, et ne devraient créer aucun obstacle artificiel, technique ou autre, visant à rendre impossible ou ineffectif le changement de plateforme. Ne devraient pas être considérées comme un obstacle interdit au changement de plateforme la simple offre d'un produit ou service donné aux consommateurs, y compris au moyen d'une préinstallation, de même que l'amélioration de l'offre pour les utilisateurs finaux, telle que des prix plus avantageux ou une qualité supérieure.

(54) Les contrôleurs d'accès peuvent entraver la capacité des utilisateurs finaux d'accéder aux contenus et services en ligne, y compris les applications logicielles. Par conséquent, il convient d'établir des règles visant à empêcher que le comportement des contrôleurs d'accès compromette les droits des utilisateurs finaux à accéder à un internet ouvert. De même, il se peut que les contrôleurs d'accès limitent techniquement la capacité des utilisateurs finaux de changer effectivement d'entreprise fournissant un service d'accès à l'internet, en particulier grâce au contrôle qu'ils exercent sur le matériel informatique ou les systèmes d'exploitation. Cela fausse les conditions de concurrence pour les services d'accès à l'internet et, en fin de compte, nuit aux utilisateurs finaux. Il convient donc de veiller à ce que les contrôleurs d'accès ne restreignent pas indûment le choix des utilisateurs finaux en ce qui concerne l'entreprise fournissant des services d'accès à l'internet.

(55) Un contrôleur d'accès peut fournir des services ou du matériel informatique, comme des appareils portables, qui ont accès à des caractéristiques matérielles ou logicielles d'un appareil accessibles ou contrôlées par l'intermédiaire d'un système d'exploitation ou d'un assistant virtuel afin d'offrir des fonctionnalités spécifiques aux utilisateurs finaux. En pareil cas, les fournisseurs concurrents de services ou de matériel informatique, tels que les fournisseurs d'appareils portables, ont besoin d'une interopérabilité tout aussi effective avec les mêmes caractéristiques matérielles ou logicielles, ainsi que d'un accès à ces caractéristiques aux fins de l'interopérabilité, pour pouvoir proposer une offre concurrentielle aux utilisateurs finaux.

(56) Les contrôleurs d'accès peuvent également jouer un double rôle en tant que développeurs de systèmes d'exploitation et en tant que fabricants d'appareils, y compris des fonctionnalités techniques qu'un appareil peut avoir. Par exemple, un contrôleur d'accès qui est également le fabricant d'un appareil peut restreindre l'accès à certaines des fonctionnalités de ce dernier, telles que la technologie de communication en champ proche, les éléments sécurisés et les processeurs, les mécanismes d'authentification et le logiciel utilisé pour exploiter ces technologies, qui peuvent être nécessaires à la fourniture effective d'un service, fournis conjointement au service de plateforme essentiel ou à l'appui de celui-ci, par le contrôleur d'accès ainsi que par toute entreprise tierce fournissant potentiellement un tel service.

(57) Si les doubles rôles sont exercés d'une manière qui empêche d'autres fournisseurs de services ou de matériel informatique d'avoir accès dans les mêmes conditions aux mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées par le contrôleur d'accès dans le cadre de la fourniture de ses propres services ou matériel informatique complémentaires ou d'appui, la capacité d'innovation de ces autres fournisseurs et le choix des utilisateurs finaux pourraient s'en trouver grandement compromis. Les contrôleurs d'accès devraient donc être tenus d'assurer, gratuitement, une interopérabilité effective avec les mêmes caractéristiques du système d'exploitation, du matériel informatique ou du logiciel que celles qui sont disponibles ou utilisées dans le cadre de la fourniture de ses propres services et matériel informatique complémentaires et d'appui, ainsi que l'accès, aux fins de l'interopérabilité, à ces caractéristiques. Un tel accès peut également être exigé par des applications logicielles liées aux services concernés fournis conjointement au service de plateforme essentiel ou à l'appui de celui-ci afin de développer et offrir effectivement des fonctionnalités interopérables avec celles proposées par les contrôleurs d'accès. Ces obligations ont pour objet de permettre à des tiers concurrents de s'interconnecter, au moyen d'interfaces ou de solutions similaires, aux caractéristiques concernées de manière aussi effective que pour les propres services ou matériel informatique du contrôleur d'accès.

(58) Les conditions dans lesquelles les contrôleurs d'accès fournissent des services de publicité en ligne aux entreprises utilisatrices, dont les annonceurs et les éditeurs, manquent souvent de transparence et sont opaques. Cela conduit souvent à un manque d'informations pour les annonceurs et éditeurs quant à l'effet d'une annonce publicitaire donnée. Dans le but de renforcer l'équité, la transparence et la contestabilité des services de publicité en ligne énumérés dans la décision de désignation, de même que ceux qui sont pleinement intégrés à d'autres services de plateforme essentiels de la même entreprise, les contrôleurs d'accès devraient fournir aux annonceurs et aux éditeurs, ainsi qu'aux tiers autorisés par les annonceurs et les éditeurs, sur demande, un accès gratuit à leurs outils de mesure de performance et aux données, tant agrégées que non agrégées, nécessaires aux annonceurs, aux tiers autorisés tels que les agences de publicité agissant pour le compte d'une entreprise de placement de publicité et aux éditeurs pour effectuer leur propre vérification indépendante de la fourniture des services de publicité en ligne concernés.

Mesure de performance de la publicité en ligne

(59) Les contrôleurs d'accès bénéficient d'un accès à de grandes quantités de données qu'ils collectent lorsqu'ils fournissent des services de plateforme essentiels, ainsi que d'autres services numériques. Afin d'empêcher les contrôleurs d'accès de nuire à la contestabilité des services de plateforme essentiels, ou au potentiel d'innovation d'un secteur numérique dynamique, en limitant le changement de plateforme ou le multihébergement, il convient d'accorder aux utilisateurs finaux, ainsi qu'aux tiers autorisés par un utilisateur final, un accès effectif et immédiat aux données qu'ils ont fournies ou qui ont été générées par leur activité sur les services de plateforme essentiels concernés du contrôleur d'accès. Les données devraient être reçues dans un format permettant qu'elles soient immédiatement et effectivement consultées et utilisées par l'utilisateur final ou le tiers concerné autorisé par l'utilisateur final à qui elles sont transmises. Les contrôleurs d'accès devraient également veiller, au moyen de mesures techniques appropriées et de haute qualité, telles que des interfaces de programmation, à ce que les utilisateurs finaux ou les tiers autorisés par les utilisateurs finaux puissent librement transférer les données en continu et en temps réel. Cela devrait également s'appliquer à toutes les autres données, à différents niveaux d'agrégation, nécessaires pour permettre effectivement cette portabilité. Pour éviter toute ambiguïté, l'obligation faite au contrôleur d'accès d'assurer la portabilité effective des données en vertu du présent règlement complète le droit à la portabilité des données prévu par le règlement (UE) 2016/679. Faciliter le changement de plateforme ou le multihébergement devrait ensuite permettre d'élargir le choix offert aux utilisateurs finaux et encourage les contrôleurs d'accès et les entreprises utilisatrices à innover.

Accès aux données - Portabilité

cf. RGPD

(60) Les entreprises utilisatrices de services de plateforme essentiels fournis par des contrôleurs d'accès et les utilisateurs finaux de ces entreprises utilisatrices fournissent et génèrent de grandes quantités de données. Afin que les entreprises utilisatrices puissent avoir accès aux données pertinentes ainsi générées, le contrôleur d'accès devrait, à leur demande, permettre un accès effectif et gratuit à ces données. Les tiers sous contrat avec l'entreprise utilisatrice, qui agissent en tant que sous-traitants de ces données pour cette entreprise, devraient également bénéficier d'un tel accès. Cet accès devrait inclure l'accès aux données fournies ou générées par les mêmes entreprises utilisatrices et les mêmes utilisateurs finaux de ces entreprises dans le cadre d'autres services fournis par le même contrôleur d'accès, y compris les services fournis conjointement aux services de plateforme essentiels ou à l'appui de ceux-ci lorsque cela est inextricablement lié à la demande concernée. À cette fin, un contrôleur d'accès ne devrait pas recourir à des restrictions contractuelles ou autres dans le but d'empêcher les entreprises utilisatrices d'accéder aux données pertinentes, et devrait permettre à ces entreprises utilisatrices d'obtenir le consentement de leurs utilisateurs finaux pour l'accès à ces données et leur extraction, lorsque ce consentement est requis en vertu du règlement (UE) 2016/679 et de la directive 2002/58/CE. Les contrôleurs d'accès devraient en outre garantir l'accès continu et en temps réel à de telles données au moyen de mesures techniques appropriées, par exemple en mettant en place des interfaces de programmation de haute qualité ou des outils intégrés pour les entreprises utilisatrices de petit volume.

cf. RGPD

(61) Les moteurs de recherche en ligne gagnent en valeur pour leurs entreprises utilisatrices et leurs utilisateurs finaux respectifs à mesure que le nombre total de ces utilisateurs augmente. Les entreprises fournissant des moteurs de recherche en ligne collectent et conservent des ensembles de données agrégées contenant des informations sur les recherches effectuées par les utilisateurs, et la manière dont ces derniers ont interagi avec les résultats qu'ils ont obtenus. Les entreprises fournissant des

Données des moteurs de recherche

moteurs de recherche en ligne collectent ces données à partir de recherches effectuées sur leur propre moteur de recherche en ligne et, le cas échéant, de recherches effectuées sur les plateformes de leurs partenaires commerciaux en aval. L'accès des contrôleurs d'accès à ces données concernant les classements, les requêtes, les clics et les vues constitue une barrière importante à l'entrée et à l'expansion, ce qui nuit à la contestabilité des moteurs de recherche en ligne. Les contrôleurs d'accès devraient donc être tenus de fournir aux autres entreprises fournissant de tels services, à des conditions équitables, raisonnables et non discriminatoires, un accès à ces données concernant les classements, les requêtes, les clics et les vues en lien avec les recherches gratuites et payantes générées par les consommateurs des moteurs de recherche en ligne, de manière à ce que ces entreprises tierces puissent optimiser leurs services et contester les services de plateforme essentiels concernés. Les tiers sous contrat avec le fournisseur d'un moteur de recherche en ligne, qui agissent en tant que sous-traitants de ces données pour ce moteur de recherche en ligne, devraient également bénéficier d'un tel accès. Lorsqu'il fournit un accès à ses données de recherche, un contrôleur d'accès devrait garantir la protection des données à caractère personnel des utilisateurs finaux, notamment contre les risques de réidentification, par des moyens adéquats, par exemple l'anonymisation des données à caractère personnel, sans altérer considérablement la qualité ou l'utilité des données. Les données concernées sont anonymisées si les données à caractères personnel sont irréversiblement modifiées de façon à ce que les informations ne soient plus liées à une personne physique identifiée ou identifiable, ou si les données à caractère personnel sont rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable.

Boutiques d'applications logicielles

(62) En ce qui concerne les boutiques d'applications logicielles, moteurs de recherche en ligne et services de réseaux sociaux en ligne énumérés dans la décision de désignation, les contrôleurs d'accès devraient publier et appliquer des conditions générales d'accès équitables, raisonnables et non discriminatoires. Ces conditions générales devraient prévoir un mécanisme de règlement extrajudiciaire des litiges au niveau de l'Union qui soit facilement accessible, impartial, indépendant et gratuit pour l'entreprise utilisatrice, sans préjudice de ses propres coûts et des mesures proportionnées visant à empêcher une utilisation abusive du mécanisme de règlement des litiges par les entreprises utilisatrices. Ce mécanisme de règlement des litiges devrait être sans préjudice du droit des entreprises utilisatrices de demander réparation devant les autorités judiciaires conformément au droit de l'Union et au droit national. En particulier, les contrôleurs d'accès qui fournissent un accès aux boutiques d'applications logicielles sont des points d'accès majeurs pour les entreprises utilisatrices qui cherchent à atteindre leurs utilisateurs finaux. Compte tenu du déséquilibre du pouvoir de négociation entre ces contrôleurs d'accès et les entreprises utilisatrices de leurs boutiques d'applications logicielles, ces contrôleurs d'accès ne devraient pas être autorisés à imposer des conditions générales, y compris en matière de tarification, qui seraient déloyales ou conduiraient à une différenciation injustifiée.

Les conditions tarifaires ou les autres conditions générales d'accès devraient être considérées comme déloyales si elles conduisent à un déséquilibre entre les droits et les obligations des entreprises utilisatrices, si elles confèrent au contrôleur d'accès un avantage qui est disproportionné par rapport au service qu'il fournit aux entreprises utilisatrices, ou si elles entraînent un désavantage pour les entreprises utilisatrices dans la fourniture de services identiques ou similaires à ceux du contrôleur d'accès. Les critères suivants peuvent servir à évaluer l'équité des conditions générales d'accès: les prix facturés ou les conditions imposées pour des services identiques ou similaires par d'autres fournisseurs de boutiques d'applications logicielles; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour des services différents, liés ou similaires, ou à différents types d'utilisateurs finaux; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour le même service dans différentes régions géographiques; les prix facturés ou les conditions imposées par le fournisseur de la boutique d'applications logicielles pour le même service que celui que le contrôleur d'accès se fournit à lui-même. Cette obligation ne devrait pas établir un droit d'accès et devrait être sans préjudice de la capacité des fournisseurs de boutiques d'applications logicielles, de moteurs de recherche en ligne et de services de réseaux sociaux en ligne d'assumer la responsabilité requise dans la lutte contre les contenus illicites et non désirés, comme le prévoit le règlement relatif au marché intérieur des services numériques.

(63) Les contrôleurs d'accès peuvent entraver la capacité des entreprises utilisatrices et des utilisateurs finaux de se désabonner d'un service de plateforme essentiel auquel ils s'étaient précédemment abonnés. Par conséquent, il convient d'établir des règles afin d'éviter une situation dans laquelle les contrôleurs d'accès portent atteinte au droit des entreprises utilisatrices et des utilisateurs finaux de choisir librement le service de plateforme essentiel qu'ils utilisent. Afin de préserver la liberté de choix des entreprises utilisatrices et des utilisateurs finaux, un contrôleur d'accès ne devrait pas être autorisé à rendre inutilement difficile ou compliqué, pour les entreprises utilisatrices ou les utilisateurs finaux, le désabonnement d'un service de plateforme essentiel. Il convient de ne pas rendre la clôture d'un compte ou le désabonnement d'un service plus compliqués que l'ouverture de ce compte ou l'abonnement à ce service. Les contrôleurs d'accès ne devraient pas exiger de frais supplémentaires lorsqu'ils résilient les contrats conclus avec leurs utilisateurs finaux ou entreprises utilisatrices. Les contrôleurs d'accès devraient veiller à ce que les conditions de résiliation des contrats soient toujours proportionnées et à ce que les utilisateurs finaux puissent les faire jouer sans difficultés excessives, par exemple en ce qui concerne les motifs de la résiliation, le délai de préavis ou la forme de la résiliation. Cela est sans préjudice de la législation nationale applicable conformément au droit de l'Union établissant des droits et obligations concernant les conditions de résiliation de la fourniture de services de plateforme essentiels par les utilisateurs finaux.

(64) Le manque d'interopérabilité permet aux contrôleurs d'accès qui fournissent des services de communications interpersonnelles non fondés sur la numérotation de bénéficier d'effets de réseau importants, ce qui contribue à affaiblir la contestabilité. En outre, indépendamment de la question de savoir si les utilisateurs finaux optent ou non pour un « multihébergement », les contrôleurs d'accès fournissent souvent des services de communications interpersonnelles non fondés sur la numérotation dans le cadre de leur écosystème de plateforme, et cela exacerbe encore les barrières à l'entrée pour les autres fournisseurs de tels services et augmente les coûts de changement de fournisseur pour les utilisateurs finaux. Sans préjudice de la directive (UE) 2018/1972 du Parlement européen et du Conseil[14] et, en particulier, des conditions et procédures prévues à son article 61, les contrôleurs d'accès devraient donc assurer, gratuitement et sur demande, l'interopérabilité avec certaines fonctionnalités de base de leurs services de communications interpersonnelles non fondés sur la numérotation qu'ils fournissent à leurs propres utilisateurs finaux, pour les tiers fournisseurs de tels services.

Les contrôleurs d'accès devraient assurer l'interopérabilité pour les tiers fournisseurs de services de communications interpersonnelles non fondés sur la numérotation qui proposent ou entendent proposer ces services aux utilisateurs finaux et entreprises utilisatrices dans l'Union. Afin de faciliter la mise en œuvre pratique de cette interopérabilité, le contrôleur d'accès concerné devrait être tenu de publier une offre de référence énonçant les détails techniques et les conditions générales d'interopérabilité avec ses services de communications interpersonnelles non fondés sur la numérotation. La Commission devrait avoir la possibilité, le cas échéant, de consulter l'Organe des régulateurs européens des communications électroniques, afin de déterminer si les détails techniques et les conditions générales publiés dans l'offre de référence et que le contrôleur d'accès entend mettre en œuvre ou a mis en œuvre permettent de se conformer avec cette obligation.

Dans tous les cas, le contrôleur d'accès et le fournisseur demandeur devraient veiller à ce que l'interopérabilité ne compromette pas un niveau élevé de sécurité et de protection des données, conformément aux obligations qui leur incombent en vertu du présent règlement et du droit applicable de l'Union, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. L'obligation relative à l'interopérabilité devrait être sans préjudice des informations et des choix à mettre à la disposition des utilisateurs finaux des services de communications interpersonnelles non fondés sur la numérotation du contrôleur d'accès et du fournisseur demandeur en vertu du présent règlement et d'autres dispositions du droit de l'Union, en particulier du règlement (UE) 2016/679.

cf. RGPD

cf. RGPD

(65) Pour garantir que les obligations prévues par le présent règlement soient effectives, tout en veillant à ce qu'elles se limitent à ce qui est nécessaire pour assurer la

14. Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

contestabilité et contrer les effets néfastes des pratiques déloyales des contrôleurs d'accès, il est important de les définir et circonscrire clairement, de manière à permettre au contrôleur d'accès de s'y conformer en tous points, tout en respectant pleinement le droit applicable, et en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE ainsi que la législation sur la protection des consommateurs, la cybersécurité, la sécurité des produits et les exigences en matière d'accessibilité, y compris la directive (UE) 2019/882 et la directive (UE) 2016/2102 du Parlement européen et du Conseil[15]. Les contrôleurs d'accès devraient garantir le respect du présent règlement dès la conception. Dès lors, les mesures nécessaires devraient être intégrées autant que possible dans la conception technologique utilisée par les contrôleurs d'accès.

cf. RGPD

Il peut, dans certains cas, être approprié pour la Commission, après avoir dialogué avec le contrôleur d'accès concerné, et après avoir permis aux tiers de présenter des observations, de préciser davantage certaines des mesures que le contrôleur d'accès devrait adopter afin de se conformer effectivement aux obligations susceptibles d'être précisées davantage ou, en cas de contournement, à toutes les obligations. En particulier, il devrait être possible d'apporter de telles précisions complémentaires lorsque la mise en œuvre d'une obligation susceptible d'être précisée peut être affectée par des variations de services au sein d'une seule catégorie de services de plateforme essentiels. À cet effet, le contrôleur d'accès devrait pouvoir demander à la Commission d'engager un processus dans le cadre duquel elle peut préciser davantage certaines des mesures que le contrôleur d'accès devrait adopter afin de se conformer effectivement à ces obligations.

La Commission devrait disposer d'un pouvoir d'appréciation quant à la question de savoir s'il y a lieu d'apporter des précisions complémentaires, et à quel moment, dans le respect de l'égalité de traitement, de la proportionnalité et du principe de bonne administration. À cet égard, la Commission devrait fournir les principales raisons qui sous- tendent son évaluation, y compris toute priorité pour le contrôle du respect de la législation. Ce processus ne devrait pas être utilisé pour nuire à l'efficacité du présent règlement. En outre, il est sans préjudice du pouvoir de la Commission d'adopter une décision constatant le non-respect, par un contrôleur d'accès, d'une des obligations énoncées dans le présent règlement, y compris de la possibilité d'infliger des amendes ou des astreintes. La Commission devrait pouvoir rouvrir une procédure, y compris lorsque les mesures précisées se révèlent inefficaces. Une réouverture due à l'inefficacité des précisions adoptées par voie de décision devrait permettre à la Commission de modifier ces précisions de manière prospective. La Commission devrait également être en mesure de fixer un délai raisonnable dans lequel la procédure peut être rouverte si les mesures précisées s'avèrent inefficaces.

(66) Également pour garantir la proportionnalité, un contrôleur d'accès devrait avoir la possibilité de demander la suspension, dans la mesure nécessaire, d'une obligation spécifique dans des circonstances exceptionnelles échappant à son contrôle, telles qu'un choc externe imprévu le privant temporairement d'une part considérable de la demande des utilisateurs finaux pour le service de plateforme essentiel concerné, s'il démontre que le respect de cette obligation particulière peut menacer la viabilité économique de ses activités dans l'Union. La Commission devrait déterminer les circonstances exceptionnelles justifiant la suspension et réexaminer celle-ci régulièrement pour évaluer si les conditions de son octroi sont toujours viables.

(67) Dans des circonstances exceptionnelles, uniquement justifiées par des raisons de santé ou de sécurité publiques définies par le droit de l'Union et interprétées par la Cour de justice, la Commission devrait être en mesure de décider qu'une obligation donnée ne s'applique pas à un service de plateforme essentiel spécifique. Si une atteinte est portée à ces intérêts publics, cela pourrait indiquer que la mise en œuvre d'une obligation spécifique est, dans un cas exceptionnel précis, trop coûteuse pour la société dans son ensemble, et donc disproportionnée. Lorsqu'il y a lieu, la Commission devrait être en mesure de faciliter le respect en évaluant si une suspension ou exemption limitée et dûment motivée est justifiée. Cela devrait garantir la proportionnalité des obligations énoncées dans le présent règlement sans compromettre les effets

15. Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

ex ante escomptés sur l'équité et la contestabilité. Lorsqu'une exemption est accordée, la Commission devrait revoir sa décision tous les ans.

(68) Dans le délai imparti pour respecter leurs obligations au titre du présent règlement, les contrôleurs d'accès devraient informer la Commission, par des rapports obligatoires, des mesures qu'ils comptent mettre en œuvre ou ont mis en œuvre afin d'assurer le respect effectif de ces obligations, y compris les mesures concernant le respect du règlement (UE) 2016/679, dans la mesure où elles sont pertinentes pour le respect des obligations prévues par le présent règlement, et qui devraient permettre à la Commission de s'acquitter de ses missions en vertu du présent règlement. En outre, il convient de rendre publique une synthèse non confidentielle claire et compréhensible de ces informations, tout en tenant compte de l'intérêt légitime des contrôleurs d'accès à la protection de leurs secrets d'affaires et autres informations confidentielles. Cette publication non confidentielle devrait permettre aux tiers d'évaluer si les contrôleurs d'accès respectent les obligations énoncées dans le présent règlement. Ces rapports devraient être sans préjudice de toute mesure d'exécution prise par la Commission à quelque moment que ce soit après ces rapports. La Commission devrait publier en ligne un lien vers la synthèse non confidentielle du rapport, ainsi que toutes les autres informations publiques à communiquer en application des obligations d'information prévues par le présent règlement, afin de garantir l'accessibilité desdites informations sous une forme utilisable et exhaustive, en particulier pour les petites et moyennes entreprises (PME).

RGPD

(69) Les obligations des contrôleurs d'accès ne devraient être actualisées qu'à la suite d'une enquête rigoureuse portant sur la nature et l'incidence de pratiques spécifiques qui pourraient être à leur tour désignées, après une enquête approfondie, comme étant déloyales ou limitant la contestabilité de la même manière que les pratiques déloyales décrites dans le présent règlement, tout en étant potentiellement exclues du champ d'application de l'ensemble actuel d'obligations. La Commission devrait pouvoir, soit de sa propre initiative, soit à la suite d'une demande motivée d'au moins trois États membres, ouvrir une enquête en vue de déterminer si les obligations existantes doivent être actualisées. Lorsqu'ils présentent ces demandes motivées, les États membres devraient avoir la possibilité d'inclure des informations sur les offres nouvelles de produits, de services, de logiciels ou de caractéristiques qui suscitent des préoccupations du point de vue de la contestabilité ou de l'équité, qu'elles soient mises en œuvre dans le cadre de services de plateforme essentiels existants ou non. Lorsque, à la suite d'une enquête de marché, la Commission juge nécessaire de modifier des éléments essentiels du présent règlement, par exemple en incluant de nouvelles obligations qui s'écartent des mêmes questions de contestabilité ou d'équité que celles régies par le présent règlement, la Commission devrait présenter une proposition de modification du présent règlement.

(70) Compte tenu du pouvoir économique considérable des contrôleurs d'accès, il est important que les obligations soient appliquées de manière effective et qu'elles ne soient pas contournées. À cette fin, les règles en question devraient s'appliquer à toute pratique d'un contrôleur d'accès, quelle que soit sa forme et indépendamment de sa nature contractuelle, commerciale, technique ou autre, dans la mesure où cette pratique correspond au type de pratique visé par l'une des obligations prévues par le présent règlement. Les contrôleurs d'accès ne devraient pas adopter un comportement susceptible de compromettre le caractère effectif des interdictions et obligations prévues par le présent règlement. Un tel comportement peut être la conception utilisée par le contrôleur d'accès, la présentation des choix de l'utilisateur final d'une façon qui n'est pas neutre ou l'utilisation de la structure, du fonctionnement ou du mode opératoire d'une interface utilisateur ou d'une partie de celle-ci pour réduire ou compromettre l'autonomie, la capacité décisionnelle ou le choix de l'utilisateur. En outre, le contrôleur d'accès ne devrait pas être autorisé à adopter un comportement compromettant l'interopérabilité exigée par le présent règlement, par exemple en recourant à des mesures techniques de protection injustifiées, à des conditions de service discriminatoires, en revendiquant illégalement un droit d'auteur sur des interfaces de programmation ou en fournissant des informations dénaturées. Les contrôleurs d'accès ne devraient pas être autorisés à contourner leur désignation en segmentant, divisant, subdivisant, fragmentant ou fractionnant artificiellement leurs services de plateforme essentiels dans le but de contourner les seuils quantitatifs fixés par le présent règlement.

(71) Afin de garantir l'efficacité du réexamen du statut de contrôleur d'accès ainsi que la possibilité d'adapter la liste des services de plateforme essentiels fournis par un contrôleur d'accès, il convient que les contrôleurs d'accès informent la Commission de toutes les acquisitions prévues, avant leur mise en œuvre, d'autres entreprises fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou d'autres services qui permettent la collecte de données. De telles informations devraient non seulement servir au processus de réexamen en ce qui concerne le statut des contrôleurs d'accès individuels, mais aussi fournir des renseignements cruciaux pour le suivi des tendances plus générales en matière de contestabilité dans le secteur numérique; elles peuvent par conséquent être utilement prises en considération lors des enquêtes de marché prévues par le présent règlement. En outre, la Commission devrait communiquer ces informations aux États membres, étant donné qu'elles peuvent être utilisées à des fins de contrôle des concentrations au niveau national et que, dans certaines circonstances, l'autorité nationale compétente a la possibilité de soumettre ces acquisitions à la Commission aux fins du contrôle des concentrations. La Commission devrait également publier chaque année une liste des acquisitions signalées par le contrôleur d'accès. Afin de garantir la nécessaire transparence de ces informations ainsi que leur utilité pour les différentes fins prévues par le présent règlement, les contrôleurs d'accès devraient fournir au moins les renseignements relatifs aux entreprises concernées par la concentration, leur chiffre d'affaires annuel dans l'Union et au niveau mondial, leur domaine d'activité, y compris les activités directement liées à la concentration, la valeur transactionnelle ou une estimation de celle-ci, un résumé relatif à la concentration, y compris sa nature et sa justification, ainsi qu'une liste des États membres concernés par l'opération.

(72) Les intérêts des utilisateurs finaux en matière de protection des données et de la vie privée sont à prendre en considération pour toute appréciation des effets néfastes potentiels des pratiques des contrôleurs d'accès observées en ce qui concerne la collecte et l'accumulation de grandes quantités de données auprès des utilisateurs finaux. Assurer un niveau adéquat de transparence en ce qui concerne les pratiques de profilage utilisées par les contrôleurs d'accès, notamment mais pas uniquement le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679, permet de faciliter la contestabilité des services de plateforme essentiels. La transparence exerce une pression extérieure sur les contrôleurs d'accès pour ne pas faire du profilage approfondi du consommateur la norme dans le secteur, étant donné que les entrants potentiels ou les jeunes entreprises ne peuvent pas accéder à des données aussi étendues et profondes, et à une échelle similaire. Une plus grande transparence devrait permettre aux autres entreprises fournissant des services de plateforme essentiels de se démarquer davantage grâce à l'utilisation de garanties de protection de la vie privée plus performantes.

Protection des données et vie privée

cf. RGPD

Afin d'assurer une efficacité minimale à cette obligation de transparence, les contrôleurs d'accès devraient fournir, au moins, une description, faisant l'objet d'un audit indépendant, de la base sur laquelle le profilage est effectué, en précisant si les données à caractère personnel et les données issues de l'activité de l'utilisateur, au sens du règlement (UE) 2016/679, sont utilisées, le traitement appliqué, les finalités pour lesquelles le profil est conçu et finalement utilisé, la durée du profilage, son incidence sur les services du contrôleur d'accès et les mesures prises pour permettre effectivement aux utilisateurs finaux d'avoir connaissance de l'utilisation voulue de ce profilage, de même que les mesures prises pour obtenir leur consentement ou leur donner la possibilité de le refuser ou de le retirer. La Commission devrait transférer la description faisant l'objet d'un audit au comité européen de la protection des données afin d'éclairer l'application des règles de l'Union en matière de protection des données. La Commission devrait être habilitée à mettre au point la méthodologie et la procédure pour la description devant faire l'objet d'un audit, en concertation avec le Contrôleur européen de la protection des données, le comité européen de la protection des données, la société civile et des experts, conformément aux règlements (UE) no 182/2011[16] et (UE) 2018/1725[17] du Parlement européen et du Conseil.

cf. RGPD

16. Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).
17. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

Rôle de la Commission

(73) Afin de garantir la réalisation pleine et durable des objectifs du présent règlement, la Commission devrait être en mesure d'apprécier si une entreprise fournissant des services de plateforme essentiels doit être désignée comme contrôleur d'accès sans qu'elle atteigne les seuils quantitatifs fixés dans le présent règlement; si le non-respect systématique par un contrôleur d'accès justifie l'imposition de mesures correctives supplémentaires; s'il convient d'ajouter davantage de services relevant du secteur numérique à la liste des services de plateforme essentiels; et si d'autres pratiques tout aussi déloyales et limitant également la contestabilité des marchés numériques doivent faire l'objet d'enquêtes. Cette appréciation devrait reposer sur des enquêtes de marché à conduire en temps opportun, moyennant des procédures et des délais clairs, afin de renforcer les effets ex ante du présent règlement sur la contestabilité et l'équité dans le secteur numérique, et de fournir le degré requis de sécurité juridique.

(74) La Commission devrait être en mesure de constater, à la suite d'une enquête de marché, qu'une entreprise fournissant un service de plateforme essentiel remplit tous les critères qualitatifs globaux pour être désignée comme contrôleur d'accès. De ce fait, cette entreprise devrait, en principe, se conformer à toutes les obligations pertinentes prévues par le présent règlement. Toutefois, pour les contrôleurs d'accès qui ont été désignés par la Commission parce qu'il est prévisible qu'ils jouiront d'une position solide et durable dans un avenir proche, la Commission ne devrait imposer que les obligations nécessaires et appropriées pour les empêcher d'acquérir une position solide et durable dans leurs activités. En ce qui concerne ces contrôleurs d'accès émergents, la Commission devrait tenir compte de la nature en principe temporaire de ce statut et il faudra donc décider, en temps voulu, si une telle entreprise fournissant des services de plateforme essentiels devrait être soumise à l'ensemble des obligations imposées aux contrôleurs d'accès parce qu'elle a acquis une position solide et durable, ou si les conditions de désignation ne sont finalement pas satisfaites et si, par conséquent, toutes les obligations précédemment imposées devraient être levées.

(75) La Commission devrait examiner et apprécier si des mesures correctives comportementales ou, le cas échéant, structurelles sont justifiées afin de veiller à ce que le contrôleur d'accès ne puisse contrarier les objectifs du présent règlement par le non-respect systématique d'au moins une des obligations qui y sont définies. Tel est le cas si la Commission a émis à l'encontre d'un contrôleur d'accès, sur une période de huit ans, au moins trois décisions constatant un non-respect, qui peuvent concerner des services de plateforme essentiels différents et différentes obligations prévues par le présent règlement, et si le contrôleur d'accès a maintenu, étendu ou encore renforcé son impact au sein du marché intérieur, la dépendance économique de ses entreprises utilisatrices et utilisateurs finaux vis-à-vis de ses services de plateforme essentiels ou la solidité de sa position. Un contrôleur d'accès devrait être réputé avoir maintenu, étendu ou renforcé sa position lorsque, malgré les mesures d'exécution prises par la Commission, il conserve ou a encore consolidé ou accru son importance en tant que point d'accès permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux.

La Commission devrait dans ces cas de figure avoir le pouvoir d'imposer toute mesure corrective, qu'elle soit comportementale ou structurelle, dans le respect du principe de proportionnalité. Dans ce contexte, la Commission devrait avoir le pouvoir d'interdire au contrôleur d'accès, dans la mesure où cette mesure corrective est proportionnée et nécessaire pour préserver ou rétablir l'équité et la contestabilité affectées par le non-respect systématique, pendant une période limitée, de procéder à une concentration concernant ces services de plateforme essentiels, les autres services fournis dans le secteur numérique ou les services permettant la collecte de données concernées par le non-respect systématique. Afin de permettre la participation effective de tiers et de donner la possibilité de tester les mesures correctives avant de les appliquer, la Commission devrait publier une synthèse non confidentielle détaillée de la situation et des mesures à prendre. La Commission devrait être en mesure de rouvrir une procédure, y compris lorsque les mesures précisées se révèlent inefficaces. Une réouverture due à l'inefficacité de mesures correctives adoptées par voie de décision devrait permettre à la Commission de modifier les mesures correctives de manière prospective. La Commission devrait également être en mesure de fixer un délai raisonnable dans lequel il devrait être possible de rouvrir la procédure si les mesures correctives se révèlent inefficaces.

(76) Lorsque, au cours d'une enquête portant sur un non-respect systématique, un contrôleur d'accès propose à la Commission de prendre des engagements, cette dernière devrait être en mesure d'adopter une décision rendant ces engagements obliga-

toires pour le contrôleur d'accès concerné, si elle estime que ces engagements garantissent le respect effectif des obligations énoncées dans le présent règlement. Cette décision devrait également constater qu'il n'y a plus lieu pour la Commission d'agir en ce qui concerne le non-respect systématique faisant l'objet de l'enquête. Lorsqu'elle évalue si les engagements que le contrôleur d'accès propose de prendre sont suffisants pour assurer le respect effectif des obligations prévues par le présent règlement, la Commission devrait être autorisée à tenir compte des tests effectués par le contrôleur d'accès pour démontrer l'efficacité pratique des engagements proposés. La Commission devrait vérifier que la décision relative aux engagements est pleinement respectée et atteint ses objectifs, et elle devrait être habilitée à rouvrir la décision si elle estime que les engagements ne sont pas efficaces.

Révision du Règlement

(77) Les services du secteur numérique et les types de pratiques liées à ces services peuvent évoluer rapidement et de façon considérable. Afin de veiller à ce que le présent règlement reste à jour et constitue une réponse réglementaire efficace et globale aux problèmes que posent les contrôleurs d'accès, il est important de prévoir un réexamen régulier des listes des services de plateforme essentiels, ainsi que des obligations prévues par le présent règlement. Cela est particulièrement important pour garantir qu'une pratique qui est susceptible de limiter la contestabilité des services de plateforme essentiels ou qui est déloyale soit mise en évidence. Bien qu'il importe de procéder régulièrement à des réexamens, compte tenu de l'évolution dynamique du secteur numérique, tout réexamen devrait être effectué dans un délai raisonnable et adéquat afin de procurer une sécurité juridique en ce qui concerne les conditions réglementaires. Les enquêtes de marché devraient également permettre à la Commission de disposer d'une base factuelle solide lui permettant d'apprécier si elle doit proposer de modifier le présent règlement de manière à réexaminer, élargir, ou détailler davantage les listes des services de plateforme essentiels. Elles devraient en outre permettre à la Commission de disposer d'une base factuelle solide lui permettant d'apprécier si elle doit proposer une modification des obligations prévues par le présent règlement, ou si elle doit adopter un acte délégué pour mettre à jour ces obligations.

(78) En ce qui concerne les procédés des contrôleurs d'accès qui ne relèvent pas des obligations énoncées dans le présent règlement, la Commission devrait avoir la possibilité d'ouvrir une enquête de marché sur de nouveaux services et de nouvelles pratiques afin de déterminer si les obligations énoncées dans le présent règlement doivent être complétées par un acte délégué relevant du champ d'application de l'habilitation établie pour de tels actes délégués dans le présent règlement, ou en présentant une proposition visant à modifier le présent règlement. Cette disposition est sans préjudice de la possibilité pour la Commission, dans les cas appropriés, d'intenter une procédure au titre de l'article 101 ou 102 du traité sur le fonctionnement de l'Union européenne. Ces procédures devraient être conduites conformément au règlement (CE) no 1/2003 du Conseil[18]. Dans les cas d'urgence justifiés par le fait qu'un préjudice grave et irréparable risque d'être causé à la concurrence, la Commission devrait envisager d'adopter des mesures provisoires conformément à l'article 8 du règlement (CE) no 1/2003.

Contrôle et sanction

(79) Si les contrôleurs d'accès se livrent à une pratique déloyale ou qui limite la contestabilité des services de plateforme essentiels déjà désignés en application du présent règlement, mais que cette pratique n'est pas explicitement couverte par les obligations prévues par le présent règlement, la Commission devrait être en mesure de mettre à jour le présent règlement au moyen d'actes délégués. Ces mises à jour par voie d'actes délégués devraient être soumises à la même norme en matière d'enquête et devraient donc être précédées d'une enquête de marché. La Commission devrait également appliquer une norme prédéfinie pour identifier ce type de pratiques. Cette norme juridique devrait donc garantir que le type d'obligations qui pourraient être imposées à tout moment aux contrôleurs d'accès en vertu du présent règlement est suffisamment prévisible.

(80) Afin d'assurer la mise en œuvre et le respect effectifs du présent règlement, la Commission devrait disposer de pouvoirs d'enquête et de coercition étendus pour lui permettre d'enquêter, de faire respecter et de contrôler les règles énoncées dans le présent règlement, tout en veillant au respect du droit fondamental d'être entendu et d'accéder au dossier dans le cadre des procédures d'exécution. La Commission devrait

18. Règlement (CE) no 1/2003 du Conseil du 16 décembre 2002 relatif à la mise en œuvre des règles de concurrence prévues aux articles 81 et 82 du traité (JO L 1 du 4.1.2003, p. 1).

en outre disposer de ces pouvoirs d'enquête pour mener des enquêtes de marché, y compris aux fins de la mise à jour et du réexamen du présent règlement.

(81) La Commission devrait disposer dans toute l'Union du pouvoir de demander les renseignements nécessaires aux fins du présent règlement. La Commission devrait, en particulier, avoir accès à tous les documents, données, bases de données, algorithmes et informations pertinents nécessaires à l'ouverture et à la conduite d'enquêtes ainsi qu'au contrôle du respect des obligations énoncées dans le présent règlement, quel que soit le détenteur de ces informations, et indépendamment de leur forme, format, support de stockage ou lieu de conservation.

(82) La Commission devrait pouvoir demander directement aux entreprises ou associations d'entreprises de fournir toutes preuves, données et informations pertinentes. De plus, la Commission devrait être en mesure de demander tout renseignement pertinent aux autorités compétentes d'un État membre, ou à toute personne physique ou morale aux fins du présent règlement. Lorsqu'elles se conforment à la décision de la Commission, les entreprises sont tenues de répondre à des questions portant sur les faits et de fournir des documents.

(83) La Commission devrait également être habilitée à procéder à l'inspection de toute entreprise ou association d'entreprises, à auditionner toute personne susceptible de disposer d'informations utiles et à enregistrer ses déclarations.

(84) Les mesures provisoires peuvent constituer un instrument important pour garantir que l'infraction faisant l'objet d'une enquête en cours n'entraîne pas de préjudice grave et irréparable aux entreprises utilisatrices ou aux utilisateurs finaux des contrôleurs d'accès. Cet instrument joue un rôle important pour éviter une évolution qu'il serait très difficile d'inverser par une décision prise par la Commission à la fin de la procédure. La Commission devrait par conséquent avoir le pouvoir d'ordonner des mesures provisoires dans le cadre d'une procédure engagée en vue de l'adoption éventuelle d'une décision constatant un non-respect. Ce pouvoir devrait s'appliquer dans les cas où la Commission a constaté à première vue l'existence d'une infraction aux obligations qui incombent aux contrôleurs d'accès et où il existe un risque de préjudice grave et irréparable pour les entreprises utilisatrices ou les utilisateurs finaux des contrôleurs d'accès. Des mesures provisoires ne devraient s'appliquer que pour une durée déterminée, soit jusqu'au terme de la procédure engagée par la Commission, soit pour une période déterminée, qui peut être renouvelée dans la mesure où cela est nécessaire et opportun.

(85) La Commission devrait pouvoir prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues par le présent règlement. Au titre de ces mesures, la Commission devrait avoir la capacité de nommer des experts externes indépendants et des auditeurs chargés de l'assister dans ce processus, y compris, le cas échéant, issus des autorités compétentes des États membres, par exemple les autorités chargées de la protection des données ou des consommateurs. Lors de la désignation des auditeurs, la Commission devrait assurer une rotation suffisante.

(86) Le respect des obligations imposées par le présent règlement devrait pouvoir être assuré au moyen d'amendes et d'astreintes. À cette fin, il y a lieu de prévoir également des amendes et des astreintes d'un montant approprié en cas de non-respect des obligations et de violation des règles de procédure, sous réserve des délais de prescription appropriés, conformément aux principes de proportionnalité et ne bis in idem. La Commission et les autorités nationales compétentes devraient coordonner leurs efforts en matière de contrôle de l'application afin de veiller au respect des principes susmentionnés. En particulier, la Commission devrait tenir compte de toutes les amendes et astreintes imposées à la même personne morale pour les mêmes faits par une décision finale dans le cadre d'une procédure relative à une infraction à d'autres règles de l'Union ou nationales, de manière à veiller à ce que l'ensemble des amendes et astreintes imposées correspondent à la gravité des infractions commises.

(87) Afin de garantir le recouvrement effectif d'une amende infligée à une association d'entreprises pour une infraction qu'elle a commise, il est nécessaire de fixer les conditions auxquelles il est possible pour la Commission d'exiger le paiement de l'amende auprès des entreprises membres de cette association d'entreprises lorsque celle-ci n'est pas solvable.

(88) Dans le contexte des procédures menées au titre du présent règlement, il convient de consacrer le droit de l'entreprise intéressée d'être entendue par la Commission, et les décisions prises devraient faire l'objet d'une large publicité. Tout en assurant le droit à une bonne administration, le droit d'accès au dossier et le droit d'être entendu, il est indispensable de protéger les informations confidentielles. De plus, tout en respectant la confidentialité des informations, la Commission devrait garantir que toute information sur laquelle la décision repose est divulguée dans la mesure nécessaire pour que le destinataire de la décision comprenne les faits et les considérations qui ont guidé celle-ci. Il convient en outre de veiller à ce que la Commission n'utilise que des informations recueillies en vertu du présent règlement aux fins du présent règlement, sauf disposition expresse contraire. Enfin, il devrait être possible, dans certaines conditions, de considérer certains documents d'affaires, tels que les communications entre les avocats et leurs clients, comme confidentiels si les conditions applicables sont réunies.

(89) Lorsqu'elle élabore des synthèses non confidentielles à publier afin de permettre effectivement aux tiers intéressés de présenter des observations, la Commission devrait tenir dûment compte de l'intérêt légitime des entreprises à la protection de leurs secrets d'affaires et autres informations confidentielles.

Coordination entre la Commission et les autorités nationales

(90) L'application cohérente, efficace et complémentaire des instruments juridiques disponibles aux contrôleurs d'accès nécessite une coopération et une coordination entre la Commission et les autorités nationales dans le cadre de leurs compétences. La Commission et les autorités nationales devraient coopérer et coordonner leurs actions nécessaires pour l'application des instruments juridiques disponibles aux contrôleurs d'accès au sens du présent règlement et respecter le principe de coopération loyale énoncé à l'article 4 du traité sur l'Union européenne. Le soutien qu'apportent les autorités nationales à la Commission devrait pouvoir comprendre la fourniture à cette dernière de toutes les informations nécessaires en leur possession ou, à la demande de celle-ci et dans l'exercice de ses compétences, d'une assistance qui lui permette de mieux pouvoir accomplir les tâches qui lui sont assignées par le présent règlement.

(91) La Commission est la seule autorité habilitée à faire appliquer le présent règlement. Afin de soutenir la Commission, les États membres devraient avoir la possibilité d'habiliter leurs autorités nationales compétentes chargées de faire appliquer les règles de concurrence à mener des enquêtes sur d'éventuelles cas de non-respect par les contrôleurs d'accès de certaines obligations prévues par le présent règlement. Cette démarche pourrait notamment se justifier lorsqu'il n'est pas possible de déterminer d'emblée si le comportement d'un contrôleur d'accès est de nature à constituer une infraction au présent règlement, aux règles de concurrence que l'autorité nationale compétente est habilitée à faire appliquer, ou aux deux. L'autorité nationale compétente chargée de faire appliquer les règles de concurrence devrait communiquer à la Commission un rapport sur ses constatations concernant d'éventuels cas de non-respect par les contrôleurs d'accès de certaines obligations prévues par le présent règlement, afin que celle-ci ouvre des procédures d'enquête sur tout cas de non-respect en tant que seule instance habilitée à faire appliquer les dispositions du présent règlement.

La Commission devrait avoir toute latitude pour décider d'ouvrir de telles procédures. Afin d'éviter un chevauchement des enquêtes menées au titre du présent règlement, l'autorité nationale compétente concernée devrait informer la Commission avant de prendre sa première mesure d'enquête sur un éventuel cas de non-respect par les contrôleurs d'accès de certaines obligations prévues par le présent règlement. Les autorités nationales compétentes devraient également agir en étroite coopération et coordination avec la Commission lorsqu'elles font appliquer les règles nationales de concurrence à l'encontre des contrôleurs d'accès, y compris en ce qui concerne la fixation d'amendes. À cette fin, elles devraient informer la Commission lorsqu'elles engagent une procédure fondée sur des règles nationales de concurrence à l'encontre des contrôleurs d'accès, ainsi qu'avant d'imposer des obligations aux contrôleurs d'accès dans le cadre d'une telle procédure. Afin d'éviter les doubles emplois, le fait d'informer du projet de décision conformément à l'article 11 du règlement (CE) no 1/2003 devrait pouvoir, le cas échéant, servir de notification au titre du présent règlement.

(92) Afin de garantir que le présent règlement est appliqué et exécuté de façon harmonisée, il importe de veiller à ce que les autorités nationales, y compris les juridictions nationales, disposent de toutes les informations nécessaires pour s'assurer que leurs décisions ne soient pas contraires à une décision adoptée par la Commission en vertu du présent règlement. Les juridictions nationales devraient être autorisées à demander à la Commission de leur transmettre des informations ou des avis sur des questions concernant l'application du présent règlement. Dans le même temps, la Commission devrait pouvoir présenter des observations orales ou écrites aux juridictions nationales. Cette disposition est sans préjudice de la possibilité qu'ont les juridictions nationales d'introduire une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.

(93) Afin d'assurer la cohérence et une complémentarité effective dans la mise en œuvre du présent règlement et d'autres réglementations sectorielles applicables aux contrôleurs d'accès, la Commission devrait bénéficier de l'expertise d'un groupe de haut niveau spécialisé. Ce groupe de haut niveau devrait également avoir la possibilité d'assister la Commission par le biais d'avis, d'expertise et de recommandations, le cas échéant, concernant des questions générales liées à la mise en œuvre ou à l'application du présent règlement. Le groupe de haut niveau devrait se composer des organes et réseaux européens concernés, et sa composition devrait garantir un niveau élevé d'expertise et un équilibre géographique. Les membres du groupe de haut niveau devraient régulièrement faire rapport aux organes et réseaux qu'ils représentent sur les tâches effectuées dans le cadre du groupe, et les consulter à cet égard.

(94) Étant donné que les décisions prises par la Commission en application du présent règlement sont soumises au contrôle de la Cour de justice conformément au traité sur le fonctionnement de l'Union européenne, celle-ci devrait, conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, disposer d'une compétence de pleine juridiction en ce qui concerne les amendes et les astreintes.

(95) La Commission devrait avoir la possibilité d'élaborer des lignes directrices pour fournir des orientations supplémentaires sur différents aspects du présent règlement ou pour aider les entreprises fournissant des services de plateforme essentiels à mettre en œuvre les obligations découlant du présent règlement. Ces orientations devraient pouvoir se fonder en particulier sur l'expérience acquise par la Commission dans le cadre du contrôle du respect du présent règlement. La publication de toute ligne directrice au titre du présent règlement est une prérogative et relève de la seule discrétion de la Commission et ne devrait pas être considérée comme un élément constitutif aux fins de veiller à ce que les entreprises ou associations d'entreprises concernées respectent les obligations qui leur incombent en vertu du présent règlement.

(96) La mise en œuvre de certaines des obligations des contrôleurs d'accès, telles que celles liées à l'accès aux données, à leur portabilité ou à leur interopérabilité pourrait être facilitée par l'utilisation de normes techniques. À cet égard, la Commission devrait avoir la possibilité, lorsque cela est approprié et nécessaire, de demander aux organisations européennes de normalisation d'en élaborer.

Actes délégués

(97) Afin d'assurer la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès opèrent, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne afin de modifier la méthode qui figure dans une annexe du présent règlement et qui est utilisée pour déterminer si les seuils quantitatifs concernant les utilisateurs finaux actifs et les entreprises utilisatrices actives applicables à la désignation des contrôleurs d'accès sont atteints, afin de préciser davantage les éléments supplémentaires de la méthode qui ne figurent pas dans ladite annexe et qui permettent de déterminer si les seuils quantitatifs applicables à la désignation des contrôleurs d'accès sont atteints et afin de compléter les obligations existantes prévues dans le présent règlement, lorsque, sur la base d'une enquête de marché, la Commission a constaté qu'il fallait mettre à jour les obligations concernant les pratiques qui limitent la contestabilité des services de plateforme essentiels ou sont déloyales et que la mise à jour envisagée relève du champ d'application de l'habilitation établie pour de tels actes délégués dans le présent règlement.

(98) Lorsqu'elle adopte des actes délégués en vertu du présent règlement, il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient

menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 « Mieux légiférer »[19]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(99) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour préciser les mesures à mettre en œuvre par les contrôleurs d'accès en vue de respecter effectivement les obligations leur incombant en vertu du présent règlement; pour suspendre, en tout ou en partie, une obligation spécifique imposée à un contrôleur d'accès; pour exempter un contrôleur d'accès, en tout ou en partie, d'une obligation spécifique; pour préciser les mesures à mettre en œuvre par un contrôleur d'accès lorsqu'il se soustrait aux obligations prévues par le présent règlement; pour mener à bien une enquête de marché en vue de la désignation des contrôleurs d'accès; pour imposer des mesures correctives en cas de non-respect systématique; pour ordonner des mesures provisoires à l'encontre d'un contrôleur d'accès; pour rendre des engagements obligatoires pour un contrôleur d'accès; pour établir son constat de non-respect; pour fixer le montant définitif de l'astreinte; pour déterminer la forme, la teneur et les autres modalités des notifications, des communications d'informations, des demandes motivées et des rapports réglementaires transmis par les contrôleurs d'accès; pour définir les modalités opérationnelles et techniques en vue de la mise en œuvre de l'interopérabilité ainsi que la méthodologie et la procédure pour la description, devant faire l'objet d'un audit, des techniques utilisées pour le profilage des consommateurs; pour prévoir les modalités pratiques des procédures, de la prolongation des délais, de l'exercice des droits au cours de la procédure, de la divulgation, ainsi que de la coopération et de la coordination entre la Commission et les autorités nationales. Ces compétences devraient être exercées conformément au règlement (UE) no 182/2011.

(100)Il convient d'avoir recours à la procédure d'examen pour l'adoption d'un acte d'exécution relatif aux modalités pratiques de la coopération et de la coordination entre la Commission et les États membres. Il convient d'avoir recours à la procédure consultative pour les autres actes d'exécution prévus par le présent règlement. Cela se justifie par le fait que ces autres actes d'exécution ont trait à des aspects pratiques des procédures établies dans le présent règlement, tels que la forme, le contenu et d'autres détails des différentes étapes de la procédure, aux modalités pratiques des différentes étapes de la procédure, par exemple la prolongation des délais de procédure ou le droit d'être entendu, ainsi qu'aux décisions d'exécution individuelles adressées à un contrôleur d'accès.

Comité consultatif

(101)Conformément au règlement (UE) no 182/2011, chaque État membre devrait être représenté au sein du comité consultatif et décider de la composition de sa délégation. Cette délégation peut inclure, entre autres, des experts des autorités compétentes des États membres, qui possèdent l'expertise nécessaire pour une question spécifique présentée au comité consultatif.

Lanceurs d'alerte

(102)Les lanceurs d'alerte peuvent porter à l'attention des autorités compétentes de nouvelles informations qui peuvent les aider à détecter les infractions au présent règlement et leur permettre d'imposer des sanctions. Il convient de veiller à ce que des dispositifs adéquats soient mis en place afin de permettre aux lanceurs d'alerte de prévenir les autorités compétentes en cas d'infraction potentielle ou avérée du présent règlement et de protéger ces lanceurs d'alerte contre des représailles. À cette fin, il convient de prévoir dans le présent règlement que la directive (UE) 2019/1937 du Parlement européen et du Conseil[20] s'applique au signalement de violations du présent règlement et à la protection des personnes signalant de telles violations.

(103)En vue de renforcer la sécurité juridique, l'applicabilité, en vertu du présent règlement, de la directive (UE) 2019/1937 aux signalements de violations du présent règlement et à la protection des personnes qui signalent de telles violations devrait se refléter dans ladite directive. Il y a lieu de modifier en conséquence l'annexe de la

19. JO L 123 du 12.5.2016, p. 1.
20. Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).

directive (UE) 2019/1937. Il appartient aux États membres de veiller à ce que cette modification soit prise en compte dans leurs mesures de transposition adoptées conformément à la directive (UE) 2019/1937, bien que l'adoption de mesures de transposition nationales ne soit pas une condition de l'applicabilité de ladite directive, à compter de la date d'application du présent règlement, au signalement de violations du présent règlement et à la protection des personnes qui les signalent.

Associations de consommateurs

(104)Les consommateurs devraient être autorisés à faire respecter leurs droits relatifs aux obligations imposées aux contrôleurs d'accès dans le cadre du présent règlement, au titre d'actions représentatives conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil[21]. À cette fin, le présent règlement devrait prévoir que la directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs. Il y a donc lieu de modifier en conséquence l'annexe de ladite directive. Il appartient aux États membres de veiller à ce que cette modification soit prise en compte dans leurs mesures de transposition adoptées conformément à la directive (UE) 2020/1828, bien que l'adoption de mesures de transposition nationales à cet égard ne soit pas une condition de l'applicabilité de ladite directive à ces actions représentatives. L'applicabilité de la directive (UE) 2020/1828 aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs devrait commencer à partir de la date d'application des dispositions législatives, réglementaires et administratives des États membres nécessaires à la transposition de ladite directive, ou à partir de la date d'application du présent règlement, la plus récente de ces dates étant retenue.

(105)La Commission devrait évaluer périodiquement le présent règlement et suivre de près son incidence sur la contestabilité et l'équité des relations commerciales dans l'économie des plateformes en ligne, notamment en vue de déterminer la nécessité de modifications au regard des évolutions technologiques ou commerciales. Cette évaluation devrait comprendre le réexamen régulier de la liste des services de plateforme essentiels et des obligations imposées aux contrôleurs d'accès, ainsi que le contrôle de leur respect, dans le but d'assurer la contestabilité et l'équité des marchés numériques dans l'Union. Dans ce contexte, la Commission devrait également évaluer le champ de l'obligation concernant l'interopérabilité des services de communications électroniques non fondés sur la numérotation. Afin d'obtenir une vue d'ensemble de l'évolution du secteur numérique, l'évaluation devrait tenir compte des expériences des États membres et des parties prenantes concernées. À cet égard, la Commission devrait également avoir la possibilité de tenir compte des avis et rapports qui lui sont présentés par l'observatoire sur l'économie des plateformes en ligne instauré par la décision de la Commission C(2018) 2393 du 26 avril 2018. À la suite de l'évaluation, la Commission devrait prendre les mesures qui s'imposent. La Commission devrait avoir pour objectif le maintien d'un niveau élevé de protection et de respect des droits et valeurs communs, en particulier l'égalité et la non-discrimination, lorsqu'elle procède aux appréciations et réexamens des pratiques et des obligations énoncées dans le présent règlement.

(106)Sans préjudice de la procédure budgétaire et grâce aux instruments financiers existants, il convient d'allouer à la Commission des ressources humaines, financières et techniques suffisantes pour lui permettre de s'acquitter efficacement de ses tâches et d'exercer les pouvoirs nécessaires à l'exécution du présent règlement.

(107)Étant donné que l'objectif du présent règlement, à savoir assurer la contestabilité et l'équité du secteur numérique en général, et des services de plateforme essentiels en particulier, en vue d'encourager l'innovation, la qualité des produits et services numériques, l'équité et la compétitivité des prix, ainsi qu'un niveau élevé de qualité et de choix pour les utilisateurs finaux dans le secteur numérique, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison du modèle commercial et des activités des contrôleurs d'accès, ainsi que de l'ampleur et des effets de ces activités, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformé-

21. Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

ment au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(108)Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42 du règlement (UE) 2018/1725 et a rendu un avis le 10 février 2021[22].

cf. CEPD/EDPS

(109)Le présent règlement respecte les droits fondamentaux et observe les principes reconnus par la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 16, 47 et 50. En conséquence, l'interprétation et l'application du présent règlement devraient observer ces droits et principes,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
OBJET, CHAMP D'APPLICATION ET DÉFINITIONS

Article premier
Objet et champ d'application

1. L'objectif du présent règlement est de contribuer au bon fonctionnement du marché intérieur, en établissant des règles harmonisées visant à garantir à toutes les entreprises la contestabilité et l'équité des marchés dans le secteur numérique de l'Union là où des contrôleurs d'accès sont présents, au profit des entreprises utilisatrices et des utilisateurs finaux.

2. Le présent règlement s'applique aux services de plateforme essentiels fournis ou proposés par des contrôleurs d'accès à des entreprises utilisatrices établies dans l'Union ou à des utilisateurs finaux établis ou situés dans l'Union, quel que soit le lieu d'établissement ou de résidence des contrôleurs d'accès et quel que soit le droit par ailleurs applicable à la fourniture des services.

3. Le présent règlement ne s'applique pas aux marchés liés:

a) aux réseaux de communications électroniques au sens de l'article 2, point 1), de la directive (UE) 2018/1972;

b) aux services de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972, autres que ceux liés aux services de communications interpersonnelles non fondés sur la numérotation.

4. En ce qui concerne les services de communications interpersonnelles au sens de l'article 2, point 5), de la directive (UE) 2018/1972, le présent règlement est sans préjudice des pouvoirs et responsabilités confiés aux autorités de régulation nationales et autres autorités compétentes en vertu de l'article 61 de ladite directive.

5. Afin d'éviter la fragmentation du marché intérieur, les États membres n'imposent pas d'obligations supplémentaires aux contrôleurs d'accès par voie législative, réglementaire ou de mesures administratives aux fins de garantir la contestabilité et l'équité des marchés. Aucune disposition du présent règlement n'empêche les États membres d'imposer aux entreprises, y compris les entreprises fournissant des services de plateforme essentiels, des obligations sur des points ne relevant pas du champ d'application du présent règlement, pour autant que ces obligations soient compatibles avec le droit de l'Union et ne résultent pas du fait que les entreprises concernées ont le statut d'un contrôleur d'accès au sens du présent règlement.

6. Le présent règlement est sans préjudice de l'application des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Il est également sans préjudice de l'application:

22. JO C 147 du 26.4.2021, p. 4.

a) des règles de concurrence nationales interdisant les accords anticoncurrentiels, les décisions d'associations d'entreprises, les pratiques concertées et les abus de position dominante;

b) des règles de concurrence nationales interdisant d'autres formes de comportement unilatéral, dans la mesure où elles s'appliquent à des entreprises autres que les contrôleurs d'accès ou reviennent à imposer des obligations supplémentaires aux contrôleurs d'accès; et

c) du règlement (CE) no 139/2004 du Conseil[23] et des règles nationales relatives au contrôle des concentrations.

7. Les autorités nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution en se fondant sur les principes établis aux articles 37 et 38.

Article 2
Définitions

Aux fins du présent règlement, on entend par:
1) « contrôleur d'accès »: une entreprise fournissant des services de plateforme essentiels, désignée conformément à l'article 3;
2) « service de plateforme essentiel »: l'un des services suivants:
a) services d'intermédiation en ligne;
b) moteurs de recherche en ligne;
c) services de réseaux sociaux en ligne;
d) services de plateformes de partage de vidéos;
e) services de communications interpersonnelles non fondés sur la numérotation;
f) systèmes d'exploitation;
g) navigateurs internet;
h) assistants virtuels;
i) services d'informatique en nuage;
j) services de publicité en ligne, y compris tout réseau publicitaire, échange publicitaire et autre service d'intermédiation publicitaire, fourni par une entreprise qui met à disposition n'importe lequel des services de plateforme essentiels énumérés aux points a) à i);
3) « service de la société de l'information »: tout service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535;
4) « secteur numérique »: le secteur des produits et services fournis au moyen ou par l'intermédiaire de services de la société de l'information;
5) « services d'intermédiation en ligne »: les services d'intermédiation en ligne au sens de l'article 2, point 2), du règlement (UE) 2019/1150;
6) « moteur de recherche en ligne »: un moteur de recherche en ligne au sens de l'article 2, point 5), du règlement (UE) 2019/1150;
7) « service de réseaux sociaux en ligne »: une plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations;
8) « service de plateformes de partage de vidéos »: un service de plateformes de partage de vidéos au sens de l'article 1er, paragraphe 1, point a bis), de la directive 2010/13/UE;
9) « service de communications interpersonnelles non fondé sur la numérotation »: un service de communications interpersonnelles non fondé sur la numérotation au sens de l'article 2, point 7), de la directive (UE) 2018/1972;
10) « système d'exploitation »: un logiciel système qui contrôle les fonctions de base du matériel informatique ou du logiciel et permet d'y faire fonctionner des applications logicielles;
11) « navigateur internet »: une application logicielle qui permet aux utilisateurs finaux d'accéder à des contenus internet hébergés sur des serveurs connectés à des réseaux tels que l'internet, y compris les navigateurs internet autonomes, ainsi que les

23. Règlement (CE) no 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises (« le règlement CE sur les concentrations ») (JO L 24 du 29.1.2004, p. 1).

navigateurs internet intégrés ou inclus dans un logiciel ou équivalent, et d'interagir avec ces contenus;
12) « assistant virtuel »: un logiciel qui peut traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores, visuelles ou écrites, de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, donne accès à d'autres services ou contrôle des appareils connectés physiques;
13) « service d'informatique en nuage »: un service d'informatique en nuage au sens de l'article 4, point 19), de la directive (UE) 2016/1148 du Parlement européen et du Conseil[24];
14) « boutique d'applications logicielles »: un type de services d'intermédiation en ligne qui se concentre sur les applications logicielles en tant que produit ou service intermédié;
15) « application logicielle »: tout produit ou service numérique fonctionnant sur un système d'exploitation;
16) « service de paiement »: un service de paiement au sens de l'article 4, point 3), de la directive (UE) 2015/2366;
17) « service technique à l'appui d'un service de paiement »: un service au sens de l'article 3, point j), de la directive (UE) 2015/2366;
18) « système de paiement pour les achats intégrés à des applications »: une application logicielle, un service ou une interface utilisateur qui facilite les achats de contenu numérique ou de services numériques dans une application logicielle, y compris en termes de contenu, d'abonnements, de caractéristiques ou de fonctionnalité, ainsi que les paiements pour de tels achats;
19) « service d'identification »: un type de service fourni avec ou à l'appui des services de plateforme essentiels permettant toute sorte de vérification de l'identité des utilisateurs finaux ou des entreprises utilisatrices, indépendamment de la technologie utilisée;
20) « utilisateur final »: toute personne physique ou morale utilisant des services de plateforme essentiels autrement qu'en tant qu'entreprise utilisatrice;
21) « entreprise utilisatrice »: toute personne physique ou morale agissant à titre commercial ou professionnel qui utilise des services de plateforme essentiels aux fins ou dans le cadre de la fourniture de biens ou de services à des utilisateurs finaux;
22) « classement »: la priorité relative accordée aux biens ou services proposés par le biais de services d'intermédiation en ligne, de services de réseaux sociaux en ligne, de services de plateformes de partage de vidéos ou d'assistants virtuels, ou la pertinence reconnue aux résultats de recherche par les moteurs de recherche en ligne, tels qu'ils sont présentés, organisés ou communiqués par les entreprises fournissant des services d'intermédiation en ligne, des services de plateformes de partage de vidéos, des assistants virtuels ou des moteurs de recherche en ligne, indépendamment des moyens technologiques utilisés pour une telle présentation, organisation ou communication et indépendamment du fait qu'un seul résultat soit ou non présenté ou communiqué;
23) « résultats de recherche »: toute information, sous quelque format que ce soit, y compris des données textuelles, graphiques, vocales ou autres, renvoyées en réponse à une recherche, et en rapport avec celle-ci, que l'information renvoyée soit un résultat payant ou non, une réponse directe ou tout produit, service ou renseignement proposé en lien avec les résultats organiques, affiché en même temps que ceux-ci ou partiellement ou entièrement intégré dans ceux-ci;
24) « données »: toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;
25) « données à caractère personnel »: les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;
26) « données à caractère non personnel »: les données autres que les données à caractère personnel;
27) « entreprise »: une entité exerçant une activité économique, indépendamment de son statut juridique et de son mode de financement, y compris toutes les entreprises liées ou connectées formant un groupe par l'intermédiaire du contrôle direct ou indirect d'une entreprise par une autre;
28) « contrôle »: la possibilité d'exercer une influence déterminante sur l'activité d'une entreprise, au sens de l'article 3, paragraphe 2, du règlement (CE) no 139/2004;

cf. RGPD

24. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

29) « interopérabilité »: la capacité d'échanger des informations et d'utiliser mutuellement les informations échangées par le biais d'interfaces ou d'autres solutions, de telle sorte que tous les éléments du matériel informatique ou des logiciels fonctionnent de toutes les manières dont elles sont censées fonctionner avec d'autres matériels informatiques et logiciels ainsi qu'avec les utilisateurs;
30) « chiffre d'affaires »: le montant réalisé par une entreprise au sens de l'article 5, paragraphe 1, du règlement (CE) no 139/2004;
31) « profilage »: le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;
32) « consentement »: le consentement au sens de l'article 4, point 11), du règlement (UE) 2016/679;
33) « juridiction nationale »: toute juridiction d'un État membre au sens de l'article 267 du traité sur le fonctionnement de l'Union européenne.

cf. RGPD

cf. RGPD

CHAPITRE II
CONTRÔLEURS D'ACCÈS

Article 3
Désignation des contrôleurs d'accès

1. Une entreprise est désignée comme étant un contrôleur d'accès si:
a) elle a un poids important sur le marché intérieur;
b) elle fournit un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux; et
c) elle jouit d'une position solide et durable, dans ses activités, ou jouira, selon toute probabilité, d'une telle position dans un avenir proche.

2. Une entreprise est réputée satisfaire aux exigences respectives du paragraphe 1:
a) en ce qui concerne le paragraphe 1, point a), si elle a réalisé un chiffre d'affaires annuel dans l'Union supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne ou sa juste valeur marchande équivalente a atteint au moins 75 milliards d'euros au cours du dernier exercice, et qu'elle fournit le même service de plateforme essentiel dans au moins trois États membres;
b) en ce qui concerne le paragraphe 1, point b), si elle fournit un service de plateforme essentiel qui, au cours du dernier exercice, a compté au moins 45 millions d'utilisateurs finaux actifs par mois établis ou situés dans l'Union et au moins 10 000 entreprises utilisatrices actives par an établies dans l'Union, faisant l'objet d'une identification et de calculs conformément à la méthode et aux indicateurs définis dans l'annexe;
c) en ce qui concerne le paragraphe 1, point c), si les seuils visés au point b) du présent paragraphe ont été atteints au cours de chacun des trois derniers exercices.

3. Lorsqu'une entreprise fournissant des services de plateforme essentiels atteint l'ensemble des seuils mentionnés au paragraphe 2, elle en informe la Commission sans tarder et, en tout état de cause, dans les deux mois qui suivent après que ces seuils ont été atteints et lui fournit les informations pertinentes visées au paragraphe 2. Cette notification inclut les informations pertinentes visées au paragraphe 2 pour chacun des services de plateforme essentiels de l'entreprise qui atteint les seuils mentionnés au paragraphe 2, point b). Lorsqu'un autre service de plateforme essentiel fourni par l'entreprise qui a précédemment été désignée comme étant un contrôleur d'accès atteint les seuils mentionnés au paragraphe 2, points b) et c), cette entreprise en informe la Commission dans les deux mois qui suivent le respect de ces seuils.

Lorsque l'entreprise fournissant le service de plateforme essentiel n'informe pas la Commission conformément au premier alinéa du présent paragraphe et qu'elle ne parvient pas à fournir, dans le délai fixé par la Commission dans la demande de renseignements visée à l'article 21, tous les renseignements pertinents dont la Commission a besoin pour désigner l'entreprise concernée en tant que contrôleur d'accès en vertu du paragraphe 4 du présent article, la Commission conserve le droit de désigner cette entreprise en tant que contrôleur d'accès, sur la base des informations dont elle dispose.

Lorsque l'entreprise fournissant des services de plateforme essentiels se conforme à la demande de renseignement en vertu du deuxième alinéa du présent paragraphe ou que

les renseignements sont fournis après l'expiration du délai visé à cet alinéa, la Commission applique la procédure prévue au paragraphe 4.

4. La Commission désigne comme étant un contrôleur d'accès, sans retard indu et au plus tard dans un délai de 45 jours ouvrables après avoir reçu toutes les informations visées au paragraphe 3, une entreprise fournissant des services de plateforme essentiels qui atteint tous les seuils mentionnés au paragraphe 2.

5. L'entreprise fournissant des services de plateforme essentiels peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'elle atteigne tous les seuils prévus au paragraphe 2 et en raison des circonstances dans lesquelles le service de plateforme essentiel concerné opère, elle ne satisfait pas aux exigences énumérées au paragraphe 1.

Lorsque la Commission estime que les arguments présentés en vertu du premier alinéa par l'entreprise fournissant des services de plateforme essentiels ne sont pas suffisamment étayés parce qu'ils ne remettent manifestement pas en cause les présomptions énoncées au paragraphe 2 du présent article, elle peut rejeter ces arguments dans le délai visé au paragraphe 4, sans appliquer la procédure prévue à l'article 17, paragraphe 3.

Lorsque l'entreprise fournissant des services de plateforme essentiels présente de tels arguments suffisamment étayés, remettant manifestement en cause les présomptions mentionnées au paragraphe 2 du présent article, la Commission peut, nonobstant le premier alinéa du présent paragraphe et dans le délai visé au paragraphe 4 du présent article, ouvrir la procédure prévue à l'article 17, paragraphe 3.

Si la Commission conclut que l'entreprise fournissant des services de plateforme essentiels n'a pas été en mesure de démontrer que les services de plateforme essentiels qu'elle fournit ne satisfont pas aux exigences du paragraphe 1 du présent article, elle désigne cette entreprise comme étant un contrôleur d'accès conformément à la procédure prévue à l'article 17, paragraphe 3.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de compléter le présent règlement en précisant la méthode utilisée pour déterminer si les seuils quantitatifs fixés au paragraphe 2 du présent article sont atteints, et d'adapter régulièrement ladite méthode, le cas échéant, aux évolutions du marché et de la technologie.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 afin de modifier le présent règlement en mettant à jour la méthode et la liste des indicateurs définies dans l'annexe.

8. La Commission désigne comme étant un contrôleur d'accès, conformément à la procédure prévue à l'article 17, toute entreprise fournissant des services de plateforme essentiels qui satisfait à chacune des exigences visées au paragraphe 1 du présent article, mais n'atteint pas chacun des seuils mentionnés au paragraphe 2 du présent article.

À cette fin, la Commission tient compte de tout ou partie des éléments ci-après, pour autant qu'ils soient pertinents pour l'entreprise considérée fournissant des services de plateforme essentiels:

a) la taille, y compris le chiffre d'affaires et la capitalisation boursière, les activités et la position de ladite entreprise;

b) le nombre d'entreprises utilisatrices qui font appel au service de plateforme essentiel pour atteindre des utilisateurs finaux et le nombre d'utilisateurs finaux;

c) les effets de réseau et les avantages tirés des données, en particulier en ce qui concerne l'accès aux données à caractère personnel et non personnel et la collecte de ces données par ladite entreprise, ou les capacités d'analyse de cette dernière;

d) tout effet d'échelle et de gamme dont bénéficie l'entreprise, y compris en ce qui concerne les données et, le cas échéant, ses activités en dehors de l'Union;

e) la captivité des entreprises utilisatrices ou des utilisateurs finaux, y compris les coûts de changement et les biais comportementaux qui réduisent la capacité des entreprises utilisatrices et des utilisateurs finaux à changer de fournisseur ou à opter pour un multihébergement;

f) une structure d'entreprise conglomérale ou l'intégration verticale de cette entreprise, permettant par exemple à celle-ci de pratiquer des subventions croisées, de combiner des données provenant de différentes sources ou de tirer parti de sa position; ou

g) d'autres caractéristiques structurelles des entreprises ou des services.

Dans le cadre de la réalisation de son appréciation au titre du présent paragraphe, la Commission tient compte de l'évolution prévisible en relation avec les éléments énumérés au deuxième alinéa, y compris tout projet de concentration faisant intervenir une autre entreprise fournissant des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettant la collecte de données.

Si une entreprise fournissant un service de plateforme essentiel qui n'atteint pas les seuils quantitatifs visés au paragraphe 2 ne se conforme pas de manière substantielle aux mesures d'enquête ordonnées par la Commission et si ce manquement persiste après que cette entreprise a été invitée à s'y conformer dans un délai raisonnable et à soumettre ses observations, la Commission peut désigner cette entreprise comme étant un contrôleur d'accès sur la base des faits dont dispose la Commission.

9. Pour chaque entreprise désignée comme étant un contrôleur d'accès en vertu du paragraphe 4 ou 8, la Commission énumère dans la décision de désignation les services de plateforme essentiels concernés qui sont fournis au sein de cette entreprise et qui constituent, individuellement, des points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, comme indiqué au paragraphe 1, point b).

10. Le contrôleur d'accès se conforme aux obligations prévues aux articles 5, 6 et 7 dans les six mois suivant l'énumération d'un service de plateforme essentiel dans la décision de désignation conformément au paragraphe 9 du présent article.

Article 4
Réexamen du statut de contrôleur d'accès

1. La Commission peut, sur demande ou de sa propre initiative, revoir, modifier ou abroger à tout moment une décision de désignation adoptée au titre de l'article 3 pour l'une des raisons suivantes:

a) l'un des faits sur lesquels la décision de désignation repose subit un changement important;

b) la décision de désignation repose sur des informations incomplètes, inexactes ou dénaturées.

2. La Commission réexamine régulièrement, et au moins tous les trois ans, si les contrôleurs d'accès continuent de satisfaire aux exigences fixées à l'article 3, paragraphe 1. Ce réexamen détermine également s'il faut modifier la liste des services de plateforme essentiels du contrôleur d'accès qui constituent, individuellement, des points d'accès majeurs permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, comme indiqué à l'article 3, paragraphe 1, point
b). Ces réexamens n'ont pas d'effet suspensif sur les obligations du contrôleur d'accès.

La Commission examine également au moins une fois par an si de nouvelles entreprises fournissant des services de plateforme essentiels satisfont à ces exigences.

Si la Commission constate, sur la base des examens menés conformément au premier alinéa, que les faits sur lesquels repose la désignation des entreprises fournissant des services de plateforme essentiels comme contrôleurs d'accès ont évolué, elle adopte une décision confirmant, modifiant ou abrogeant la décision de désignation.

3. La Commission publie et tient à jour de façon continue une liste des contrôleurs d'accès et la liste des services de plateforme essentiels pour lesquels ils doivent se conformer aux obligations prévues au chapitre III.

CHAPITRE III
PRATIQUES DES CONTRÔLEURS D'ACCÈS QUI LIMITENT LA CONTESTABILITÉ OU SONT DÉLOYALES

Article 5
Obligations incombant aux contrôleurs d'accès

1. Le contrôleur d'accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9.

2. Tout contrôleur d'accès est tenu de ne pas:
a) traiter, aux fins de la fourniture de services de publicité en ligne, les données à caractère personnel des utilisateurs finaux qui recourent à des services de tiers utilisant des services de plateforme essentiels fournis par le contrôleur d'accès;
b) combiner les données à caractère personnel provenant du service de plateforme essentiel concerné avec les données à caractère personnel provenant de tout autre service de plateforme essentiel ou de tout autre service fourni par le contrôleur d'accès, ni avec des données à caractère personnel provenant de services tiers;
c) utiliser de manière croisée les données à caractère personnel provenant du service de plateforme essentiel concerné dans le cadre d'autres services fournis séparément par le contrôleur d'accès, y compris d'autres services de plateforme essentiels, et inversement; et
d) inscrire les utilisateurs finaux à d'autres services du contrôleur d'accès dans le but de combiner des données à caractère personnel, à moins que ce choix précis ait été présenté à l'utilisateur final et que ce dernier ait donné son consentement au sens de l'article 4, point 11), et de l'article 7 du règlement (UE) 2016/679.

cf. RGPD

Lorsque le consentement donné aux fins du premier alinéa a été refusé ou retiré par l'utilisateur final, le contrôleur d'accès ne réitère pas sa demande de consentement pour la même finalité plus d'une fois par période d'un an.

Le présent paragraphe est sans préjudice de la possibilité pour le contrôleur d'accès de se fonder sur l'article 6, paragraphe 1, points c), d) et e), du règlement (UE) 2016/679, le cas échéant.

cf. RGPD

3. Le contrôleur d'accès n'empêche pas les entreprises utilisatrices de proposer les mêmes produits ou services aux utilisateurs finaux au moyen de services d'intermédiation en ligne tiers ou de leur propre canal de vente directe en ligne à des prix ou conditions différents de ceux qui sont proposés par les services d'intermédiation en ligne du contrôleur d'accès.

4. Le contrôleur d'accès permet aux entreprises utilisatrices de communiquer et de promouvoir leurs offres gratuitement, y compris à des conditions différentes, auprès des utilisateurs finaux acquis grâce à son service de plateforme essentiel ou via d'autres canaux, et de conclure des contrats avec ces utilisateurs finaux, en utilisant ou non à cette fin les services de plateforme essentiels du contrôleur d'accès.

5. Le contrôleur d'accès permet aux utilisateurs finaux, par l'intermédiaire de ses services de plateforme essentiels, d'accéder à des contenus, abonnements, fonctionnalités ou autres éléments et de les utiliser en se servant de l'application logicielle de l'entreprise utilisatrice, y compris lorsque ces utilisateurs finaux ont acquis de tels éléments auprès des entreprises utilisatrices concernées sans avoir recours aux services de plateforme essentiels du contrôleur d'accès.

6. Le contrôleur d'accès n'empêche ni ne restreint directement ou indirectement la possibilité pour les entreprises utilisatrices ou les utilisateurs finaux de faire part à toute autorité publique compétente, y compris les juridictions nationales, de tout problème de non-respect, par le contrôleur d'accès, du droit de l'Union ou national pertinent dans le cadre des pratiques de ce dernier. Cela s'entend sans préjudice du droit

des entreprises utilisatrices et des contrôleurs d'accès d'établir, dans leurs accords, les conditions d'utilisation de mécanismes légaux de traitement des plaintes.

7. Le contrôleur d'accès n'exige pas des utilisateurs finaux qu'ils utilisent, ni des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification, un moteur de navigateur internet ou un service de paiement, ou un service technique qui appuie la fourniture des services de paiement, tels que des systèmes de paiement destinés aux achats dans des applications, de ce contrôleur d'accès dans le cadre des services fournis par les entreprises utilisatrices en ayant recours aux services de plateforme essentiels de ce contrôleur d'accès.

8. Le contrôleur d'accès n'exige pas des entreprises utilisatrices ou des utilisateurs finaux qu'ils s'abonnent ou s'enregistrent à tout autre service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, ou atteignant les seuils visés à l'article 3, paragraphe 2, point b), comme condition pour être en mesure d'utiliser l'un des services de plateforme essentiels de ce contrôleur d'accès énumérés en vertu dudit article, d'y accéder, de s'y inscrire ou de s'y enregistrer.

9. Le contrôleur d'accès communique quotidiennement à chaque annonceur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les annonceurs, à la demande de l'annonceur, des informations gratuites relatives à chaque publicité mise en ligne par l'annonceur, en ce qui concerne:

a) le prix et les frais payés par cet annonceur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d'accès;

b) la rémunération perçue par l'éditeur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l'éditeur; et
c) les mesures quantitatives à partir desquelles chacun des prix, frais et rémunérations est calculé.

Dans le cas où un éditeur ne consent pas au partage d'informations sur la rémunération perçue, comme visé au point b) du premier alinéa, le contrôleur d'accès fournit gratuitement à chaque annonceur des informations sur la rémunération moyenne quotidienne perçue par cet éditeur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

10. Le contrôleur d'accès communique quotidiennement à chaque éditeur à qui il fournit des services de publicité en ligne, ou aux tiers autorisés par les éditeurs, à la demande de l'éditeur, des informations gratuites relatives à chaque publicité affichée dans l'inventaire de l'éditeur, en ce qui concerne:

a) la rémunération perçue et les frais payés par cet éditeur, y compris les déductions et suppléments éventuels, pour chacun des services de publicité en ligne concernés fournis par le contrôleur d'accès;

b) le prix payé par l'annonceur, y compris les déductions et suppléments éventuels, sous réserve du consentement de l'annonceur; et
c) la mesure à partir de laquelle chacun des prix, frais et rémunérations est calculé.

Dans le cas où un annonceur ne consent pas au partage d'informations, le contrôleur d'accès fournit gratuitement à chaque éditeur des informations sur le prix moyen quotidien payé par cet annonceur, y compris les déductions et suppléments éventuels, pour les publicités concernées.

Article 6
Obligations incombant aux contrôleurs d'accès susceptibles d'être précisées en vertu de l'article 8

1. Le contrôleurs d'accès se conforme à toutes les obligations énoncées au présent article pour chacun de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9.

2. Le contrôleur d'accès n'utilise pas, en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par ces entreprises utilisatrices dans le cadre de leur utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices.

Aux fins du premier alinéa, les données qui ne sont pas accessibles au public comprennent toutes les données agrégées et non agrégées générées par les entreprises utilisatrices qui peuvent être déduites ou collectées au travers des activités commerciales de ces entreprises ou de leurs clients, y compris les données concernant les clics, les recherches, les vues et la voix, dans le cadre des services de plateforme essentiels concernés ou de services fournis conjointement aux services de plateforme essentiels concernés du contrôleur d'accès, ou à leur appui.

3. Le contrôleur d'accès autorise et permet techniquement la désinstallation facile par les utilisateurs finaux de toute application logicielle dans son système d'exploitation, sans préjudice de la possibilité pour ce contrôleur d'accès de restreindre cette désinstallation si elle concerne une application logicielle essentielle au fonctionnement du système d'exploitation ou de l'appareil et qui ne peut techniquement pas être proposée séparément par des tiers.

Le contrôleur d'accès autorise et permet techniquement la modification facile par les utilisateurs finaux des paramètres par défaut de son système d'exploitation, son assistant virtuel et son navigateur internet qui dirigent ou orientent les utilisateurs finaux vers des produits et des services proposés par le contrôleur d'accès. Pour ce faire, il invite notamment les utilisateurs finaux, au moment de leur première utilisation de son moteur de recherche en ligne, son assistant virtuel ou son navigateur internet énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, à choisir dans une liste des principaux fournisseurs de services disponibles, le moteur de recherche en ligne, assistant virtuel ou navigateur internet vers lequel le système d'exploitation du contrôleur d'accès dirige ou oriente les utilisateurs par défaut, et le moteur de recherche en ligne vers lequel l'assistant virtuel et le navigateur internet du contrôleur d'accès dirige ou oriente les utilisateurs par défaut.

4. Le contrôleur d'accès autorise et permet techniquement l'installation et l'utilisation effective d'applications logicielles ou de boutiques d'applications logicielles de tiers utilisant ou interopérant avec son système d'exploitation, et permet l'accès à ces applications logicielles ou boutiques d'applications logicielles par des moyens autres que les services de plateforme essentiels concernés du contrôleur d'accès. Le cas échéant, le contrôleur d'accès n'empêche pas une application logicielle ou boutique d'application logicielle de tiers téléchargée d'inviter les utilisateurs finaux à choisir s'ils souhaitent utiliser par défaut ladite application logicielle ou boutique d'application logicielle téléchargée. Le contrôleur d'accès permet techniquement aux utilisateurs finaux qui choisissent d'utiliser par défaut ladite application logicielle ou boutique d'application logicielle téléchargée de procéder facilement à ce changement.

Rien n'empêche le contrôleur d'accès de prendre, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures visant à éviter que les applications logicielles ou les boutiques d'applications logicielles de tiers ne compromettent l'intégrité du matériel informatique ou du système d'exploitation qu'il fournit, à condition que ces mesures soient dûment justifiées par le contrôleur d'accès.

En outre, rien n'empêche le contrôleur d'accès d'appliquer, dans la mesure où elles ne vont pas au-delà de ce qui est strictement nécessaire et proportionné, des mesures et des paramètres autres que les paramètres par défaut permettant aux utilisateurs finaux de protéger efficacement la sécurité en ce qui concerne les applications logicielles ou les boutiques d'applications logicielles de tiers, à condition que ces mesures et paramètres autres que les paramètres par défaut soient dûment justifiés par le contrôleur d'accès.

5. Le contrôleur d'accès n'accorde pas, en matière de classement ainsi que pour l'indexation et l'exploration qui y sont liées, un traitement plus favorable aux services

et produits proposés par le contrôleur d'accès lui-même qu'aux services ou produits similaires d'un tiers. Le contrôleur d'accès applique des conditions transparentes, équitables et non discriminatoires à ce classement.

6. Le contrôleur d'accès ne restreint pas techniquement ou d'une autre manière la capacité des utilisateurs finaux de changer d'applications logicielles et de services qui sont accessibles en utilisant les services de plateforme essentiels du contrôleur d'accès et de s'y abonner, y compris en ce qui concerne le choix des services d'accès à l'internet pour les utilisateurs finaux.

7. Le contrôleur d'accès permet gratuitement aux fournisseurs de services et aux fournisseurs de matériel informatique d'interopérer efficacement avec les mêmes caractéristiques matérielles et logicielles auxquelles on accède ou qui sont contrôlées par l'intermédiaire du système d'exploitation ou de l'assistant virtuel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, que celles qui sont disponibles pour les services ou le matériel fournis par le contrôleur d'accès, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité. En outre, le contrôleur d'accès permet gratuitement aux entreprises utilisatrices et à d'autres fournisseurs de services fournis conjointement à des services de plateforme essentiels, ou à l'appui de ceux-ci, d'interopérer effectivement avec les mêmes caractéristiques du système d'exploitation, matérielles ou logicielles, que ces caractéristiques fassent partie ou non d'un système d'exploitation, que celles qui sont disponibles pour ce contrôleur d'accès ou que celui-ci utilise dans le cadre de la fourniture de tels services, ainsi que d'accéder à ces caractéristiques aux fins de l'interopérabilité.

Rien n'empêche le contrôleur d'accès de prendre des mesures strictement nécessaires et proportionnées visant à éviter que l'interopérabilité ne compromette l'intégrité du système d'exploitation, de l'assistant virtuel, du matériel informatique ou du logiciel qu'il fournit, à condition que ces mesures soient dûment justifiées par le contrôleur d'accès.

8. Le contrôleur d'accès fournit aux annonceurs et aux éditeurs, ainsi qu'aux tiers autorisés par les annonceurs et les éditeurs, à leur demande et gratuitement, un accès aux outils de mesure de performance du contrôleur d'accès et aux données qui leur sont nécessaires pour effectuer leur propre vérification indépendante de l'inventaire publicitaire, notamment les données agrégées et non agrégées. Ces données sont fournies de manière à permettre aux annonceurs et aux éditeurs d'utiliser leurs propres outils de vérification et de mesure afin d'évaluer la performance des services de plateforme essentiels fournis par le contrôleur d'accès.

9. Le contrôleur d'accès assure aux utilisateurs finaux et aux tiers autorisés par un utilisateur final, à leur demande et gratuitement, la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final dans le cadre de l'utilisation du service de plateforme essentiel concerné, y compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données.

10. Le contrôleur d'accès assure gratuitement aux entreprises utilisatrices et aux tiers autorisés par les entreprises utilisatrices, à leur demande, un accès et une utilisation effectifs, de haute qualité, continus et en temps réel en ce qui concerne les données agrégées et non agrégées, y compris les données à caractère personnel, fournies ou générées dans le cadre de l'utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, par ces entreprises utilisatrices et par les utilisateurs finaux qui se servent des produits et services fournis par ces entreprises utilisatrices. En ce qui concerne les données à caractère personnel, le contrôleur d'accès ne donne un tel accès aux données à caractère personnel et ne les utilise que lorsque les données sont directement liées à l'utilisation faite par les utilisateurs finaux en lien avec les produits ou services que l'entreprise utilisatrice concernée fournit par l'intermédiaire du service de plateforme essentiel concerné, et lorsque les utilisateurs finaux optent pour un tel partage de données en donnant leur consentement.

11. Le contrôleur d'accès procure à toute entreprise tierce fournissant des moteurs de recherche en ligne, à sa demande et à des conditions équitables, raisonnables et non discriminatoires, un accès aux données concernant les classements, requêtes, clics et vues en lien avec les recherches gratuites et payantes générées par les utilisateurs

finaux sur ses moteurs de recherche en ligne. Toutes ces données concernant les requêtes, clics et vues constituent des données à caractère personnel et sont anonymisées.

12. Le contrôleur d'accès applique aux entreprises utilisatrices des conditions générales d'accès équitables, raisonnables et non discriminatoires à ses boutiques d'applications logicielles, moteurs de recherche en ligne et services de réseaux sociaux en ligne énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9.

À cette fin, le contrôleur d'accès publie des conditions générales d'accès, comportant notamment un mécanisme de règlement extrajudiciaire des litiges.

La Commission évalue si les conditions générales d'accès publiées sont conformes au présent paragraphe.

13. Le contrôleur d'accès ne dispose pas de conditions générales de résiliation de la fourniture d'un service de plateforme essentiel qui soient disproportionnées. Le contrôleur d'accès veille à ce que les conditions de résiliation puissent être appliquées sans difficulté excessive.

Article 7
Obligations incombant aux contrôleurs d'accès concernant l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation

1. Lorsqu'un contrôleur d'accès fournit des services de communications interpersonnelles non fondés sur la numérotation qui sont énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9, il rend les fonctionnalités de base de ses services de communications interpersonnelles non fondés sur la numérotation interopérables avec les services de communications interpersonnelles non fondés sur la numérotation de tout autre fournisseur qui propose ou a l'intention de proposer de tels services dans l'Union, en fournissant sur demande et gratuitement les interfaces techniques nécessaires ou des solutions similaires qui facilitent l'interopérabilité.

2. Le contrôleur d'accès rend interopérables au moins les fonctionnalités de base visées au paragraphe 1 énumérées ci-après dès lors qu'il fournit lui-même ces fonctionnalités à ses propres utilisateurs finaux:

a) à la suite de l'établissement de la liste figurant dans la décision de désignation conformément à l'article 3, paragraphe 9:

i) messagerie textuelle de bout en bout entre deux utilisateurs finaux individuels;

ii) partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre deux utilisateurs finaux individuels;

b) dans un délai de deux ans à compter de la désignation:

i) messagerie textuelle de bout en bout entre des groupes d'utilisateurs finaux individuels;

ii) partage d'images, de messages vocaux, de vidéos et d'autres fichiers joints dans les communications de bout en bout entre une conversation de groupe et un utilisateur final individuel;

c) dans un délai de quatre ans à compter de la désignation:

i) appels vocaux de bout en bout entre deux utilisateurs finaux individuels;

ii) appels vidéo de bout en bout entre deux utilisateurs finaux individuels;

iii) appels vocaux de bout en bout entre une conversation de groupe et un utilisateur final individuel;

iv) appels vidéo de bout en bout entre une conversation de groupe et un utilisateur final individuel.

3. Le niveau de sécurité, y compris le chiffrement de bout en bout, le cas échéant, que le contrôleur d'accès fournit à ses propres utilisateurs finaux est maintenu dans l'ensemble des services interopérables.

4. Le contrôleur d'accès publie une offre de référence énonçant les détails techniques et les conditions générales d'interopérabilité avec ses services de communications interpersonnelles non fondés sur la numérotation, y compris les détails nécessaires concernant le niveau de sécurité et le chiffrement de bout en bout. Le contrôleur d'accès publie cette offre de référence avant la fin de la période visée à l'article 3, paragraphe 10, et la met à jour si nécessaire.

5. À la suite de la publication de l'offre de référence conformément au paragraphe 4, tout fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui propose ou a l'intention de proposer de tels services dans l'Union peut demander l'interopérabilité avec les services de communications interpersonnelles non fondés sur la numérotation fournis par le contrôleur d'accès. Une telle demande peut porter sur tout ou partie des fonctionnalités de base énumérées au paragraphe 2. Le contrôleur d'accès accepte toute demande raisonnable d'interopérabilité dans un délai de trois mois à compter de la réception de cette demande en rendant opérationnelles les fonctionnalités de base demandées.

6. La Commission peut, à titre exceptionnel et sur demande motivée du contrôleur d'accès, reporter les délais prévus pour se conformer au paragraphe 2 ou 5 lorsque le contrôleur d'accès démontre que cela est nécessaire pour assurer l'interopérabilité effective et maintenir le niveau de sécurité requis, y compris le chiffrement de bout en bout, le cas échéant.

7. Les utilisateurs finaux des services de communications interpersonnelles non fondés sur la numérotation du contrôleur d'accès et du fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule la demande demeurent libres de décider s'ils utilisent les fonctionnalités de base interopérables qui peuvent être fournies par le contrôleur d'accès au titre du paragraphe 1.

8. Le contrôleur d'accès recueille et échange avec le fournisseur de services de communications interpersonnelles non fondés sur la numérotation qui formule une demande d'interopérabilité uniquement les données à caractère personnel d'utilisateurs finaux qui sont strictement nécessaires à la fourniture d'une interopérabilité effective. Toute collecte et tout échange de données à caractère personnel de ce type sont pleinement conformes au règlement (UE) 2016/679 et à la directive 2002/58/CE.

cf. RGPD

9. Rien n'empêche le contrôleur d'accès de prendre des mesures visant à éviter que les demandes d'interopérabilité formulées par des fournisseurs tiers de services de communications interpersonnelles non fondés sur la numérotation ne compromettent l'intégrité, la sécurité et la confidentialité de ses services, à condition que ces mesures soient strictement nécessaires et proportionnées, et soient dûment justifiées par le contrôleur d'accès.

Article 8
Respect des obligations incombant aux contrôleurs d'accès

1. Le contrôleur d'accès assure et démontre le respect des obligations prévues aux articles 5, 6 et 7 du présent règlement. Les mesures que le contrôleur d'accès met en œuvre pour garantir la conformité avec lesdits articles atteignent effectivement les objectifs du présent règlement et de l'obligation concernée. Le contrôleur d'accès veille à ce que la mise en œuvre de ces mesures respecte le droit applicable, en particulier le règlement (UE) 2016/679, la directive 2002/58/CE, la législation relative à la cybersécurité, à la protection des consommateurs et à la sécurité des produits, ainsi que les exigences en matière d'accessibilité.

cf. RGPD

2. La Commission peut, de sa propre initiative ou à la demande d'un contrôleur d'accès conformément au paragraphe 3 du présent article, ouvrir la procédure prévue à l'article 20.

La Commission peut adopter un acte d'exécution, qui précise les mesures que le contrôleur d'accès concerné est tenu de mettre en œuvre afin de se conformer effectivement aux obligations énoncées aux articles 6 et 7. Cet acte d'exécution est adopté dans les six mois suivant l'ouverture de la procédure prévue à l'article 20, en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Lorsqu'elle ouvre la procédure de sa propre initiative, en cas de contournement, conformément à l'article 13, ces mesures peuvent porter sur les obligations énoncées aux articles 5, 6 et 7.

3. Un contrôleur d'accès peut demander à la Commission d'engager un processus afin de déterminer si les mesures que ce contrôleur d'accès entend mettre en œuvre ou a mises en œuvre pour se conformer aux articles 6 et 7 atteignent effectivement l'objectif de l'obligation pertinente dans la situation spécifique du contrôleur d'accès. La Commission dispose d'une marge d'appréciation pour décider s'il y a lieu d'engager un tel processus, dans le respect des principes d'égalité de traitement, de proportionnalité et de bonne administration.

Dans sa demande, le contrôleur d'accès fournit un mémoire motivé pour expliquer les mesures qu'il entend mettre en œuvre ou a mises en œuvre. Le contrôleur d'accès fournit en outre une version non confidentielle de son mémoire motivé qui peut être partagée avec des tiers conformément au paragraphe 6.

4. Les paragraphes 2 et 3 sont sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

5. En vue de l'adoption de la décision visée au paragraphe 2, la Commission fait part de ses constatations préliminaires au contrôleur d'accès dans un délai de trois mois à compter de l'ouverture de la procédure au titre de l'article 20. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

6. Afin de permettre effectivement aux tiers intéressés de présenter des observations, la Commission publie, lorsqu'elle communique ses constatations préliminaires au contrôleur d'accès conformément au paragraphe 5 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de la situation et les mesures qu'elle envisage de prendre ou que le contrôleur d'accès concerné devrait prendre selon elle. La Commission fixe un délai raisonnable dans lequel ces observations peuvent être formulées.

7. En précisant les mesures visées au paragraphe 2, la Commission veille à ce qu'elles atteignent effectivement les objectifs du présent règlement et de l'obligation pertinente et à ce qu'elles soient proportionnées compte tenu de la situation spécifique du contrôleur d'accès et du service concerné.

8. Dans le but de préciser les obligations prévues à l'article 6, paragraphes 11 et 12, la Commission évalue en outre si les mesures envisagées ou mises en œuvre garantissent qu'aucun déséquilibre ne demeure entre les droits et les obligations des entreprises utilisatrices et si les mesures ne confèrent pas elles-mêmes au contrôleur d'accès un avantage disproportionné par rapport au service qu'il fournit aux entreprises utilisatrices.

9. En ce qui concerne la procédure visée au paragraphe 2, la Commission peut, sur demande ou de sa propre initiative, décider de la rouvrir lorsque:

a) l'un des faits sur lesquels la décision repose subit un changement important; ou

b) la décision repose sur des informations incomplètes, inexactes ou dénaturées; ou

c) les mesures énoncées dans la décision ne sont pas efficaces.

Article 9
Suspension

1. Lorsque le contrôleur d'accès démontre dans une demande motivée que le respect d'une obligation spécifique énoncée à l'article 5, 6 ou 7 concernant un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, menacerait, en raison de circonstances exceptionnelles échappant à son contrôle, la viabilité économique de ses activités dans l'Union, la Commission peut adopter un acte d'exécution établissant sa décision de suspendre, à titre exceptionnel, entièrement ou partiellement, l'obligation spécifique visée dans cette demande motivée (ci-après dénommée « décision de suspension »). Dans cet acte d'exécution, la Commission étaye sa décision de suspension en indiquant les circonstances exceptionnelles justifiant la suspension. La portée et la durée de cet acte d'exécution sont limitées à ce qui est nécessaire pour remédier à cette menace pour la viabilité du contrôleur d'accès. La Commission s'efforce d'adopter cet acte d'exécution sans tarder et au plus tard trois mois après réception d'une demande complète et motivée. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une suspension est accordée en vertu du paragraphe 1, la Commission réexamine sa décision de suspension chaque année, à moins qu'un intervalle plus court ne soit indiqué dans ladite décision. À la suite de ce réexamen, la Commission lève entièrement ou partiellement la suspension, ou décide que les conditions visées au paragraphe 1 demeurent remplies.

3. En cas d'urgence, sur demande motivée d'un contrôleur d'accès, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme essentiels spécifiques, avant même d'adopter la décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

4. Lors de l'évaluation de la demande visée aux paragraphes 1 et 3, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur la viabilité économique des activités du contrôleur d'accès dans l'Union ainsi que sur les tiers, en particulier les PME et les consommateurs. La suspension peut être soumise à des conditions et obligations devant être définies par la Commission afin de garantir un juste équilibre entre ces intérêts et les objectifs du présent règlement.

Article 10
Exemption pour raisons de santé publique et de sécurité publique

1. Sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut adopter un acte d'exécution établissant sa décision d'exempter ce contrôleur d'accès, entièrement ou partiellement, d'une obligation particulière prévue à l'article 5, 6 ou 7 en ce qui concerne un service de plateforme essentiel énuméré dans la décision de désignation conformément à l'article 3, paragraphe 9, lorsqu'une telle exemption est justifiée par les motifs énoncés au paragraphe 3 du présent article (ci-après dénommée « décision d'exemption »). La Commission adopte la décision d'exemption dans un délai de trois mois après réception d'une demande complète et motivée, et fournit une déclaration motivée expliquant les raisons de l'exemption. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Lorsqu'une exemption est accordée en vertu du paragraphe 1, la Commission réexamine sa décision d'exemption lorsque le motif de l'exemption n'existe plus ou au minimum chaque année. À la suite de ce réexamen, la Commission lève entièrement ou partiellement l'exemption ou décide que les conditions du paragraphe 1 demeurent remplies.

3. Une exemption en vertu du paragraphe 1 ne peut être accordée que pour des motifs de santé publique ou de sécurité publique.

4. En cas d'urgence, sur demande motivée d'un contrôleur d'accès ou de sa propre initiative, la Commission peut suspendre provisoirement l'application d'une obligation spécifique visée au paragraphe 1 pour un ou plusieurs services de plateforme

essentiels spécifiques, avant même d'adopter la décision visée audit paragraphe. Une telle demande peut être présentée et acceptée à tout moment, dans l'attente de l'évaluation de la Commission en application du paragraphe 1.

5. Lors de l'évaluation de la demande visée aux paragraphes 1 et 4, la Commission tient compte en particulier de l'incidence du respect de l'obligation spécifique sur les motifs énumérés au paragraphe 3, ainsi que des effets sur le contrôleur d'accès concerné et sur les tiers. La Commission peut soumettre la suspension à des conditions et obligations afin de garantir un juste équilibre entre les objectifs visés par les motifs énoncés au paragraphe 3 et les objectifs du présent règlement.

Article 11
Établissement de rapports

1. Dans les six mois suivant sa désignation au titre de l'article 3, et conformément à l'article 3, paragraphe 10, le contrôleur d'accès remet à la Commission un rapport décrivant de manière détaillée et transparente les mesures qu'il a mises en œuvre pour garantir le respect des obligations énoncées aux articles 5, 6 et 7.

2. Dans le délai visé au paragraphe 1, le contrôleur d'accès publie et remet à la Commission une synthèse non confidentielle de ce rapport.

Le contrôleur d'accès met à jour au moins annuellement ce rapport et cette synthèse non confidentielle. La Commission insère sur son site internet un lien vers cette synthèse non confidentielle.

Article 12
Mise à jour des obligations des contrôleurs d'accès

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour compléter le présent règlement en ce qui concerne les obligations existantes énoncées aux articles 5 et 6. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées aux articles 5 et 6.

2. Le champ d'application d'un acte délégué adopté conformément au paragraphe 1 se limite à:

a) élargir une obligation qui s'applique uniquement dans le cadre de certains services de plateforme essentiels à d'autres services de plateforme essentiels énumérés à l'article 2, point 2);

b) élargir une obligation dont bénéficient certaines entreprises utilisatrices ou utilisateurs finaux de manière à ce que d'autres entreprises utilisatrices ou utilisateurs finaux en soient bénéficiaires;

c) préciser les modalités d'exécution par les contrôleurs d'accès des obligations énoncées aux articles 5 et 6 afin de garantir le respect effectif de ces obligations;

d) élargir une obligation qui s'applique uniquement dans le cadre de certains services fournis conjointement à des services de plateforme essentiels, ou à leur appui, à d'autres services fournis conjointement à des services de plateforme essentiels, ou à leur appui;

e) élargir une obligation qui s'applique uniquement dans le cadre de certains types de données afin qu'elle s'applique à d'autres types de données;

f) ajouter des conditions supplémentaires lorsqu'une obligation impose certaines conditions concernant le comportement d'un contrôleur d'accès; ou

g) appliquer une obligation qui régit la relation entre plusieurs services de plateforme essentiels du contrôleur d'accès à la relation entre un service de plateforme essentiel et d'autres services du contrôleur d'accès.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour modifier le présent règlement en ce qui concerne la liste des fonctionnalités de base recensées à l'article 7, paragraphe 2, en ajoutant ou en supprimant des fonctionnalités de services de communications interpersonnelles non fondés sur la numérotation.

Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées à l'article 7.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 49 pour compléter le présent règlement en ce qui concerne les obligations prévues à l'article 7 en précisant les modalités d'exécution des obligations afin de garantir le respect effectif de ces obligations. Ces actes délégués sont fondés sur une enquête de marché menée en vertu de l'article 19 qui a mis en évidence la nécessité de maintenir à jour ces obligations afin de lutter contre les pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyales au même titre que les pratiques qui sont l'objet des obligations énoncées à l'article 7.

5. Une pratique visée aux paragraphes 1, 3 et 4 est considérée comme limitant la contestabilité des services de plateforme essentiels ou comme déloyale:

a) lorsque cette pratique est le fait des contrôleurs d'accès et est susceptible d'entraver l'innovation et de limiter le choix pour les entreprises utilisatrices et les utilisateurs finaux parce qu'elle:

i) porte atteinte ou risque de porter atteinte durablement à la contestabilité d'un service de plateforme essentiel ou d'autres services dans le secteur numérique en raison de la création ou du renforcement d'obstacles empêchant d'autres entreprises de s'implanter ou de se développer en tant que fournisseurs d'un service de plateforme essentiel ou d'autres services dans le secteur numérique; ou

ii) empêche les autres opérateurs d'avoir le même accès que le contrôleur d'accès à un intrant clé; ou

b) lorsqu'il existe un déséquilibre entre les droits et les obligations des entreprises utilisatrices et que le contrôleur d'accès obtient un avantage des entreprises utilisatrices qui est disproportionné par rapport au service fourni par ce contrôleur d'accès à ces entreprises utilisatrices.

Article 13
Anticontournement

1. Une entreprise fournissant des services de plateforme essentiels ne segmente pas, ni ne divise, subdivise, fragmente ou fractionne ces services par des moyens contractuels, commerciaux, techniques ou autres dans le but de contourner les seuils quantitatifs fixés à l'article 3, paragraphe 2. Aucune de ces pratiques de la part d'une entreprise n'empêche la Commission de désigner celle-ci comme contrôleur d'accès au titre de l'article 3, paragraphe 4.

2. Lorsqu'elle soupçonne qu'une entreprise fournissant des services de plateforme essentiels met en œuvre une pratique visée au paragraphe 1, la Commission peut exiger de cette entreprise toute information qu'elle juge nécessaire pour déterminer si cette entreprise s'est livrée à une telle pratique.

3. Le contrôleur d'accès veille à ce que les obligations des articles 5, 6 et 7 soient pleinement et effectivement respectées.

4. Le contrôleur d'accès ne se livre à aucun comportement compromettant le respect effectif des obligations des articles 5, 6 et 7, que ce comportement soit de nature contractuelle, commerciale, technique ou autre, ou qu'il consiste en l'utilisation de techniques comportementales ou d'une conception d'interface.

5. Si le consentement est requis pour la collecte, le traitement, l'utilisation croisée et le partage de données à caractère personnel afin que le respect du présent règlement soit garanti, le contrôleur d'accès prend les mesures nécessaires, soit pour permettre aux entreprises utilisatrices d'obtenir directement le consentement requis au traitement de ces données, lorsque ce consentement est exigé en application du règlement (UE) 2016/679 ou de la directive 2002/58/CE, soit pour se conformer aux règles et principes de l'Union en matière de protection des données et de la vie privée par d'autres moyens, dont la fourniture aux entreprises utilisatrices de données dûment anonymisées, s'il y a lieu. Le contrôleur d'accès ne rend pas l'obtention de ce consentement par les entreprises utilisatrices plus lourde que pour ses propres services.

cf. RGPD

6. Le contrôleur d'accès ne détériore ni les conditions, ni la qualité de l'un de ses services de plateforme essentiels fournis aux entreprises utilisatrices ou aux utilisateurs finaux qui font valoir leurs droits ou choix prévus aux articles 5, 6 et 7, et ne rend pas l'exercice de ces droits ou choix excessivement difficile, y compris en proposant des choix à l'utilisateur final de manière partiale, ou encore en utilisant la structure, la conception, la fonction ou le mode de fonctionnement d'une interface utilisateur ou d'une partie connexe pour perturber l'autonomie des utilisateurs finaux ou des entreprises utilisatrices, leur prise de décision ou leur libre choix.

7. Lorsque le contrôleur d'accès contourne ou tente de contourner l'une des obligations énoncées à l'article 5, 6 ou 7 d'une manière décrite aux paragraphes 4, 5 et 6 du présent article, la Commission peut ouvrir la procédure prévue à l'article 20 et adopter un acte d'exécution visé à l'article 8, paragraphe 2, afin de préciser les mesures que le contrôleur d'accès est tenu de mettre en œuvre.

8. Le paragraphe 6 du présent article est sans préjudice des pouvoirs conférés à la Commission en vertu des articles 29, 30 et 31.

Article 14
Obligation d'informer sur les concentrations

1. Le contrôleur d'accès informe la Commission de tout projet de concentration au sens de l'article 3 du règlement (CE) no 139/2004, lorsque les entités qui fusionnent ou la cible de la concentration fournissent des services de plateforme essentiels ou tout autre service dans le secteur numérique ou permettent la collecte de données, que ce projet soit soumis à une obligation de notification à la Commission en application dudit règlement ou à une autorité nationale de concurrence compétente selon les règles nationales en matière de concentrations.

Le contrôleur d'accès informe la Commission de cette concentration avant sa réalisation et après la conclusion de l'accord, la publication de l'offre publique d'achat ou d'échange ou l'acquisition d'une participation de contrôle.

2. Les informations communiquées par le contrôleur d'accès conformément au paragraphe 1 renseignent au moins sur les entreprises concernées par la concentration, leurs chiffres d'affaires annuels mondiaux et au sein de l'Union, leurs domaines d'activité, y compris les activités directement liées à la concentration et la valeur transactionnelle de l'accord ou une estimation de celle-ci, et sont accompagnées d'un résumé relatif à la concentration, y compris sa nature et sa justification, et d'une liste des États membres concernés par la concentration.

Les informations communiquées par le contrôleur d'accès indiquent également, pour tous les services de plateforme essentiels concernés, leurs chiffres d'affaires annuels au sein de l'Union, le nombre d'entreprises utilisatrices actives par an et le nombre d'utilisateurs finaux actifs par mois, respectivement.

3. Si à la suite d'une concentration visée au paragraphe 1 du présent article, d'autres services de plateforme essentiels atteignent, individuellement, les seuils fixés à l'article 3, paragraphe 2, point b), le contrôleur d'accès concerné en informe la Commission dans les deux mois à compter de la réalisation de la concentration et fournit à la Commission les informations visées à l'article 3, paragraphe 2.

4. La Commission communique aux autorités compétentes des États membres toute information reçue en application du paragraphe 1 et publie chaque année la liste des

acquisitions dont elle a été informée par les contrôleurs d'accès en application dudit paragraphe.

La Commission tient compte de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués.

5. Les autorités compétentes des États membres peuvent utiliser les informations reçues au titre du paragraphe 1 du présent article pour demander à la Commission d'examiner la concentration conformément à l'article 22 du règlement (CE) no 139/2004.

Article 15
Obligation d'audit

1. Dans les six mois suivant sa désignation conformément à l'article 3, le contrôleur d'accès soumet à la Commission une description ayant fait l'objet d'un audit indépendant de toutes les techniques de profilage des consommateurs qu'il applique dans le cadre de ses services de plateforme essentiels énumérés dans la décision de désignation conformément à l'article 3, paragraphe 9. La Commission transmet cette description ayant fait l'objet d'un audit au comité européen de la protection des données.

2. La Commission peut adopter un acte d'exécution visé à l'article 46, paragraphe 1, point g), afin de mettre au point la méthodologie et la procédure de l'audit.

3. Le contrôleur d'accès met à la disposition du public un aperçu de la description ayant fait l'objet d'un audit visée au paragraphe 1. Ce faisant, le contrôleur d'accès est autorisé à tenir compte de la nécessité que ses secrets d'affaires ne soient pas divulgués. Le contrôleur d'accès met à jour au moins annuellement cette description et cet aperçu.

CHAPITRE IV
ENQUÊTE DE MARCHÉ

Article 16
Ouverture d'une enquête de marché

1. Lorsque la Commission a l'intention de mener une enquête de marché en vue de l'adoption éventuelle de décisions en vertu des articles 17, 18 et 19, elle adopte une décision relative à l'ouverture d'une enquête de marché.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une enquête de marché conformément audit paragraphe.

3. La décision visée au paragraphe 1 précise:

a) la date d'ouverture de l'enquête de marché;

b) la description de la question sur laquelle porte l'enquête de marché;

c) le but de l'enquête de marché.

4. La Commission peut rouvrir une enquête de marché qu'elle a clôturée si:

a) l'un des faits sur lesquels repose une décision adoptée en vertu de l'article 17, 18 ou 19 subit un changement important; ou

b) la décision adoptée en vertu de l'article 17, 18 ou 19 repose sur des renseignements incomplets, inexacts ou dénaturés.

5. La Commission peut demander à une ou plusieurs autorités nationales compétentes de l'assister dans son enquête de marché.

Article 17
Enquête de marché pour la désignation des contrôleurs d'accès

1. La Commission peut mener une enquête de marché afin d'examiner si une entreprise fournissant des services de plateforme essentiels devrait être désignée comme étant un contrôleur d'accès en vertu de l'article 3, paragraphe 8, ou aux fins de déterminer les services de plateforme essentiels devant être recensés dans la décision de désignation en vertu de l'article 3, paragraphe 9. La Commission s'efforce de conclure son enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Afin de conclure son enquête de marché, la Commission adopte un acte d'exécution énonçant sa décision. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. Au cours d'une enquête de marché menée en vertu du paragraphe 1 du présent article, la Commission s'efforce de communiquer ses constatations préliminaires à l'entreprise fournissant des services de plateforme essentiels concernée, dans un délai de six mois à compter de la date visée à l'article 16, paragraphe 3, point a). Dans ses constatations préliminaires, la Commission explique si elle estime, à titre provisoire, qu'il est approprié que ladite entreprise soit désignée comme contrôleur d'accès en vertu de l'article 3, paragraphe 8, et que les services de plateforme essentiels concernés soient énumérés conformément à l'article 3, paragraphe 9.

3. Lorsque l'entreprise fournissant des services de plateforme essentiels atteint les seuils fixés à l'article 3, paragraphe 2, mais qu'elle a présenté des arguments suffisamment étayés en vertu de l'article 3, paragraphe 5, qui ont manifestement remis en cause la présomption énoncée à l'article 3, paragraphe 2, la Commission s'efforce de conclure l'enquête de marché dans un délai de cinq mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Dans un tel cas, la Commission s'efforce de communiquer à l'entreprise concernée ses constatations préliminaires conformément au paragraphe 2 du présent article dans un délai de trois mois à compter de la date visée à l'article 16, paragraphe 3, point a).

4. Lorsque la Commission, en vertu de l'article 3, paragraphe 8, désigne comme contrôleur d'accès une entreprise fournissant des services de plateforme essentiels qui ne jouit pas encore d'une position solide et durable dans ses activités, mais en jouira de manière prévisible dans un avenir proche, elle peut ne déclarer applicable à ce contrôleur d'accès qu'une ou plusieurs des obligations énoncées à l'article 5, paragraphes 3 à 6, et à l'article 6, paragraphes 4, 7, 9, 10 et 13, telles qu'elles sont précisées dans la décision de désignation. La Commission ne déclare applicables que les obligations appropriées et nécessaires pour empêcher le contrôleur d'accès concerné d'acquérir, par des moyens déloyaux, une position solide et durable dans ses activités. La Commission réexamine cette désignation conformément à la procédure prévue à l'article 4.

Article 18
Enquête de marché portant sur un non-respect systématique

1. La Commission peut mener une enquête de marché afin d'examiner si un contrôleur d'accès a fait preuve d'un non- respect systématique. La Commission conclut cette enquête de marché dans un délai de douze mois à compter de la date visée à l'article 16, paragraphe 3, point a). Lorsqu'il ressort de l'enquête de marché qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues à l'article 5, 6 ou 7 et qu'il a maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1, la Commission peut adopter un acte d'exécution imposant à un tel contrôleur d'accès toute mesure corrective comportementale ou structurelle qui soit proportionnée et nécessaire pour garantir le respect effectif du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La mesure corrective imposée conformément au paragraphe 1 du présent article peut inclure, dans la mesure où cette mesure corrective est proportionnée et nécessaire pour préserver ou rétablir l'équité et la contestabilité affectées par le non- respect systématique, l'interdiction faite au contrôleur d'accès, pendant une période limitée, de se lancer dans une concentration au sens de l'article 3 du règlement (CE) no 139/2004 en

ce qui concerne les services de plateforme essentiels ou d'autres services fournis dans le secteur numérique ou permettant la collecte de données, qui sont affectés par le non-respect systématique.

3. Un contrôleur d'accès est réputé avoir systématiquement contrevenu aux obligations prévues aux articles 5, 6 et 7 lorsque la Commission a émis au moins trois décisions constatant un manquement au titre de l'article 29 à l'encontre d'un contrôleur d'accès en ce qui concerne l'un de ses services de plateforme essentiels au cours d'une période de huit ans ayant précédé l'adoption de la décision d'ouverture d'une enquête de marché en vue de l'adoption éventuelle d'une décision selon le présent article.

4. La Commission communique ses constatations préliminaires au contrôleur d'accès concerné dans un délai de six mois à compter de la date visée à l'article 16, paragraphe 3, point a). Dans ses constatations préliminaires, la Commission explique si elle estime, à titre préliminaire, que les conditions prévues au paragraphe 1 du présent article sont réunies et quelle mesure ou quelles mesures correctives elle considère, à titre préliminaire, comme nécessaires et proportionnées.

5. Afin de permettre aux tiers intéressés de formuler effectivement des observations, la Commission publie, en même temps qu'elle communique ses constatations préliminaires au contrôleur d'accès conformément au paragraphe 4 ou le plus tôt possible après une telle communication, une synthèse non confidentielle de l'affaire et des mesures correctives qu'elle envisage d'imposer. La Commission fixe un délai raisonnable dans lequel de telles observations doivent être formulées.

6. Lorsque la Commission a l'intention d'adopter une décision en vertu du paragraphe 1 du présent article en rendant obligatoires les engagements que le contrôleur d'accès propose de prendre en vertu de l'article 25, elle publie une synthèse non confidentielle de l'affaire ainsi que l'essentiel du contenu des engagements. Les tiers intéressés peuvent soumettre leurs observations dans un délai raisonnable qui est fixé par la Commission.

7. Au cours de l'enquête de marché, la Commission peut en prolonger la durée, à condition que cette prolongation se justifie par des motifs objectifs et soit proportionnée. Cette prolongation peut s'appliquer au délai imparti à la Commission pour formuler ses constatations préliminaires ou au délai imparti pour l'adoption de la décision finale. La durée totale de la ou des prolongations décidées en vertu du présent paragraphe ne dépasse pas six mois.

8. Afin de garantir le respect effectif des obligations prévues aux articles 5, 6 et 7 par le contrôleur d'accès, la Commission réexamine régulièrement les mesures correctives qu'elle impose conformément aux paragraphes 1 et 2 du présent article. La Commission est habilitée à modifier ces mesures correctives si, après une nouvelle enquête de marché, elle estime que celles-ci ne sont pas efficaces.

Article 19
Enquête de marché portant sur les nouveaux services et les nouvelles pratiques

1. La Commission peut mener une enquête de marché afin d'examiner s'il conviendrait d'inscrire un ou plusieurs services du secteur numérique sur la liste des services de plateforme essentiels prévus à l'article 2, point 2), ou afin de détecter des pratiques qui limitent la contestabilité des services de plateforme essentiels ou qui sont déloyaux et auxquels le présent règlement ne permet pas de remédier de manière effective. Dans son évaluation, la Commission tient compte de toutes les conclusions pertinentes des procédures au titre des articles 101 et 102 du traité sur le fonctionnement de l'Union européenne concernant les marchés numériques, ainsi que de toute autre évolution pertinente.

2. La Commission peut, lorsqu'elle mène une enquête de marché en vertu du paragraphe 1, consulter des tiers, y compris des entreprises utilisatrices et des utilisateurs finaux de services du secteur numérique qui font l'objet d'une enquête, ainsi que des entreprises utilisatrices et des utilisateurs finaux soumis à des pratiques faisant l'objet d'une enquête.

3. La Commission publie ses constatations dans un rapport dans un délai de dix-huit mois à compter de la date visée à l'article 16, paragraphe 3, point a).

Ce rapport est présenté au Parlement européen et au Conseil tout en étant, s'il y a lieu, assorti:
a) d'une proposition législative modifiant le présent règlement dans le but d'inclure des services supplémentaires du secteur numérique dans la liste des services de plateforme essentiels établie à l'article 2, point 2), ou d'intégrer de nouvelles obligations au chapitre III; ou
b) d'un projet d'acte délégué complétant le présent règlement en ce qui concerne les obligations énoncées aux articles 5 et 6, ou d'un projet d'acte délégué modifiant ou complétant le présent règlement en ce qui concerne les obligations énoncées à l'article 7, comme prévu à l'article 12.

Le cas échéant, la proposition législative modifiant le présent règlement visé au deuxième alinéa, point a), peut également viser à supprimer les services existants de la liste des services de plateforme essentiels établie à l'article 2, point 2), ou à supprimer des obligations existantes de l'article 5, 6 ou 7.

CHAPITRE V
POUVOIRS D'ENQUÊTE, DE COERCITION ET DE CONTRÔLE

Article 20
Ouverture d'une procédure

1. Lorsque la Commission a l'intention d'ouvrir une procédure en vue de l'adoption éventuelle de décisions au titre des articles 8, 29 et 30, elle adopte une décision relative à l'ouverture d'une procédure.

2. Nonobstant le paragraphe 1, la Commission peut exercer ses pouvoirs d'enquête en vertu du présent règlement avant d'ouvrir une procédure conformément audit paragraphe.

Article 21
Demandes de renseignements

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut, par simple demande ou par voie de décision, exiger des entreprises et associations d'entreprises qu'elles fournissent tous les renseignements nécessaires. La Commission peut également, par simple demande ou par voie de décision, exiger l'accès à toutes les données et algorithmes des entreprises et à des renseignements concernant les essais, ainsi que demander des explications les concernant.

2. Lorsqu'elle envoie une simple demande de renseignements à une entreprise ou à une association d'entreprises, la Commission indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel ils doivent être fournis, ainsi que les amendes prévues à l'article 30 qui est d'application au cas où des renseignements ou des explications incomplets, inexacts ou dénaturés seraient fournis.

3. Lorsque la Commission demande, par décision, aux entreprises et associations d'entreprises de fournir des renseignements, elle indique la base juridique et le but de la demande, précise les renseignements demandés et fixe le délai dans lequel les renseignements doivent être fournis. Lorsque la Commission demande aux entreprises de donner accès à toutes les données, tous les algorithmes et à des renseignements concernant les essais, elle indique le but de la demande et fixe le délai dans lequel il doit être accordé. Elle énonce également les amendes prévues à l'article 30 et indique ou inflige les astreintes prévues à l'article 31. De plus, elle informe du droit de faire examiner la décision par la Cour de justice.

4. Les entreprises ou associations d'entreprises ou leurs représentants fournissent les renseignements demandés, au nom de l'entreprise ou de l'association d'entreprises concernées. Les avocats dûment mandatés peuvent fournir les renseignements deman-

dés au nom de leurs mandants. Ces derniers restent pleinement responsables du caractère complet, exact et non dénaturé des renseignements fournis.

5. À la demande de la Commission, les autorités compétentes des États membres fournissent à la Commission tous les renseignements en leur possession qui sont nécessaires à l'accomplissement des tâches qui lui sont assignées par le présent règlement.

Article 22
Pouvoir de mener des auditions et de recueillir des déclarations

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut entendre toute personne physique ou morale qui accepte d'être auditionnée, aux fins de la collecte d'informations, en lien avec l'objet d'une enquête. La Commission a le droit d'enregistrer ces auditions par tout moyen technique.

2. Lorsqu'une audition au titre du paragraphe 1 du présent article est menée dans les locaux d'une entreprise, la Commission en informe l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et sur le territoire duquel l'audition a lieu. Si cette autorité le demande, les agents de celle-ci peuvent prêter assistance aux agents et aux autres personnes les accompagnant mandatés par la Commission pour conduire l'audition.

Article 23
Pouvoirs d'effectuer des inspections

1. Pour l'accomplissement de ses tâches au titre du présent règlement, la Commission peut procéder à toutes les inspections nécessaires d'une entreprise ou d'une association d'entreprises.

2. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection sont investis des pouvoirs suivants:
a) accéder à tous les locaux, terrains et moyens de transport des entreprises et associations d'entreprises;
b) contrôler les livres et autres documents en rapport avec l'activité, quel qu'en soit le support;
c) prendre ou obtenir sous quelque forme que ce soit copie ou extrait des livres et documents;
d) exiger de l'entreprise ou de l'association d'entreprises qu'elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments, et enregistrer ou consigner les explications données par tout moyen technique;
e) apposer des scellés sur tous les locaux commerciaux et livres ou documents pendant la durée de l'inspection et dans la mesure où cela est nécessaire aux fins de celle-ci;

f) demander à tout représentant ou membre du personnel de l'entreprise ou de l'association d'entreprises des explications sur des faits ou documents en rapport avec l'objet et le but de l'inspection et enregistrer ses réponses par tout moyen technique.

3. Pour effectuer les inspections, la Commission peut demander le concours d'auditeurs ou d'experts nommés par la Commission en vertu de l'article 26, paragraphe 2, ainsi que celui de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée.

4. Au cours des inspections, la Commission, les auditeurs ou experts nommés par cette dernière et l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée peuvent exiger de l'entreprise ou de l'association d'entreprises qu'elle donne accès à son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales et qu'elle fournisse des explications sur ces différents éléments. La Commission et les auditeurs ou experts nommés par celle-ci et l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le

territoire duquel l'inspection doit être menée peuvent poser des questions à tout représentant ou membre du personnel.

5. Les agents et les autres personnes les accompagnant mandatés par la Commission pour procéder à une inspection exercent leurs pouvoirs sur production d'un mandat écrit qui indique l'objet et le but de l'inspection, ainsi que les amendes prévues à l'article 30, qui s'appliquent au cas où les livres ou autres documents professionnels qui sont requis seraient présentés de manière incomplète et où les réponses aux demandes faites en application des paragraphes 2 et 4 du présent article seraient inexactes ou dénaturées. La Commission avise, en temps utile avant l'inspection, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1, paragraphe 6, sur le territoire duquel l'inspection doit être effectuée.

6. Les entreprises ou associations d'entreprises sont tenues de se soumettre à une inspection ordonnée par une décision de la Commission. Cette décision indique l'objet et le but de l'inspection, fixe la date à laquelle elle commence, indique les amendes et astreintes prévues aux articles 30 et 31 respectivement et informe du droit de faire examiner ladite décision devant la Cour de justice.

7. Les agents de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, sur le territoire duquel l'inspection doit être menée et les personnes mandatées ou nommées par cette autorité prêtent, à la demande de ladite autorité ou de la Commission, un concours actif aux agents et aux autres personnes les accompagnant mandatés par la Commission. Ils disposent à cette fin des pouvoirs prévus aux paragraphes 2 et 4 du présent article.

8. Lorsque les agents ou les autres personnes les accompagnant mandatés par la Commission constatent qu'une entreprise ou une association d'entreprises s'oppose à une inspection ordonnée en vertu du présent article, l'État membre concerné leur prête l'assistance nécessaire, en requérant au besoin la force publique ou une autorité disposant d'un pouvoir de contrainte équivalent, pour leur permettre d'exécuter leur mission d'inspection.

9. Si, en vertu du droit national, l'assistance prévue au paragraphe 8 du présent article requiert l'autorisation d'une autorité judiciaire, la Commission, l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou les agents mandatés par ces autorités la sollicitent. Cette autorisation peut également être sollicitée par mesure de précaution.

10. Lorsqu'une autorisation visée au paragraphe 9 du présent article est sollicitée, l'autorité judiciaire nationale vérifie que la décision de la Commission est authentique et que les mesures coercitives envisagées ne sont ni arbitraires ni excessives par rapport à l'objet de l'inspection. Lorsqu'elle contrôle la proportionnalité des mesures coercitives, l'autorité judiciaire nationale peut demander à la Commission, directement ou par l'intermédiaire de l'autorité nationale compétente de l'État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, des explications détaillées, notamment sur les motifs qui incitent la Commission à suspecter une infraction au présent règlement, ainsi que sur la gravité de l'infraction suspectée et sur la nature de l'implication de l'entreprise concernée. Cependant, l'autorité judiciaire nationale ne peut ni remettre en cause la nécessité de l'inspection ni exiger la communication des informations figurant dans le dossier de la Commission. Le contrôle de la légalité de la décision de la Commission est réservé à la Cour de justice.

Article 24
Mesures provisoires

En cas d'urgence justifiée par le fait qu'un préjudice grave et irréparable risque d'être causé aux entreprises utilisatrices ou aux utilisateurs finaux des contrôleurs d'accès, la Commission peut adopter un acte d'exécution ordonnant des mesures provisoires à l'encontre d'un contrôleur d'accès sur la base d'un constat prima facie d'infraction à l'article 5, 6 ou 7. Cet acte d'exécution est uniquement adopté dans le cadre d'une procédure ouverte en vue de l'adoption éventuelle d'une décision constatant un non-respect en application de l'article 29, paragraphe 1. Il est uniquement applicable pour une durée déterminée et est renouvelable dans la mesure où cela est nécessaire et opportun.

Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Article 25
Engagements

1. Si, au cours d'une procédure prévue par l'article 18, le contrôleur d'accès concerné propose de prendre des engagements pour les services de plateforme essentiels en cause afin de garantir le respect des obligations énoncées aux articles 5, 6 et 7, la Commission peut adopter un acte d'exécution rendant ces engagements obligatoires pour ce contrôleur d'accès et déclarer qu'il n'y a plus lieu d'agir. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La Commission peut, sur demande ou de sa propre initiative, rouvrir la procédure concernée par voie de décision lorsque:
a) l'un des faits sur lesquels la décision repose subit un changement important;
b) le contrôleur d'accès concerné contrevient à ses engagements;
c) la décision repose sur des informations incomplètes, inexactes ou dénaturées fournies par les parties;
d) les engagements ne sont pas effectifs.

3. Si la Commission devait estimer que les engagements proposés par le contrôleur d'accès concerné ne peuvent pas garantir le respect effectif des obligations prévues aux articles 5, 6 et 7, elle explique les raisons pour lesquelles elle ne rend pas ces engagements obligatoires dans la décision concluant la procédure en question.

Article 26
Contrôle des obligations et mesures

1. La Commission prend les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues aux articles 5, 6 et 7 et des décisions prises en vertu des articles 8, 18, 24, 25 et 29. Ces mesures peuvent notamment consister à imposer au contrôleur d'accès l'obligation de conserver tous les documents jugés pertinents pour évaluer la mise en œuvre et le respect de ces obligations et décisions.

2. Les mesures visées au paragraphe 1 peuvent comprendre la nomination d'experts et d'auditeurs externes indépendants, ainsi que la désignation d'agents par les autorités nationales compétentes des États membres, pour aider la Commission à contrôler les obligations et mesures et lui apporter une expertise et des connaissances spécifiques.

Article 27
Renseignements en provenance de tiers

1. Tous les tiers, y compris les entreprises utilisatrices, les concurrents ou les utilisateurs finaux des services de plateforme essentiels énumérés dans la décision de désignation en vertu de l'article 3, paragraphe 9, ainsi que leurs représentants, peuvent informer l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, ou directement la Commission concernant toute pratique ou tout comportement des contrôleurs d'accès relevant du champ d'application du présent règlement.

2. L'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, et la Commission ont toute latitude en ce qui concerne les mesures appropriées et ne sont pas tenues de donner suite aux renseignements reçus.

3. Lorsque l'autorité nationale compétente de l'État membre, chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, détermine, sur la base des renseignements reçus en vertu du paragraphe 1 du présent article, qu'il peut y avoir un cas de non-respect du présent règlement, elle transmet ces renseignements à la Commission.

Article 28
Fonction de vérification de la conformité

1. Les contrôleurs d'accès mettent en place une fonction de vérification de la conformité, qui est indépendante des fonctions opérationnelles du contrôleur d'accès et fait appel à un ou plusieurs responsables de la conformité, y compris le responsable général de la fonction de vérification de la conformité.

2. Le contrôleur d'accès veille à ce que la fonction de vérification de la conformité visée au paragraphe 1 dispose d'une autorité, d'une stature et de ressources suffisantes, ainsi que d'un accès à l'organe de direction du contrôleur d'accès pour contrôler le respect du présent règlement par ce dernier.

3. L'organe de direction du contrôleur d'accès s'assure que les responsables de la conformité désignés conformément au paragraphe 1 disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe 5.

L'organe de direction du contrôleur d'accès veille également à ce que le responsable général de la fonction de vérification de la conformité soit un cadre supérieur ayant une responsabilité distincte pour la fonction de vérification de la conformité.

4. Le responsable général de la fonction de vérification de la conformité fait directement rapport à l'organe de direction du contrôleur d'accès et peut soulever des préoccupations et avertir cet organe en cas de risque de non-respect du présent règlement, sans préjudice des responsabilités de l'organe de direction dans ses fonctions de surveillance et de gestion.

Il ne peut être congédié sans l'accord préalable de l'organe de direction du contrôleur d'accès.

5. Les responsables de la conformité désignés par le contrôleur d'accès en vertu du paragraphe 1 sont chargés des tâches suivantes:
a) organiser, suivre et contrôler les mesures et activités des contrôleurs d'accès visant à assurer le respect du présent règlement;
b) informer et conseiller la direction et les employés du contrôleur d'accès en ce qui concerne le respect du présent règlement;
c) contrôler, le cas échéant, le respect des engagements rendus contraignants en vertu de l'article 25, sans préjudice de la possibilité pour la Commission de désigner des experts externes indépendants conformément à l'article 26, paragraphe 2;
d) coopérer avec la Commission aux fins du présent règlement.

6. Les contrôleurs d'accès communiquent à la Commission le nom et les coordonnées du responsable général de la fonction de vérification de la conformité.

7. L'organe de direction du contrôleur d'accès définit, supervise et rend compte de la mise en œuvre des dispositifs de gouvernance du contrôleur d'accès qui garantissent l'indépendance de la fonction de vérification de la conformité, y compris la répartition des responsabilités dans l'organisation du contrôleur d'accès et la prévention des conflits d'intérêts.

8. L'organe de direction approuve et réexamine périodiquement, au moins une fois par an, les stratégies et les politiques relatives à la prise en compte, à la gestion et au suivi du respect du présent règlement.

9. L'organe de direction consacre suffisamment de temps à la gestion et au suivi du respect du présent règlement. Il participe activement aux décisions relatives à la gestion et à l'exécution du présent règlement et veille à ce que des ressources suffisantes soient allouées en la matière.

Article 29
Non-respect

1. La Commission adopte un acte d'exécution établissant son constat de non-respect (ci-après dénommé « décision constatant un non-respect ») lorsqu'elle constate qu'un contrôleur d'accès ne respecte pas un ou plusieurs des éléments suivants:

a) l'une des obligations prévues à l'article 5, 6 ou 7;
b) les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;
c) les mesures correctives imposées en vertu de l'article 18, paragraphe 1;
d) les mesures provisoires ordonnées en vertu de l'article 24; ou
e) les engagements rendus juridiquement obligatoires en vertu de l'article 25.

Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

2. La Commission s'efforce d'adopter sa décision constatant un non-respect dans les douze mois suivant l'ouverture de la procédure prévue à l'article 20.

3. Avant d'adopter la décision constatant un non-respect, la Commission fait part de ses constatations préliminaires au contrôleur d'accès concerné. Dans ces constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre ou que le contrôleur d'accès devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

4. Lorsqu'elle prévoit d'adopter une décision constatant un non-respect, la Commission peut consulter des tiers.

5. Dans la décision constatant un non-respect, la Commission ordonne au contrôleur d'accès de mettre fin au non- respect dans un délai approprié et de fournir des explications sur la manière dont il envisage de se mettre en conformité avec cette décision.

6. Le contrôleur d'accès fournit à la Commission la description des mesures qu'il a prises pour garantir le respect de la décision constatant un non-respect.

7. Lorsque la Commission décide de ne pas adopter une décision constatant un non-respect, elle clôt la procédure par voie de décision.

Article 30
Amendes

1. Dans la décision constatant un non-respect, la Commission peut infliger à un contrôleur d'accès des amendes jusqu'à concurrence de 10 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsqu'elle constate que le contrôleur d'accès, volontairement ou par négligence, ne respecte pas:
a) l'une des obligations prévues aux articles 5, 6 et 7;
b) les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;
c) les mesures correctives imposées en vertu de l'article 18, paragraphe 1;
d) les mesures provisoires ordonnées en vertu de l'article 24; ou
e) les engagements rendus juridiquement obligatoires en vertu de l'article 25.

2. Nonobstant le paragraphe 1 du présent article, dans une décision constatant un non-respect, la Commission peut infliger à un contrôleur d'accès des amendes allant jusqu'à 20 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsqu'elle constate qu'un contrôleur d'accès a commis la même infraction à une obligation prévue à l'article 5, 6 ou 7, ou une infraction similaire, en ce qui concerne le même service de plateforme essentiel que celui pour lequel une infraction avait été constatée dans une décision constatant un non-respect adoptée au cours des huit années précédentes.

3. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès le cas échéant, et aux associations d'entreprises, des amendes jusqu'à concurrence de 1 % de leur chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent lorsque, volontairement ou par négligence, elles:

a) ne fournissent pas, dans le délai imparti, les renseignements requis pour l'appréciation de leur désignation comme contrôleurs d'accès en vertu de l'article 3 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

b) ne respectent pas l'obligation d'information de la Commission prévue à l'article 3, paragraphe 3;

c) ne communiquent pas les renseignements exigés conformément à l'article 14, ou fournissent des renseignements inexacts, incomplets ou dénaturés;

d) ne présentent pas la description exigée au titre de l'article 15 ou fournissent des renseignements inexacts, incomplets ou dénaturés;

e) ne donnent pas l'accès aux données et algorithmes ou aux renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3;

f) ne fournissent pas les renseignements exigés dans le délai fixé en vertu de l'article 21, paragraphe 3, ou fournissent des renseignements ou des explications, qui sont exigés en vertu de l'article 21 ou fournis lors d'une audition en vertu de l'article 22, inexacts, incomplets ou dénaturés;

g) omettent de rectifier, dans le délai fixé par la Commission, les renseignements inexacts, incomplets ou dénaturés donnés par un représentant ou un membre du personnel, ou omettent ou refusent de fournir des renseignements complets sur des faits en rapport avec l'objet et le but d'une inspection décidée en vertu de l'article 23;

h) refusent de se soumettre à une inspection décidée en vertu de l'article 23;

i) ne se conforment pas aux obligations imposées par la Commission en vertu de l'article 26; ou

j) n'introduisent pas une fonction de vérification de la conformité conformément à l'article 28; ou

k) ne respectent pas les conditions d'accès au dossier de la Commission conformément à l'article 34, paragraphe 4.

4. Pour déterminer le montant d'une amende, la Commission tient compte de la gravité, de la durée et de la récurrence ainsi que, pour les amendes infligées au titre du paragraphe 3, du retard causé à la procédure.

5. Lorsqu'une amende est infligée à une association d'entreprises en tenant compte du chiffre d'affaires de ses membres réalisé au niveau mondial et que cette association n'est pas solvable, cette dernière est tenue de lancer à ses membres un appel à contributions pour couvrir le montant de l'amende.

Si ces contributions n'ont pas été versées à l'association d'entreprises dans un délai fixé par la Commission, celle-ci peut exiger le paiement de l'amende directement par toute entreprise dont les représentants étaient membres des organes décisionnels concernés de ladite association.

Après avoir exigé le paiement conformément au deuxième alinéa, la Commission peut, lorsque cela est nécessaire pour garantir le paiement intégral de l'amende, exiger le paiement du solde par l'un quelconque des membres de l'association d'entreprises.

Cependant, la Commission n'exige pas le paiement visé au deuxième ou au troisième alinéa auprès des entreprises qui démontrent qu'elles n'ont pas appliqué la décision de l'association d'entreprises qui enfreignait le présent règlement et que soit elles en ignoraient l'existence, soit elles s'en étaient activement désolidarisées avant que la Commission n'ouvre une procédure en vertu de l'article 20.

La responsabilité financière de chaque entreprise en ce qui concerne le paiement de l'amende ne peut excéder 20 % de son chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent.

Article 31
Astreintes

1. La Commission peut adopter une décision infligeant aux entreprises, y compris aux contrôleurs d'accès s'il y a lieu, et aux associations d'entreprises des astreintes jusqu'à concurrence de 5 % du chiffre d'affaires journalier moyen réalisé au niveau mondial au cours de l'exercice précédent par jour, à compter de la date qu'elle fixe dans sa décision, pour les contraindre:
a) à respecter les mesures précisées par la Commission dans une décision adoptée en vertu de l'article 8, paragraphe 2;
b) à respecter la décision prise en vertu de l'article 18, paragraphe 1;
c) à fournir des renseignements exacts et complets dans le délai requis par une demande de renseignements formulée par voie de décision en vertu de l'article 21;

d) à garantir l'accès aux données, algorithmes et renseignements concernant les essais en réponse à une demande faite en vertu de l'article 21, paragraphe 3, et à fournir des explications les concernant, tel qu'exigé par une décision prise en vertu de l'article 21;
e) à se soumettre à une inspection ordonnée par voie de décision prise en vertu de l'article 23;
f) à respecter une décision ordonnant des mesures provisoires prises en vertu de l'article 24;
g) à respecter des engagements rendus juridiquement obligatoires par décision en vertu de l'article 25, paragraphe 1;
h) à respecter une décision prise en application de l'article 29, paragraphe 1.

2. Lorsque les entreprises, ou associations d'entreprises, ont satisfait à l'obligation pour l'exécution de laquelle l'astreinte a été infligée, la Commission peut adopter un acte d'exécution fixant le montant définitif de l'astreinte à un chiffre inférieur à celui qui résulte de la décision initiale. Cet acte d'exécution est adopté en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

Article 32
Prescription en matière d'imposition de sanctions

1. Les pouvoirs conférés à la Commission en vertu des articles 30 et 31 sont soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où l'infraction a été commise. Toutefois, pour les infractions continues ou répétées, la prescription ne court qu'à compter du jour où l'infraction a pris fin.

3. La prescription en matière d'imposition d'amendes ou d'astreintes est interrompue par tout acte de la Commission visant à mener une enquête sur le marché ou à poursuivre l'infraction. L'interruption de la prescription prend effet le jour où l'acte est notifié à au moins une entreprise ou association d'entreprises ayant participé à l'infraction. Constituent notamment des actes interrompant la prescription:

a) les demandes de renseignements de la Commission;
b) les autorisations écrites d'effectuer des inspections délivrées par la Commission à ses agents;
c) l'ouverture d'une procédure par la Commission en application de l'article 20.

4. La prescription court à nouveau à partir de chaque interruption. Toutefois, la prescription est acquise au plus tard le jour où un délai égal au double du délai de prescription arrive à expiration sans que la Commission ait prononcé une amende ou astreinte. Ce délai est prolongé de la période pendant laquelle la prescription est suspendue conformément au paragraphe 5.

5. La prescription en matière d'imposition d'amendes ou d'astreintes est suspendue aussi longtemps que la décision de la Commission fait l'objet d'une procédure pendante devant la Cour de justice.

Article 33
Prescription en matière d'exécution des sanctions

1. Le pouvoir de la Commission d'exécuter les décisions prises en vertu des articles 30 et 31 est soumis à un délai de prescription de cinq ans.

2. La prescription court à compter du jour où la décision est devenue définitive.

3. La prescription en matière d'exécution des sanctions est interrompue:
a) par la notification d'une décision modifiant le montant initial de l'amende ou de l'astreinte ou rejetant une demande tendant à obtenir une telle modification; ou
b) par tout acte de la Commission ou d'un État membre, agissant à la demande de la Commission, visant au recouvrement forcé de l'amende ou de l'astreinte.

4. La prescription court à nouveau à partir de chaque interruption.

5. La prescription en matière d'exécution des sanctions est suspendue:
a) aussi longtemps qu'un délai de paiement est accordé; ou
b) aussi longtemps que l'exécution forcée du paiement est suspendue en vertu d'une décision de la Cour de justice ou d'une décision d'une juridiction nationale.

Article 34
Droit d'être entendu et droit d'accès au dossier

1. Avant d'adopter une décision au titre de l'article 8, de l'article 9, paragraphe 1, de l'article 10, paragraphe 1, des articles 17, 18, 24, 25, 29 et 30 et de l'article 31, paragraphe 2, la Commission donne au contrôleur d'accès ou à l'entreprise ou à l'association d'entreprises concerné l'occasion de faire connaître son point de vue sur:
a) les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et
b) les mesures que la Commission peut avoir l'intention de prendre au vu des constatations préliminaires visées au point a) du présent paragraphe.

2. Les contrôleurs d'accès, les entreprises et les associations d'entreprises concernés peuvent présenter à la Commission leurs observations en ce qui concerne les constatations préliminaires de la Commission dans un délai fixé par la Commission dans ses constatations préliminaires et qui ne peut être inférieur à 14 jours.

3. La Commission ne fonde ses décisions que sur les constatations préliminaires, y compris sur tout grief retenu par la Commission, au sujet desquelles les contrôleurs d'accès, les entreprises et les associations d'entreprises concernés ont pu faire valoir leurs observations.

4. Les droits de la défense du contrôleur d'accès, de l'entreprise ou de l'association d'entreprises concerné sont pleinement assurés dans le déroulement de la procédure. Le contrôleur d'accès, l'entreprise ou l'association d'entreprises concerné a le droit d'avoir accès au dossier de la Commission conformément aux modalités de divulgation, sous réserve de l'intérêt légitime des entreprises à ce que leurs secrets d'affaires ne soient pas divulgués. En cas de désaccord entre les parties, la Commission peut adopter des décisions fixant ces modalités de divulgation. Le droit d'accès au dossier de la Commission ne s'étend pas aux informations confidentielles et aux documents internes de la Commission ou des autorités compétentes des États membres. En particulier, le droit d'accès ne s'étend pas à la correspondance entre la Commission et les autorités compétentes des États membres. Aucune disposition du présent paragraphe n'empêche la Commission de divulguer et d'utiliser des informations nécessaires pour apporter la preuve d'une infraction.

Article 35
Rapports annuels

1. La Commission présente au Parlement européen et au Conseil un rapport annuel sur la mise en œuvre du présent règlement et sur les progrès accomplis dans la réalisation de ses objectifs.

2. Le rapport visé au paragraphe 1 comprend:
a) un résumé des activités de la Commission, y compris toute mesure ou décision adoptée et les enquêtes de marché en cours en rapport avec le présent règlement;

b) les constatations résultant du suivi de la mise en œuvre par les contrôleurs d'accès des obligations au titre du présent règlement;
c) une évaluation de la description ayant fait l'objet d'un audit visée à l'article 15;
d) une vue d'ensemble de la coopération entre la Commission et les autorités nationales dans le cadre du présent règlement;
e) un aperçu des activités et des tâches effectuées par le groupe de haut niveau des régulateurs numériques, y compris la manière dont ses recommandations concernant l'application du présent règlement doivent être mises en œuvre.

3. La Commission publie le rapport sur son site internet.

Article 36
Secret professionnel

1. Les informations recueillies en vertu du présent règlement sont utilisées aux fins de celui-ci.

2. Les informations recueillies en vertu de l'article 14 sont utilisées aux fins du présent règlement, du règlement (CE) no 139/2004 et des règles nationales en matière de concentration.

3. Les informations recueillies en vertu de l'article 15 sont utilisées aux fins du présent règlement et du règlement (UE) 2016/679.

4. Sans préjudice de l'échange et de l'utilisation des informations fournies aux fins d'utilisation selon les articles 38, 39, 41 et 43, la Commission, les autorités compétentes des États membres, leurs fonctionnaires, agents et les autres personnes travaillant sous la supervision de ces autorités, ainsi que toute personne physique ou morale, dont les auditeurs et experts nommés en vertu de l'article 26, paragraphe 2, sont tenus de ne pas divulguer les informations qu'ils ont recueillies ou échangées en application du présent règlement et qui, par leur nature, sont couvertes par le secret professionnel.

Article 37
Coopération avec les autorités nationales

1. La Commission et les États membres travaillent en étroite coopération et coordonnent leurs mesures d'exécution pour assurer une application cohérente, efficace et complémentaire des instruments juridiques disponibles appliqués aux contrôleurs d'accès au sens du présent règlement.

2. La Commission peut, le cas échéant, consulter les autorités nationales sur toute question relative à l'application du présent règlement.

Article 38
Coopération et coordination avec les autorités nationales compétentes chargées de faire appliquer les règles de concurrence

1. La Commission et les autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, coopèrent les unes avec les autres et s'échangent des informations sur leurs mesures d'exécution respectives par l'intermédiaire du Réseau européen de la concurrence (REC). Elles ont le pouvoir de se communiquer toute information relative à un élément de fait ou de droit, y compris s'il s'agit d'une information confidentielle. Si l'autorité compétente n'est pas membre du REC, la Commission établit les modalités nécessaires pour cette coopération et cet échange d'informations sur les dossiers concernant l'application du présent règlement et l'application des règles dans les cas visés à l'article 1er, paragraphe 6. La Commission peut établir ces modalités dans un acte d'exécution visé à l'article 46, paragraphe 1, point l).

2. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'ouvrir une enquête sur des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle informe la Commission par écrit de la première mesure d'enquête formelle, avant ou immédiatement après le début de cette mesure. Cette information peut également être mise à la disposition des autorités

nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

3. Lorsqu'une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, a l'intention d'imposer des obligations à des contrôleurs d'accès en application de dispositions législatives nationales visées à l'article 1er, paragraphe 6, elle communique le projet de mesure et ses motifs à la Commission, au plus tard 30 jours avant son adoption. Dans le cas de mesures provisoires, l'autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, communique à la Commission les projets de mesures envisagées dès que possible et au plus tard immédiatement après l'adoption de ces mesures. Cette information peut également être mise à la disposition des autorités nationales compétentes chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, des autres États membres.

4. Les mécanismes d'information prévus aux paragraphes 2 et 3 ne s'appliquent pas aux décisions envisagées en vertu des règles nationales en matière de concentrations.

5. Les informations échangées en vertu des paragraphes 1 à 3 du présent article ne sont échangées et utilisées qu'aux fins de la coordination de l'application du présent règlement et des règles visées à l'article 1er, paragraphe 6.

6. La Commission peut demander aux autorités nationales compétentes des États membres chargées de faire appliquer les règles visées à l'article 1er, paragraphe 6, de soutenir toute enquête de marché qu'elle mène en application du présent règlement.

7. Lorsque, en vertu du droit national, une autorité nationale compétente d'un État membre chargée de faire appliquer les règles visées à l'article 1er, paragraphe 6, dispose de la compétence et des pouvoirs d'enquête voulus, elle peut, de sa propre initiative, mener une enquête sur un cas de non-respect éventuel des articles 5, 6 et 7 du présent règlement sur son territoire. Avant de prendre une première mesure d'enquête formelle, cette autorité en informe la Commission par écrit.

RGPD

L'ouverture d'une procédure par la Commission en vertu de l'article 20 enlève aux autorités nationales compétentes des États membres chargées de contrôler le respect des règles visées à l'article 1er, paragraphe 6, la possibilité de mener une telle enquête ou de la clôturer lorsqu'elle est déjà en cours. Ces autorités communiquent à la Commission les résultats de l'enquête en question afin d'appuyer la Commission dans son rôle de seule instance habilitée à faire appliquer le présent règlement.

Article 39
Coopération avec les juridictions nationales

1. Dans le cadre des procédures engagées pour l'application du présent règlement, les juridictions nationales peuvent demander à la Commission de leur transmettre des informations en sa possession ou son avis sur des questions relatives à l'application du présent règlement.

2. Les États membres transmettent à la Commission une copie de toute décision écrite des juridictions nationales statuant sur l'application du présent règlement. Cette copie est transmise sans tarder lorsque le jugement complet est notifié par écrit aux parties.

3. Lorsqu'une application cohérente du présent règlement l'exige, la Commission, agissant de sa propre initiative, peut présenter des observations écrites aux juridictions nationales. Avec l'autorisation de la juridiction concernée, elle peut aussi présenter des observations orales.

4. Aux seules fins de l'élaboration de ses observations, la Commission peut demander à la juridiction nationale concernée de lui transmettre ou de lui faire transmettre tout document nécessaire à l'appréciation de l'affaire.

5. Les juridictions nationales ne prennent aucune décision qui va à l'encontre d'une décision adoptée par la Commission en vertu du présent règlement. Elles évitent également de prendre des décisions qui iraient à l'encontre d'une décision envisagée par la Commission dans une procédure qu'elle a intentée en vertu du présent règlement. À

cette fin, la juridiction nationale peut évaluer s'il est nécessaire de suspendre sa procédure. Cette disposition est sans préjudice de la possibilité qu'ont les juridictions nationales d'introduire une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.

Article 40
Le groupe de haut niveau

1. La Commission met en place un groupe de haut niveau pour le règlement sur les marchés numériques (ci-après dénommé « groupe de haut niveau »).

2. Le groupe de haut niveau se compose des organes et réseaux européens suivants:
a) l'organe des régulateurs européens des communications électroniques,
b) le Contrôleur européen de la protection des données et le comité européen de la protection des données,
c) le réseau européen de la concurrence,
d) le réseau de coopération en matière de protection des consommateurs, et
e) le groupe des régulateurs européens pour les services de médias audiovisuels.

3. Les organes et réseaux européens visés au paragraphe 2 ont chacun un nombre égal de représentants au sein du groupe de haut niveau. Le nombre maximal de membres du groupe de haut niveau ne dépasse pas trente personnes.

4. La Commission fournit des services de secrétariat au groupe de haut niveau afin de faciliter ses travaux. Le groupe de haut niveau est présidé par la Commission, qui participe à ses réunions. Le groupe de haut niveau se réunit à la demande de la Commission au moins une fois par année civile. La Commission convoque également une réunion du groupe à la demande de la majorité des membres qui le composent afin de traiter une question spécifique.

5. Le groupe de haut niveau peut fournir à la Commission des conseils et une expertise dans les domaines relevant de la compétence de ses membres, notamment:
a) des conseils et des recommandations relevant de leur expertise et présentant un intérêt pour toute question générale quant à la mise en œuvre ou à l'application du présent règlement; ou
b) des conseils et une expertise en faveur d'une approche réglementaire cohérente entre les différents instruments réglementaires.

6. Le groupe de haut niveau peut, en particulier, recenser et évaluer les interactions actuelles et potentielles entre le présent règlement et les règles sectorielles appliquées par les autorités nationales composant les organismes et réseaux européens visés au paragraphe 2 et soumettre à la Commission un rapport annuel présentant cette évaluation et recensant les éventuels problèmes transréglementaires. Ce rapport peut être accompagné de recommandations visant à converger vers des approches transdisciplinaires cohérentes et des synergies entre la mise en œuvre du présent règlement et celle d'autres réglementations sectorielles. Ce rapport est communiqué au Parlement européen et au Conseil.

7. Dans le cadre d'enquêtes de marché sur de nouveaux services et de nouvelles pratiques, le groupe de haut niveau peut apporter son expertise à la Commission sur la nécessité de modifier, d'ajouter ou de supprimer des règles figurant dans le présent règlement afin de faire en sorte que les marchés numériques dans l'ensemble de l'Union soient contestables et équitables.

Article 41
Demande d'enquête de marché

1. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 17 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner qu'une entreprise devrait être désignée comme contrôleur d'accès.

2. Un ou plusieurs États membres peuvent demander à la Commission d'ouvrir une enquête de marché conformément à l'article 18 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner qu'un contrôleur d'accès a systématiquement contrevenu à une ou plusieurs des obligations prévues aux articles 5, 6 et 7, et qu'il a

maintenu, renforcé ou étendu sa position de contrôleur d'accès au regard des caractéristiques énoncées à l'article 3, paragraphe 1.

3. Trois États membres ou plus peuvent solliciter auprès de la Commission l'ouverture d'une enquête de marché conformément à l'article 19 parce qu'il existe, selon eux, des motifs raisonnables de soupçonner:
a) qu'il faudrait ajouter davantage de services relevant du secteur numérique à la liste des services de plateforme essentiels établie à l'article 2, point 2); ou
b) que le présent règlement ne permet pas de remédier de manière effective à une ou plusieurs pratiques et que ces pratiques sont susceptibles de limiter la contestabilité des service de plateforme essentiels ou d'être inéquitables.

4. Les États membres apportent des éléments de preuve à l'appui de leurs demandes introduites en vertu des paragraphes 1, 2 et 3. Pour les demandes introduites en vertu du paragraphe 3, ces éléments de preuve peuvent inclure des informations sur les offres nouvelles de produits, de services, de logiciels ou de fonctionnalités qui suscitent des préoccupations du point de vue de la contestabilité ou de l'équité, qu'elles soient mises en œuvre dans le cadre de services de plateforme essentiels existants ou d'une autre façon.

5. Dans les quatre mois suivant la réception d'une demande introduite en vertu du présent article, la Commission examine s'il existe des motifs raisonnables pour ouvrir une enquête de marché en vertu du paragraphe 1, 2 ou 3. La Commission publie les résultats de cette évaluation.

Article 42
Actions représentatives

La directive (UE) 2020/1828 est applicable aux actions représentatives intentées en raison des infractions commises par des contrôleurs d'accès aux dispositions du présent règlement qui portent atteinte ou risquent de porter atteinte aux intérêts collectifs des consommateurs.

Article 43
Signalement de violations et protection des auteurs de signalement

Le signalement de toutes les violations du présent règlement et la protection des personnes signalant ces violations sont régis par la directive (UE) 2019/1937.

CHAPITRE VI
DISPOSITIONS FINALES

Article 44
Publication des décisions

1. La Commission publie les décisions qu'elle prend au titre des articles 3 et 4, de l'article 8, paragraphe 2, des articles 9, 10, 16 à 20 et 24, de l'article 25, paragraphe 1, et des articles 29, 30 et 31. Cette publication mentionne le nom des parties intéressées et l'essentiel de la décision, y compris les sanctions imposées.

2. La publication tient compte de l'intérêt légitime des contrôleurs d'accès ou des tiers à ce que leurs informations confidentielles ne soient pas divulguées.

Article 45
Contrôle de la Cour de justice

Conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, la Cour de justice statue avec compétence de pleine juridiction sur les recours dirigés contre les décisions par lesquelles la Commission inflige des amendes ou des astreintes. Elle peut supprimer, réduire ou majorer l'amende ou l'astreinte infligée.

Article 46
Dispositions d'exécution

1. La Commission peut adopter des actes d'exécution établissant les modalités détaillées pour l'application de ce qui suit:

a) la forme, la teneur et les autres modalités des notifications et communications d'informations en application de l'article 3;
b) la forme, la teneur et les autres modalités des mesures techniques que les contrôleurs d'accès mettent en œuvre pour garantir le respect de l'article 5, 6 ou 7;
c) les modalités opérationnelles et techniques en vue de la mise en œuvre de l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation conformément à l'article 7;
d) la forme, la teneur et les autres modalités de la demande motivée présentée en application de l'article 8, paragraphe 3;
e) la forme, la teneur et les autres modalités des demandes motivées présentées en application des articles 9 et 10;
f) la forme, la teneur et les autres modalités des rapports réglementaires communiqués en application de l'article 11;
g) la méthodologie et la procédure pour la description, devant faire l'objet d'un audit, des techniques utilisées pour le profilage des consommateurs prévue à l'article 15, paragraphe 1; lorsqu'elle élabore un projet d'acte d'exécution à cette fin, la Commission consulte le Contrôleur européen de la protection des données et peut consulter le comité européen de la protection des données, la société civile et d'autres experts compétents;
h) la forme, la teneur et les autres modalités des notifications et communications d'informations en application des articles 14 et 15;
i) les modalités des procédures relatives aux enquêtes de marché prévues aux articles 17, 18 et 19 et des procédures définies aux articles 24, 25 et 29;
j) les modalités d'exercice du droit d'être entendu prévu à l'article 34;
k) les modalités pour les conditions de la divulgation prévue à l'article 34;
l) les modalités de la coopération et de la coordination entre la Commission et les autorités nationales prévues aux articles 37 et 38; et
m) les modalités de calcul et de prolongation des délais.

2. Les actes d'exécution visés au paragraphe 1, points a) à k) et m), du présent article sont adoptés en conformité avec la procédure consultative visée à l'article 50, paragraphe 2.

L'acte d'exécution visé au paragraphe 1, point l), du présent article est adopté en conformité avec la procédure d'examen visée à l'article 50, paragraphe 3.

3. Avant l'adoption de tout acte d'exécution en vertu du paragraphe 1, la Commission en publie le projet et invite toutes les parties intéressées à lui soumettre leurs observations dans un délai qui ne peut être inférieur à un mois.

Article 47
Lignes directrices

La Commission peut adopter des lignes directrices sur tout aspect du présent règlement afin de faciliter sa mise en œuvre et son application effectives.

Article 48
Normalisation

Si elle le juge opportun et nécessaire, la Commission peut charger les organisations européennes de normalisation d'élaborer des normes appropriées pour faciliter la mise en œuvre des obligations fixées dans le présent règlement.

Article 49
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, est conféré à la Commission pour une période de cinq ans à compter du 1er novembre 2022. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 3, paragraphes 6 et 7, et à l'article 12, paragraphes 1, 3 et 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 « Mieux légiférer ».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 3, paragraphes 6 et 7, et de l'article 12, paragraphes 1, 3 et 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 50
Comité

1. La Commission est assistée par un comité (ci-après dénommé « comité consultatif en matière de marchés numériques »). Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) no 182/2011 s'applique.

Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai pour émettre un avis, le président du comité le décide ou une majorité simple des membres du comité le demandent.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

4. La Commission fait part au destinataire d'une décision individuelle de l'avis du comité, accompagné de cette décision. Elle rend publics l'avis et la décision individuelle, en tenant compte de l'intérêt légitime à la protection du secret professionnel.

Article 51
Modification de la directive (UE) 2019/1937

À la partie I, point J, de l'annexe de la directive (UE) 2019/1937, le point suivant est ajouté:
« iv) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1). ».

Article 52
Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:
« 67) Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 21.9.2022, p. 1). ».

Article 53
Réexamen

1. Au plus tard le 3 mai 2026, et tous les trois ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen, au Conseil et au Comité économique et social.

2. Les évaluations déterminent si les objectifs du présent règlement consistant à garantir que les marchés soient contestables et équitables ont été atteints, et elles mesurent l'incidence du présent règlement pour les entreprises utilisatrices, notamment les PME, et les utilisateurs finaux. De plus, la Commission évalue si le champ de l'article 7 peut être élargi aux services de réseaux sociaux en ligne.
3. Les évaluations déterminent s'il est nécessaire de modifier les règles, notamment en ce qui concerne la liste des services de plateforme essentiels établie à l'article 2, point 2), les obligations prévues aux articles 5, 6 et 7 et le contrôle de leur respect, afin de garantir la contestabilité et l'équité des marchés numériques dans l'Union. À la suite des évaluations, la Commission prend les mesures appropriées, qui peuvent comprendre des propositions législatives.
4. Les autorités compétentes des États membres communiquent toutes les informations pertinentes dont elles disposent que la Commission pourrait solliciter aux fins de l'établissement du rapport visé au paragraphe 1.

Article 54
Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. Il est applicable à partir du 2 mai 2023.
Cependant, l'article 3, paragraphes 6 et 7, ainsi que les articles 40, 46, 47, 48, 49 et 50 sont applicables à partir du 1er novembre 2022, et les articles 42 et 43 sont applicables à partir du 25 juin 2023.
Toutefois, si la date du 25 juin 2023 précède la date d'application visée au deuxième alinéa du présent article, l'application des articles 42 et 43 est repoussée à la date d'application visée au deuxième alinéa du présent article.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 14 septembre 2022

Par le Parlement européen La présidente
R. METSOLA

Par le Conseil Le président
M. BEK

ANNEXE

A. Généralités

1. La présente annexe vise à préciser la méthode d'identification et de calcul des « utilisateurs finaux actifs » et des « entreprises utilisatrices actives » pour chaque service de plateforme essentiel énumérés à l'article 2, point 2). Elle fournit une référence permettant à une entreprise d'évaluer si ses services de plateforme essentiels respectent les seuils quantitatifs fixés à l'article 3, paragraphe 2, point b), et sont donc présumés satisfaire à l'exigence énoncée à l'article 3, paragraphe 1, point b). Cette référence sera donc également pertinente pour toute appréciation plus large au titre de l'article 3, paragraphe 8. Il incombe à l'entreprise de parvenir à la meilleure estimation possible, conformément aux principes communs et à la méthode spécifique énoncés dans la présente annexe. Aucune disposition de la présente annexe n'empêche la Commission, dans les délais fixés par les dispositions pertinentes du présent règlement,

d'exiger de l'entreprise fournissant des services de plateforme essentiels qu'elle fournisse toutes les informations nécessaires pour identifier les « utilisateurs finaux actifs » et les « entreprises utilisatrices actives » et en calculer le nombre. Aucune disposition de la présente annexe ne devrait constituer une base juridique pour le traçage des utilisateurs. La méthode figurant dans la présente annexe est également sans préjudice de l'une quelconque des obligations fixées par le présent règlement, notamment celles énoncées à l'article 3, paragraphes 3 et 8, et à l'article 13, paragraphe 3. En particulier, le respect de l'article 13, paragraphe 3, signifie également qu'il convient d'identifier les « utilisateurs finaux actifs » et les « entreprises utilisatrices actives » et d'en calculer le nombre sur la base d'une mesure précise ou de la meilleure estimation possible, conformément aux capacités réelles d'identification et de calcul dont dispose au moment voulu l'entreprise fournissant des services de plateforme essentiels. Ces mesures ou la meilleure estimation possible doivent être cohérentes avec les informations communiquées en vertu de l'article 15 et les inclure.

2. À l'article 2, les points 20) et 21) énoncent les définitions d'« utilisateur final » et d'« entreprise utilisatrice », qui sont communes à tous les services de plateforme essentiels.

3. Afin d'identifier les « utilisateurs finaux actifs » et les « entreprises utilisatrices actives » et d'en calculer le nombre, la présente annexe fait référence à la notion d'« utilisateurs uniques ». La notion d'« utilisateurs uniques » recouvre les
« utilisateurs finaux actifs » et les « entreprises utilisatrices actives » comptabilisés une seule fois, pour le service de plateforme essentiel concerné, pour une période donnée (c'est-à-dire par mois dans le cas des « utilisateurs finaux actifs » et par année dans le cas des « entreprises utilisatrices actives »), indépendamment du nombre de leurs interactions avec le service de plateforme essentiel concerné au cours de cette période. Cela est sans préjudice du fait que la même personne physique ou morale peut simultanément constituer un « utilisateur final actif » ou une « entreprise utilisatrice active » pour différents services de plateforme essentiels.

B. « Utilisateurs finaux actifs »

1. Le nombre d'« utilisateurs uniques » au regard des « utilisateurs finaux actifs » est établi en fonction de la mesure la plus précise déclarée par l'entreprise fournissant l'un des services de plateforme essentiels, en particulier:
a) On considère que la collecte de données sur l'utilisation des services de plateforme essentiels à partir d'environnements fonctionnant par inscription ou connexion présenterait, à première vue, le risque le plus faible de duplication, par exemple concernant le comportement des utilisateurs sur l'ensemble des appareils ou des plateformes. Par conséquent, l'entreprise soumet des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques par service de plateforme essentiel concerné sur la base des environnements fonctionnant par inscription ou connexion, si de telles données existent.
b) Dans le cas des services de plateforme essentiels auxquels des utilisateurs finaux ont également accès en dehors des environnements fonctionnant par inscription ou connexion, l'entreprise soumet en outre des données anonymisées agrégées sur le nombre d'utilisateurs finaux uniques du service de plateforme essentiel concerné, sur la base d'une autre mesure prenant en compte également les utilisateurs finaux en dehors des environnements fonctionnant par inscription ou connexion, tels que les adresses de protocole internet, les témoins de connexion (cookies) ou d'autres identifiants tels que les étiquettes d'identification par radiofréquence, pour autant que ces adresses ou témoins de connexion soient objectivement nécessaires à la fourniture de services de plateforme essentiels.

2. Le nombre d'« utilisateurs finaux actifs par mois » est fondé sur le nombre moyen d'utilisateurs finaux actifs chaque mois durant la majeure partie de l'exercice. La notion de « majeure partie de l'exercice » vise à permettre à une entreprise fournissant des services de plateforme essentiels d'écarter des valeurs exceptionnelles au cours d'une année donnée. On

entend par valeurs exceptionnelles celles qui sortent nettement de ce qui ressort de l'ordinaire et du prévisible. Une situation où, de manière inattendue, au cours d'un seul mois de l'exercice, la participation des utilisateurs atteindrait un niveau record ou connaîtrait une forte baisse est un exemple de ce qui pourrait constituer de telles valeurs exceptionnelles. Les valeurs en rapport avec des événements intervenant

chaque année, tels que les promotions annuelles des ventes, ne constituent pas des valeurs exceptionnelles.

C. « Entreprises utilisatrices actives »

Le nombre d'« utilisateurs uniques » au regard des « entreprises utilisatrices actives » doit être déterminé, s'il y a lieu, au niveau du compte, chaque compte d'entreprise distinct, associé à l'utilisation d'un service de plateforme essentiel fourni par l'entreprise, constituant une entreprise utilisatrice unique de ce service de plateforme essentiel. Si la notion de
« compte d'entreprise » ne s'applique pas à un service de plateforme essentiel donné, l'entreprise concernée fournissant des services de plateforme essentiels détermine le nombre d'entreprises utilisatrices uniques en se référant à l'entreprise concernée.

D. Communication d'informations

1. L'entreprise qui communique à la Commission, conformément à l'article 3, paragraphe 3, des informations concernant le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives par service de plateforme essentiel est chargée de veiller à l'exhaustivité et à l'exactitude de ces informations. À cet égard:
a) l'entreprise est tenue de transmettre les données pour un service de plateforme essentiel donné en évitant de sous- évaluer ou de surévaluer le nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives (par exemple, lorsque les utilisateurs accèdent aux services de plateforme essentiels à partir de différentes plateformes ou de différents appareils);
b) l'entreprise est tenue de fournir des explications précises et succinctes sur la méthode utilisée pour obtenir les informations fournies et elle est responsable de tout risque de sous-évaluation ou de surévaluation du nombre d'utilisateurs finaux actifs et d'entreprises utilisatrices actives pour un service de plateforme essentiel donné et des solutions adoptées pour remédier à ce risque;
c) l'entreprise fournit des données basées sur une autre méthode de mesure lorsque la Commission a des doutes quant à l'exactitude des données fournies par l'entreprise fournissant les services de plateforme essentiels.

2. Aux fins du calcul du nombre d'« utilisateurs finaux actifs » et d'« entreprises utilisatrices actives »:
a) l'entreprise fournissant un ou des services de plateforme essentiels ne répertorie pas les services de plateforme essentiels appartenant à une même catégorie de services de plateforme essentiels définis à l'article 2, point 2), comme étant distincts en se basant principalement sur le fait qu'ils sont fournis en utilisant des noms de domaine différents, qu'il s'agisse de domaines de premier niveau nationaux (ccTLD) ou de domaines de premier niveau génériques (gTLD), ou sur tout attribut géographique;
b) l'entreprise fournissant un ou des services de plateforme essentiels considère comme distincts les services de plateforme essentiels qui sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s'ils appartiennent à la même catégorie de services de plateforme essentiels définis à l'article 2, point 2);
c) l'entreprise fournissant un ou des services de plateforme essentiels considère comme étant des services de plateforme essentiels distincts les services que l'entreprise concernée propose de manière intégrée, mais qui:
i) n'appartiennent pas à la même catégorie de services de plateforme essentiels définis à l'article 2, point 2), ou
ii) sont utilisés à des fins différentes soit par leurs utilisateurs finaux, soit par leurs entreprises utilisatrices, soit encore par les deux, même si leurs utilisateurs finaux ou leurs entreprises utilisatrices peuvent être identiques et même s'ils appartiennent à la même catégorie de services de plateforme essentiels en vertu de l'article 2, point 2).

E. « Définitions spécifiques »

Le tableau ci-dessous contient des définitions spécifiques des notions d'« utilisateurs finaux actifs » et d'« entreprises utilisatrices actives » pour chaque service de plateforme essentiel.

Services de plateforme essentiels	Utilisateurs finaux actifs	Entreprises utilisatrices actives
Services d'intermédiation en ligne	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le service d'intermédiation en ligne, par exemple en se connectant, en effectuant une recherche, en cliquant ou en utilisant le défilement de manière active, ou qui, au moins une fois pendant le mois, ont conclu une transaction via le service d'intermédiation en ligne.	Nombre d'entreprises utilisatrices uniques dont au moins un article a figuré sur une liste dans le service d'intermédiation en ligne pendant toute l'année ou qui, pendant l'année, ont conclu une transaction rendue possible par le service d'intermédiation en ligne.
Moteurs de recherche en ligne	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le moteur de recherche en ligne, par exemple en effectuant une recherche.	Nombre d'entreprises utilisatrices uniques disposant de sites internet commerciaux (c'est-à-dire de sites internet utilisés à des fins commerciales ou professionnelles) qui sont indexés par le moteur de recherche en ligne ou font partie de l'index du moteur de recherche en ligne pendant l'année.
Services de réseaux sociaux en ligne	Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de réseau social en ligne au moins une fois pendant le mois, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en lançant une recherche, en publiant ou en commentant, de manière active.	Nombre d'entreprises utilisatrices uniques qui sont inscrites sur la liste d'entreprises ou disposent d'un compte d'entreprise dans le service de réseau social en ligne et qui ont interagi avec le service, de quelque manière que ce soit, au moins une fois pendant l'année, par exemple en se connectant, en ouvrant une page, en utilisant le défilement, en cliquant, en utilisant la fonction «Like/J'aime», en effectuant une recherche, en publiant, en commentant ou en utilisant ses outils pour les entreprises, de manière active.
Services de plateformes de partage de vidéos	Nombre d'utilisateurs finaux uniques qui ont interagi avec le service de plateforme de partage de vidéos au moins une fois pendant le mois, par exemple en diffusant un segment de contenu audiovisuel, en effectuant une recherche ou en téléchargeant un contenu audiovisuel vers la plateforme, y compris des vidéos créées par les utilisateurs.	Nombre d'entreprises utilisatrices uniques qui, pendant l'année, ont fourni au moins un contenu audiovisuel téléchargé vers le service de la plateforme de partage de vidéos ou diffusé sur celle-ci.
Services de communications interpersonnelles non fondés sur la numérotation	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont lancé d'une manière ou d'une autre une communication ou y ont participé par l'intermédiaire du service de communications interpersonnelles non fondé sur la numérotation.	Nombre d'entreprises utilisatrices uniques qui, au moins une fois pendant l'année, ont utilisé un compte d'entreprise ou qui ont, de n'importe quelle autre manière, lancé une communication ou, de quelque façon que ce soit, y ont participé par l'intermédiaire du service de communication interpersonnelle non fondé sur la numérotation pour communiquer directement avec un utilisateur final.
Systèmes d'exploitation	Nombre d'utilisateurs finaux uniques qui ont utilisé un dispositif équipé du système d'exploitation ayant été activé, mis à jour ou utilisé au moins une fois pendant le mois.	Nombre de développeurs uniques qui, pendant l'année, ont publié, mis à jour ou proposé au moins une application ou un programme logiciel utilisant le langage de programmation ou tout outil de développement logiciel du système d'exploitation ou fonctionnant de quelque manière que ce soit sur le système d'exploitation.

Services de plateforme essentiels	Utilisateurs finaux actifs	Entreprises utilisatrices actives
Assistant virtuel	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec l'assistant virtuel de quelque manière que ce soit, par exemple en l'activant, en posant une question, en accédant à un service par une commande ou en contrôlant un dispositif de maison intelligente.	Nombre de développeurs uniques qui, au cours de l'année, ont proposé au moins une application logicielle d'assistant virtuel ou une fonctionnalité permettant de rendre une application logicielle existante accessible par l'intermédiaire de l'assistant virtuel.
Navigateurs internet	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec le navigateur internet, par exemple en insérant une requête ou une adresse de site internet dans la ligne URL du navigateur internet.	Nombre d'entreprises utilisatrices uniques dont les sites internet d'entreprise (c'est-à-dire les sites internet utilisés à des fins commerciales ou professionnelles) ont, au moins une fois pendant le mois, été consultés par l'intermédiaire du navigateur internet ou qui ont proposé un plug-in, une extension ou des outils complémentaires utilisés sur le navigateur internet au cours de l'année.
Services d'informatique en nuage	Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont interagi avec des services d'informatique en nuage fournis par le fournisseur concerné de services d'informatique en nuage, en échange de tout type de rémunération, que celle-ci ait eu lieu ou non le même mois.	Nombre d'entreprises utilisatrices uniques qui, au cours de l'année, ont fourni tout service d'informatique en nuage hébergé dans l'infrastructure en nuage du fournisseur de services d'informatique en nuage concerné.
Services de publicité en ligne	Pour les ventes propriétaires d'espaces publicitaires: Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité. Pour les services d'intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d'intermédiation publicitaire): Nombre d'utilisateurs finaux uniques qui, au moins une fois pendant le mois, ont été exposés à une publicité ayant déclenché le service d'intermédiation publicitaire.	Pour les ventes propriétaires d'espaces publicitaires: Nombre d'annonceurs uniques dont au moins une publicité a été exposée pendant l'année. Pour les services d'intermédiation publicitaire (y compris les réseaux publicitaires, les échanges publicitaires et tout autre service d'intermédiation publicitaire): Nombre d'entreprises utilisatrices uniques (y compris les annonceurs, les éditeurs ou d'autres intermédiaires) qui, au cours de l'année, ont interagi via le service d'intermédiation publicitaire ou ont eu recours à ses services.

DSA

DSA

RÈGLEMENT (UE) 2022/2065 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 19 octobre 2022

relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne, après transmission du projet d'acte législatif aux parlements nationaux, vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

statuant conformément à la procédure législative ordinaire[3],

considérant ce qui suit:

(1) Les services de la société de l'information et surtout les services intermédiaires sont devenus une composante importante de l'économie de l'Union et de la vie quotidienne des citoyens de l'Union. Vingt ans après l'adoption du cadre juridique existant applicable à ces services, établi par la directive 2000/31/CE du Parlement européen et du Conseil[4], des services et des modèles économiques nouveaux et innovants, tels que les réseaux sociaux et les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ont permis aux utilisateurs professionnels et aux consommateurs de transmettre et d'accéder à l'information et d'effectuer des transactions de manière inédite. Une majorité de citoyens de l'Union utilise désormais ces services au quotidien. Toutefois, la transformation numérique et l'utilisation accrue de ces services ont également engendré de nouveaux risques et défis pour les différents destinataires des services concernés, pour les entreprises et pour la société dans son ensemble.

(2) De plus en plus, les États membres adoptent ou envisagent d'adopter des législations nationales sur les matières relevant du présent règlement, imposant notamment des obligations de diligence aux fournisseurs de services intermédiaires en ce qui concerne la manière dont ils devraient combattre les contenus illicites, la désinformation en ligne ou d'autres risques pour la société. Étant donné le caractère intrinsèquement transfrontière de l'internet, qui est généralement utilisé pour fournir ces services, ces législations nationales divergentes ont une incidence négative sur le marché intérieur qui, en vertu de l'article 26 du traité sur le fonctionnement de l'Union euro-

1. JO C 286 du 16.7.2021, p. 70.
2. JO C 440 du 29.10.2021, p. 67.
3. Position du Parlement européen du 5 juillet 2022 (non encore parue au Journal officiel) et décision du Conseil du 4 octobre 2022.
4. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») (JO L 178 du 17.7.2000, p. 1).

péenne, comporte un espace sans frontières intérieures dans lequel la libre circulation des marchandises et des services et la liberté d'établissement sont assurées. Les conditions de la prestation de services intermédiaires dans l'ensemble du marché intérieur devraient être harmonisées, de manière à permettre aux entreprises d'accéder à de nouveaux marchés et à de nouvelles possibilités d'exploiter les avantages du marché intérieur, tout en offrant un choix plus étendu aux consommateurs et aux autres destinataires des services. Les utilisateurs professionnels, les consommateurs et les autres utilisateurs sont considérés comme étant des «destinataires du service» aux fins du présent règlement.

(3) Un comportement responsable et diligent des fournisseurs de services intermédiaires est indispensable pour assurer un environnement en ligne sûr, prévisible et fiable et pour permettre aux citoyens de l'Union et aux autres personnes d'exercer leurs droits fondamentaux garantis par la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), en particulier la liberté d'expression et d'information, la liberté d'entreprise, le droit à la non-discrimination et la garantie d'un niveau élevé de protection des consommateurs.

(4) Par conséquent, afin de préserver et d'améliorer le fonctionnement du marché intérieur, il convient d'établir un ensemble ciblé de règles obligatoires uniformes, efficaces et proportionnées au niveau de l'Union. Le présent règlement crée les conditions nécessaires à l'émergence et au développement de services numériques innovants dans le marché intérieur. Le rapprochement des mesures réglementaires nationales au niveau de l'Union relatives aux exigences applicables aux fournisseurs de services intermédiaires est nécessaire pour éviter et éliminer la fragmentation du marché intérieur et pour assurer la sécurité juridique, en réduisant par là même l'incertitude pour les développeurs et en favorisant l'interopérabilité. Grâce à des exigences neutres sur le plan technologique, l'innovation ne devrait pas être entravée, mais au contraire stimulée.

(5) Le présent règlement devrait s'appliquer aux fournisseurs de certains services de la société de l'information tels qu'ils sont définis dans la directive (UE) 2015/1535 du Parlement européen et du Conseil[5], c'est-à-dire tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire. Plus particulièrement, le présent règlement devrait s'appliquer aux fournisseurs de services intermédiaires, et notamment de services intermédiaires consistant en des services dits de «simple transport», de «mise en cache» et d'«hébergement», dès lors que la croissance exponentielle du recours à ces services, principalement à des fins légitimes et socialement bénéfiques de toute nature, a également accru leur rôle dans l'intermédiation et la diffusion d'informations et d'activités illégales ou susceptibles de nuire.

(6) Dans la pratique, certains fournisseurs de services intermédiaires assurent une prestation d'intermédiaire pour des services qui peuvent ou non être fournis par voie électronique, tels que des services informatiques à distance ou des services de transport, de logement ou de livraison. Le présent règlement ne devrait s'appliquer qu'aux services intermédiaires et ne devrait pas porter atteinte aux exigences énoncées dans le droit de l'Union ou le droit national concernant les produits ou services fournis par le biais de services intermédiaires, y compris dans les situations où le service intermédiaire fait partie intégrante d'un autre service qui n'est pas un service intermédiaire, comme cela est établi dans la jurisprudence de la Cour de justice de l'Union européenne.

Extraterritorialité

(7) Afin de garantir l'efficacité des règles établies dans le présent règlement et l'existence de conditions de concurrence équitables au sein du marché intérieur, ces règles devraient s'appliquer aux fournisseurs de services intermédiaires, quel que soit leur lieu d'établissement ou leur situation géographique, dans la mesure où ils proposent des services dans l'Union, pour autant qu'un lien étroit avec l'Union soit avéré.

(8) Il y a lieu de considérer qu'un tel lien étroit avec l'Union existe lorsque le fournisseur de services dispose d'un établissement dans l'Union ou, dans le cas contraire,

5. Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

lorsque le nombre de destinataires du service dans un ou plusieurs États membres est significatif au regard de leur population ou sur la base du ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités sur un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet ou ces États membres, la possibilité de commander des produits ou des services, ou l'utilisation d'un domaine de premier niveau pertinent. Le ciblage des activités sur un État membre pourrait également se déduire de la disponibilité d'une application dans la boutique d'applications nationale concernée, de la diffusion de publicités à l'échelle locale ou dans une langue utilisée dans cet État membre, ou de la gestion des relations avec la clientèle, par exemple de la fourniture d'un service clientèle dans une langue utilisée généralement dans cet État membre. Un lien étroit devrait également être présumé lorsqu'un fournisseur de services dirige ses activités vers un ou plusieurs États membres au sens de l'article 17, paragraphe 1, point c), du règlement (UE) n° 1215/2012 du Parlement européen et du Conseil[6]. En revanche, la simple accessibilité technique d'un site internet à partir de l'Union ne peut, pour ce seul motif, être considérée comme établissant un lien étroit avec l'Union.

(9) Le présent règlement harmonise pleinement les règles applicables aux services intermédiaires dans le marché intérieur dans le but de garantir un environnement en ligne sûr, prévisible et de confiance, en luttant contre la diffusion de contenus illicites en ligne et contre les risques pour la société que la diffusion d'informations trompeuses ou d'autres contenus peuvent produire, et dans lequel les droits fondamentaux consacrés par la Charte sont efficacement protégés et l'innovation est facilitée. En conséquence, les États membres ne devraient pas adopter ou maintenir des exigences nationales supplémentaires concernant les matières relevant du champ d'application du présent règlement, sauf si le présent règlement le prévoit expressément, car cela porterait atteinte à l'application directe et uniforme des règles pleinement harmonisées applicables aux fournisseurs de services intermédiaires conformément aux objectifs du présent règlement. Cela ne devrait pas empêcher l'application éventuelle d'une autre législation nationale applicable aux fournisseurs de services intermédiaires, dans le respect du droit de l'Union, y compris la directive 2000/31/CE, et notamment son article 3, lorsque les dispositions du droit national poursuivent d'autres objectifs légitimes d'intérêt général que ceux poursuivis par le présent règlement.

(10) Il convient que le présent règlement soit sans préjudice d'autres actes du droit de l'Union régissant la fourniture de services de la société de l'information en général, régissant d'autres aspects de la fourniture de services intermédiaires dans le marché intérieur ou précisant et complétant les règles harmonisées énoncées dans le présent règlement, tels que la directive 2010/13/UE du Parlement européen et du Conseil[7], y compris les dispositions de ladite directive concernant les plateformes de partage de vidéos, les règlements (UE) 2019/1148[8], (UE) 2019/1150[9], (UE) 2021/784[10] et (UE) 2021/1232[11] du Parlement européen et du Conseil et la directive 2002/58/CE du Parlement européen et du Conseil[12] et les dispositions du droit de l'Union énoncées dans un

6. Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO L 351 du 20.12.2012, p. 1).
7. Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels») (JO L 95 du 15.4.2010, p. 1).
8. Règlement (UE) 2019/1148 du Parlement européen et du Conseil du 20 juin 2019 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs, modifiant le règlement (CE) n° 1907/2006 et abrogeant le règlement (UE) n° 98/2013 (JO L 186 du 11.7.2019, p. 1).
9. Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).
10. Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (JO L 172 du 17.5.2021, p. 79).
11. Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne (JO L 274 du 30.7.2021, p. 41).
12. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et dans une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale.

De même, par souci de clarté, le présent règlement devrait être sans préjudice du droit de l'Union en matière de protection des consommateurs, en particulier les règlements (UE) 2017/2394[13] et (UE) 2019/1020[14] du Parlement européen et du Conseil, les directives 2001/95/CE[15], 2005/29/CE[16], 2011/83/UE[17] et 2013/11/UE[18] du Parlement européen et du Conseil et la directive 93/13/CEE du Conseil[19], et en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil[20].

cf. RGPD

Il convient également que le présent règlement soit sans préjudice des règles de l'Union en matière de droit international privé, en particulier les règles relatives à la compétence ainsi qu'à la reconnaissance et à l'exécution des décisions en matière civile et commerciale, comme le règlement (UE) n° 1215/2012, et les règles relatives à la loi applicable aux obligations contractuelles et non contractuelles. La protection des personnes au regard du traitement des données à caractère personnel est régie exclusivement par les règles du droit de l'Union en la matière, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE. Il convient également que le présent règlement soit sans préjudice du droit de l'Union relatif aux conditions de travail et du droit de l'Union dans le domaine de la coopération judiciaire en matière civile et pénale. Toutefois, dans la mesure où ces actes juridiques de l'Union poursuivent les mêmes objectifs que ceux énoncés dans le présent règlement, les règles du présent règlement devraient s'appliquer en ce qui concerne les aspects qui ne sont pas ou ne sont pas pleinement traités par ces autres actes juridiques ainsi que les aspects pour lesquels ces autres actes juridiques laissent aux États membres la possibilité d'adopter certaines mesures au niveau national.

cf. RGPD

(11) Il convient de préciser que le présent règlement est sans préjudice du droit de l'Union sur le droit d'auteur et les droits voisins, y compris les directives 2001/29/CE[21], 2004/48/CE[22] et (UE) 2019/790[23] du Parlement européen et du Conseil, qui établissent des règles et des procédures spécifiques qui ne devraient pas être affectées.

Contenus illicites

(12) Afin d'atteindre l'objectif consistant à garantir un environnement en ligne sûr, prévisible et fiable, il convient, aux fins du présent règlement, que la notion de «contenu illicite» corresponde de manière générale aux règles en vigueur dans l'environnement hors ligne. Il convient, en particulier, de donner une définition large de la notion de «contenu illicite» de façon à ce qu'elle couvre les informations relatives aux

13. Règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et abrogeant le règlement (CE) n° 2006/2004 (JO L 345 du 27.12.2017, p. 1).
14. Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) n° 765/2008 et (UE) n° 305/2011 (JO L 169 du 25.6.2019, p. 1).
15. Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits (JO L 11 du 15.1.2002, p. 4).
16. Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).
17. Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil (JO L 304 du 22.11.2011, p. 64).
18. Directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 2009/22/CE (JO L 165 du 18.6.2013, p. 63).
19. Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).
20. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).
21. Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO L 167 du 22.6.2001, p. 10).

contenus, produits, services et activités illégaux. En particulier, cette notion devrait être comprise comme se référant à des informations, quelle que soit leur forme, qui, en vertu du droit applicable, sont soit elles-mêmes illicites, comme les discours haineux illégaux ou les contenus à caractère terroriste et les contenus discriminatoires illégaux, soit rendues illicites par les règles applicables en raison du fait qu'elles se rapportent à des activités illégales. Il peut s'agir, par exemple, du partage d'images représentant des abus sexuels commis sur des enfants, du partage illégal d'images privées sans consentement, du harcèlement en ligne, de la vente de produits non conformes ou contrefaits, de la vente de produits ou de la fourniture de services en violation du droit en matière de protection des consommateurs, de l'utilisation non autorisée de matériel protégé par le droit d'auteur, de l'offre illégale de services de logement ou de la vente illégale d'animaux vivants. En revanche, la vidéo d'un témoin oculaire d'une infraction pénale potentielle ne devrait pas être considérée comme constituant un contenu illicite simplement parce qu'elle met en scène un acte illégal, lorsque l'enregistrement ou la diffusion au public d'une telle vidéo n'est pas illégal en vertu du droit national ou du droit de l'Union. Il importe peu à cet égard que l'illégalité de l'information ou de l'activité procède du droit de l'Union ou du droit national conforme au droit de l'Union et il est indifférent de connaître la nature ou l'objet précis du droit en question.

Plateformes en ligne

(13) Compte tenu des caractéristiques particulières des services concernés et de la nécessité qui en découle de soumettre leurs fournisseurs à certaines obligations spécifiques, il est nécessaire de distinguer, au sein de la catégorie plus large des fournisseurs de services d'hébergement telle qu'elle est définie dans le présent règlement, la sous-catégorie des plateformes en ligne. Les plateformes en ligne, telles que les réseaux sociaux ou les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, devraient être définies comme des fournisseurs de services d'hébergement qui non seulement stockent les informations fournies par les destinataires du service à leur demande, mais qui diffusent également ces informations au public, à la demande des destinataires du service. Toutefois, afin d'éviter d'imposer des obligations trop étendues, les fournisseurs de services d'hébergement ne devraient pas être considérés comme des plateformes en ligne lorsque la diffusion au public n'est qu'une caractéristique mineure et purement accessoire qui est intrinsèquement liée à un autre service, ou une fonctionnalité mineure du service principal, et que cette caractéristique ou fonctionnalité ne peut, pour des raisons techniques objectives, être utilisée sans cet autre service ou ce service principal, et que l'intégration de cette caractéristique ou fonctionnalité n'est pas un moyen de se soustraire à l'applicabilité des règles du présent règlement relatives aux plateformes en ligne. Par exemple, la section «commentaires» d'un journal en ligne pourrait constituer une telle caractéristique, lorsqu'il est clair qu'elle est accessoire au service principal représenté par la publication d'actualités sous la responsabilité éditoriale de l'éditeur. En revanche, le stockage de commentaires sur un réseau social devrait être considéré comme un service de plateforme en ligne lorsqu'il est clair qu'il ne constitue pas une caractéristique mineure du service offert, même s'il est accessoire à la publication des messages des destinataires du service. Aux fins du présent règlement, les services d'informatique en nuage ou les services d'hébergement de sites internet ne devraient pas être considérés comme une plateforme en ligne lorsque la diffusion d'informations spécifiques au public constitue une caractéristique mineure et accessoire ou une fonctionnalité mineure de ces services.

De plus, les services d'informatique en nuage et les services d'hébergement de sites internet qui servent d'infrastructure, par exemple les services de stockage et les services informatiques infrastructurels sous-jacents d'une application internet, d'un site internet ou d'une plateforme en ligne, ne devraient pas, en tant que tels, être considérés comme diffusant au public des informations stockées ou traitées à la demande d'un destinataire de l'application, du site internet ou de la plateforme en ligne qu'ils hébergent.

(14) La notion de «diffusion au public», telle qu'elle est utilisée dans le présent règlement, devrait impliquer la mise à disposition de l'information à un nombre potentiellement illimité de personnes, c'est-à-dire le fait de rendre l'information facilement

22. Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle (JO L 157 du 30.4.2004, p. 45).
23. Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

accessible aux destinataires du service en général sans que le destinataire du service ayant fourni l'information ait à intervenir, que ces personnes aient ou non effectivement accès à l'information en question. En conséquence, lorsque l'accès à une information nécessite un enregistrement ou l'admission au sein d'un groupe de destinataires du service, cette information ne devrait être considérée comme étant diffusée au public que lorsque les destinataires du service qui cherchent à accéder à cette information sont enregistrés ou admis automatiquement sans intervention humaine pour en décider ou pour sélectionner les personnes auxquelles l'accès est accordé. Les services de communication interpersonnelle, tels qu'ils sont définis dans la directive (UE) 2018/1972 du Parlement européen et du Conseil[24], comme les courriels ou les services de messagerie privée, ne relèvent pas du champ d'application de la définition des plateformes en ligne car ils sont utilisés pour la communication interpersonnelle entre un nombre fini de personnes, déterminé par l'émetteur de la communication. Cependant, les obligations prévues dans le présent règlement pour les fournisseurs de plateformes en ligne peuvent s'appliquer à des services qui permettent de mettre des informations à la disposition d'un nombre potentiellement illimité de destinataires, non déterminé par l'émetteur de la communication, notamment par l'intermédiaire de groupes publics ou de canaux ouverts. Des informations ne devraient être considérées comme étant diffusées au public au sens du présent règlement que lorsque cette diffusion se produit à la demande directe du destinataire du service qui a fourni les informations.

(15) Lorsque certains des services fournis par un fournisseur sont couverts par le présent règlement alors que d'autres ne le sont pas, ou lorsque les services fournis par un fournisseur sont couverts par différentes sections du présent règlement, les dispositions pertinentes du présent règlement devraient s'appliquer uniquement aux services qui relèvent de leur champ d'application.

(16) La sécurité juridique offerte par le cadre horizontal d'exemptions conditionnelles de responsabilité pour les fournisseurs de services intermédiaires, établi par la directive 2000/31/CE, a permis l'émergence et le développement de nombreux services nouveaux dans l'ensemble du marché intérieur. Il convient, dès lors, de conserver ce cadre. Toutefois, compte tenu des divergences dans la transposition et l'application des règles pertinentes au niveau national, et pour des raisons de clarté et de cohérence, il y a lieu d'intégrer ce cadre dans le présent règlement. Il est également nécessaire de clarifier certains éléments dudit cadre, compte tenu de la jurisprudence de la Cour de justice de l'Union européenne.

Responsabilité des fournisseurs

(17) Les règles en matière de responsabilité des fournisseurs de services intermédiaires énoncées dans le présent règlement ne devraient établir que les cas dans lesquels le fournisseur de services intermédiaires concerné ne peut pas être tenu pour responsable du contenu illicite fourni par les destinataires du service. Ces règles ne devraient pas être interprétées comme constituant une base positive pour établir les cas dans lesquels la responsabilité d'un fournisseur peut être engagée, ce que les règles applicables du droit de l'Union ou du droit national doivent déterminer. En outre, les exemptions de responsabilité établies dans le présent règlement devraient s'appliquer à tout type de responsabilité à l'égard de tout type de contenu illicite, indépendamment de l'objet ou de la nature précis de ces législations.

(18) Les exemptions de responsabilité établies dans le présent règlement ne devraient pas s'appliquer lorsque, au lieu de se limiter à fournir les services de manière neutre dans le cadre d'un simple traitement technique et automatique des informations fournies par le destinataire du service, le fournisseur de services intermédiaires joue un rôle actif de nature à lui permettre de connaître ou de contrôler ces informations. Ces exemptions ne devraient donc pas s'appliquer à la responsabilité relative aux informations fournies non pas par le destinataire du service, mais par le fournisseur du service intermédiaire lui-même, y compris lorsque les informations ont été établies sous la responsabilité éditoriale de ce fournisseur.

(19) Compte tenu de la nature différente des activités de «simple transport», de «mise en cache» et d'«hébergement», ainsi que de la position et des capacités différentes des fournisseurs des services en question, il est nécessaire de distinguer les règles appli-

24. Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

cables à ces activités, dans la mesure où, dans le cadre du présent règlement, elles sont soumises à des exigences et à des conditions différentes et leur portée diffère, selon l'interprétation qu'en donne la Cour de justice de l'Union européenne.

(20) Lorsqu'un fournisseur de services intermédiaires collabore délibérément avec un destinataire desdits services afin d'entreprendre des activités illégales, les services ne devraient pas être réputés avoir été fournis de manière neutre et le fournisseur ne devrait donc pas pouvoir bénéficier des exemptions de responsabilité prévues dans le présent règlement. Tel devrait être le cas, par exemple, lorsque le fournisseur propose son service dans le but principal de faciliter des activités illégales, par exemple en indiquant explicitement que son objectif est de faciliter des activités illégales ou que ses services sont adaptés à cette fin. Le seul fait qu'un service propose des transmissions cryptées ou tout autre système rendant l'identification de l'utilisateur impossible ne devrait pas être considéré en soi comme facilitant des activités illégales.

(21) Un fournisseur devrait pouvoir bénéficier des exemptions de responsabilité pour les services de «simple transport» et de «mise en cache» lorsqu'il n'est impliqué en aucune manière dans l'information transmise ou à laquelle il est donné accès. Cela suppose, entre autres, qu'il n'apporte pas de modification à l'information qu'il transmet ou à laquelle il donne accès. Cependant, cette exigence ne devrait pas être comprise comme couvrant les manipulations à caractère technique qui ont lieu au cours de la transmission ou de l'accès, tant que ces manipulations n'altèrent pas l'intégrité de l'information transmise ou à laquelle il est donné accès.

(22) Afin de bénéficier de l'exemption de responsabilité relative aux services d'hébergement, le fournisseur devrait, dès qu'il a effectivement connaissance ou conscience d'une activité illégale ou d'un contenu illicite, agir rapidement pour retirer ce contenu ou rendre l'accès à ce contenu impossible. Il convient de retirer le contenu ou de rendre l'accès au contenu impossible dans le respect des droits fondamentaux des destinataires du service, y compris le droit à la liberté d'expression et d'information. Le fournisseur peut avoir effectivement connaissance ou prendre conscience du caractère illicite du contenu au moyen, entre autres, d'enquêtes effectuées de sa propre initiative ou de notifications qui lui sont soumises par des particuliers ou des entités conformément au présent règlement, dans la mesure où ces notifications sont assez précises et suffisamment étayées pour permettre à un opérateur économique diligent d'identifier et d'évaluer raisonnablement le contenu présumé illicite et, le cas échéant, d'agir contre celui-ci. Toutefois, cette connaissance ou prise de conscience effective ne peut être considérée comme étant présente au seul motif que le fournisseur est conscient, de manière générale, que son service est également utilisé pour stocker des contenus illicites. En outre, le fait qu'un fournisseur indexe automatiquement les informations mises en ligne sur son service, qu'il dispose d'une fonction de recherche ou qu'il recommande des informations sur la base des profils ou des préférences des destinataires du service ne constitue pas un motif suffisant pour considérer que ce fournisseur a "spécifiquement" connaissance des activités illégales menées sur cette plateforme ou des contenus illicites stockés sur celle-ci.

(23) L'exemption de responsabilité ne devrait pas s'appliquer lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur d'un service d'hébergement. Par exemple, lorsque le fournisseur d'une plateforme en ligne qui permet aux consommateurs de conclure des contrats à distance avec des professionnels détermine le prix des biens ou services offerts par le professionnel, le professionnel pourrait être considéré comme agissant sous l'autorité ou le contrôle de ladite plateforme en ligne.

(24) Afin d'assurer une protection efficace des consommateurs lorsqu'ils effectuent des transactions commerciales intermédiées en ligne, il convient que certains fournisseurs de services d'hébergement, à savoir les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ne bénéficient pas de l'exemption de responsabilité des fournisseurs de services d'hébergement établie dans le présent règlement, dans la mesure où ces plateformes en ligne présentent les informations pertinentes relatives aux transactions en cause de manière à conduire le consommateur à croire que les informations ont été fournies par ces plateformes en ligne elles-mêmes ou par des professionnels agissant sous leur autorité ou leur contrôle, et que ces plateformes en ligne ont donc connaissance de ces informations ou les contrôlent, même si ce n'est pas le cas en réalité. Des exemples de ce comportement pourraient être, lorsqu'une plateforme en ligne ne fait pas apparaître clairement l'identité du professionnel comme l'exige le présent règlement, lorsqu'elle

retient l'identité ou les coordonnées du professionnel jusqu'à ce que le contrat entre le professionnel et le consommateur soit conclu ou lorsqu'elle commercialise le produit ou le service en son nom propre plutôt qu'au nom du professionnel qui fournira ce produit ou service. À cet égard, il convient de déterminer objectivement, sur la base de toutes les circonstances pertinentes, si la présentation est susceptible de conduire un consommateur moyen à croire que les informations en question ont été fournies par la plateforme en ligne elle-même ou par des professionnels agissant sous son autorité ou son contrôle.

(25) Les exemptions de responsabilité établies dans le présent règlement ne devraient pas affecter la possibilité de procéder à des injonctions de différents types à l'encontre des fournisseurs de services intermédiaires, alors même qu'ils remplissent les conditions fixées dans le cadre de ces exemptions. Ces injonctions peuvent notamment revêtir la forme d'injonctions de juridictions ou d'autorités administratives, émises conformément au droit de l'Union, exigeant qu'il soit mis fin à toute infraction ou que l'on prévienne toute infraction, y compris en retirant les contenus illicites spécifiés dans ces injonctions, ou en rendant impossible l'accès à ces contenus.

(26) Afin de créer une sécurité juridique et de ne pas décourager les activités visant à détecter, recenser et combattre les contenus illicites entreprises volontairement par les fournisseurs de toutes les catégories de services intermédiaires, il convient de préciser que le simple fait que les fournisseurs entreprennent de telles activités n'empêche pas le recours aux exemptions de responsabilité prévues par le présent règlement pour autant que ces activités soient menées de bonne foi et avec diligence. Il convient que la condition d'agir de bonne foi et avec diligence comprenne le fait d'agir de manière objective, non discriminatoire et proportionnée, en tenant dûment compte des droits et des intérêts légitimes de toutes les parties concernées, ainsi que le fait de fournir les garanties nécessaires contre la suppression injustifiée de contenus licites, conformément à l'objectif et aux exigences du présent règlement. À cette fin, il convient, par exemple, que les fournisseurs concernés prennent des mesures raisonnables pour garantir que, lorsque des outils automatisés sont utilisés pour mener de telles activités, la technologie concernée est suffisamment fiable pour limiter le plus possible le taux d'erreur. En outre, il convient de préciser que le simple fait que les fournisseurs prennent des mesures, de bonne foi, pour se conformer aux exigences du droit de l'Union, y compris celles énoncées dans le présent règlement en ce qui concerne la mise en œuvre de leurs conditions générales, ne devrait pas empêcher le recours aux exemptions de responsabilité prévues par le présent règlement. Par conséquent, si de telles activités et mesures étaient prises par un fournisseur, elles ne devraient pas être prises en compte pour déterminer si ledit fournisseur peut se prévaloir d'une exemption de responsabilité, notamment en ce qui concerne la question de savoir s'il fournit son service de manière neutre et peut donc relever du champ d'application de la disposition concernée, cette règle n'impliquant cependant pas que ledit fournisseur peut nécessairement se prévaloir d'une exemption de responsabilité. Les actions volontaires ne sauraient servir à contourner les obligations incombant aux fournisseurs de services intermédiaires en vertu du présent règlement.

(27) Alors que les règles sur la responsabilité des fournisseurs de services intermédiaires définies dans le présent règlement se concentrent sur l'exemption de responsabilité des fournisseurs de services intermédiaires, il est important de rappeler que, malgré le rôle généralement important joué par ces fournisseurs, le problème des contenus illicites et activités illégales en ligne ne devrait pas être traité sous le seul angle de leurs responsabilités. Dans la mesure du possible, les tiers affectés par des contenus illicites transmis ou stockés en ligne devraient tenter de résoudre les conflits relatifs à ces contenus sans impliquer les fournisseurs de services intermédiaires en question. Les destinataires du service devraient être tenus responsables des contenus illicites qu'ils fournissent et qu'ils peuvent diffuser au public par des services intermédiaires, lorsque les règles applicables du droit de l'Union et du droit national déterminant cette responsabilité le prévoient. Le cas échéant, d'autres acteurs, tels que les modérateurs de groupe dans des environnements en ligne fermés, notamment dans le cas de grands groupes, devraient également contribuer à éviter la diffusion de contenus illicites en ligne, conformément au droit applicable. En outre, lorsqu'il est nécessaire d'impliquer des fournisseurs de services de la société de l'information, y compris des fournisseurs de services intermédiaires, toute demande ou toute injonction concernant cette implication devrait, en règle générale, être adressée au fournisseur spécifique qui a la capacité technique et opérationnelle d'agir contre des éléments de contenus illicites particuliers, de manière à prévenir et à réduire au minimum tout effet négatif

éventuel sur la disponibilité et l'accessibilité d'informations qui ne constituent pas des contenus illicites.

(28) Depuis l'an 2000, de nouvelles technologies sont apparues qui améliorent la disponibilité, l'efficacité, la rapidité, la fiabilité, la capacité et la sécurité des systèmes de transmission, de "repérabilité" et de stockage des données en ligne, engendrant ainsi un écosystème en ligne de plus en plus complexe. À cet égard, il convient de rappeler que les fournisseurs de services établissant et facilitant l'architecture logique sous-jacente et le bon fonctionnement de l'internet, y compris les fonctions techniques accessoires, peuvent également bénéficier des exemptions de responsabilité prévues par le présent règlement, dans la mesure où leurs services peuvent être qualifiés de services de "simple transport", de "mise en cache" ou d'"hébergement". De tels services comprennent, le cas échéant, les réseaux locaux sans fil, les services de système de noms de domaine (DNS), les registres de noms de domaine de premier niveau, les bureaux d'enregistrement de noms de domaine, les autorités de certification qui délivrent des certificats numériques, les réseaux privés virtuels, les moteurs de recherche en ligne, les services d'infrastructure en nuage ou les réseaux d'acheminement de contenus qui permettent, localisent ou améliorent les fonctions d'autres fournisseurs de services intermédiaires. De même, les services utilisés à des fins de communication, et les moyens techniques de leur fourniture, ont également évolué de manière considérable, donnant naissance à des services en ligne tels que la voix sur IP, les services de messagerie et les services de messagerie électronique sur l'internet, pour lesquels la communication est assurée via un service d'accès à l'internet. Ces services peuvent également bénéficier d'exemptions de responsabilité, dans la mesure où ils peuvent être qualifiés de services de "simple transport", de "mise en cache" ou d'"hébergement".

(29) Les services intermédiaires couvrent un large éventail d'activités économiques qui ont lieu en ligne et évoluent en permanence pour permettre une transmission d'informations rapide, sûre et sécurisée, ainsi que pour garantir le confort de tous les participants à l'écosystème en ligne. À titre d'exemple, les services intermédiaires de "simple transport" comprennent des catégories génériques de services telles que les points d'échange internet, les points d'accès sans fil, les réseaux privés virtuels, les services de DNS et de résolution de noms de domaine, les registres de noms de domaine de premier niveau, les bureaux d'enregistrement de noms de domaine, les autorités de certification qui délivrent des certificats numériques, la voix sur IP et d'autres services de communication interpersonnelle, tandis que les exemples génériques de services intermédiaires de "mise en cache" comprennent la seule fourniture de réseaux d'acheminement de contenus, de serveurs mandataires inverses ou de serveurs mandataires d'adaptation de contenus. De tels services sont essentiels pour garantir la transmission fluide et efficace des informations fournies sur l'internet. Parmi les exemples de "services d'hébergement" figurent des catégories de services telles que l'informatique en nuage, l'hébergement de sites internet, les services de référencement payant ou les services permettant le partage d'informations et de contenus en ligne, y compris le stockage et le partage de fichiers. Les services intermédiaires peuvent être fournis isolément, dans le cadre d'un autre type de service intermédiaire, ou simultanément avec d'autres services intermédiaires. La question de savoir si un service spécifique constitue un service de "simple transport", de "mise en cache" ou d'"hébergement" dépend uniquement de ses fonctionnalités techniques, lesquelles sont susceptibles d'évoluer dans le temps, et devrait être appréciée au cas par cas.

Injonctions

(30) Les fournisseurs de services intermédiaires ne devraient pas être soumis, ni de jure ni de facto, à une obligation de surveillance en ce qui concerne les obligations de nature générale. Cela ne concerne pas les obligations de surveillance dans un cas spécifique et, en particulier, cela n'affecte pas les injonctions émises par les autorités nationales conformément à la législation nationale, dans le respect du droit de l'Union, tel qu'il est interprété par la Cour de justice de l'Union européenne, et conformément aux conditions établies dans le présent règlement. Aucune disposition du présent règlement ne devrait être interprétée comme imposant une obligation générale de surveillance ou une obligation générale de recherche active des faits, ou comme une obligation générale, pour les fournisseurs, de prendre des mesures proactives à l'égard des contenus illicites.

(31) En fonction du système juridique de chaque État membre et du domaine juridique en cause, les autorités judiciaires ou administratives nationales, y compris les autorités

répressives, peuvent enjoindre aux fournisseurs de services intermédiaires de prendre des mesures à l'encontre d'un ou de plusieurs éléments de contenus illicites spécifiques ou de fournir certaines informations spécifiques. Les législations nationales sur la base desquelles ces injonctions sont émises diffèrent considérablement et, de plus en plus souvent, les injonctions sont émises dans des contextes transfrontières. Afin de garantir le respect efficace et efficient de ces injonctions, en particulier dans un contexte transfrontière, de sorte que les autorités publiques concernées puissent accomplir leurs missions et que les fournisseurs ne soient pas soumis à des charges disproportionnées, sans porter indûment atteinte aux droits et intérêts légitimes de tiers, il est nécessaire de fixer certaines conditions auxquelles ces injonctions devraient répondre et certaines exigences complémentaires relatives au traitement de ces injonctions. En conséquence, le présent règlement devrait n'harmoniser que certaines conditions minimales spécifiques devant être respectées par ces injonctions pour donner naissance à l'obligation, pour les fournisseurs de services intermédiaires, d'informer les autorités concernées de la suite donnée à ces injonctions. Par conséquent, le présent règlement n'offre pas une base juridique pour l'émission de ces injonctions ni ne réglemente leur champ d'application territorial ou leur exécution transfrontière.

(32) Le droit national ou de l'Union applicable sur la base duquel ces injonctions sont émises pourrait prévoir des conditions supplémentaires et devrait servir de base pour l'exécution des injonctions concernées. En cas de non- respect de ces injonctions, l'État membre d'émission devrait pouvoir les faire respecter conformément à son droit national. Les législations nationales applicables devraient être conformes au droit de l'Union, y compris à la Charte et aux dispositions du traité sur le fonctionnement de l'Union européenne relatives à la liberté d'établissement et à la libre prestation des services au sein de l'Union, en particulier en ce qui concerne les services en ligne de jeux d'argent et de hasard et de paris. De même, l'application de ces législations nationales aux fins de l'exécution des injonctions concernées s'entend sans préjudice des actes juridiques de l'Union ou des accords internationaux conclus par l'Union ou par les États membres concernant la reconnaissance, la mise en œuvre et l'exécution transfrontières de ces injonctions, en particulier en matière civile et pénale. Par ailleurs, il convient que l'exécution de l'obligation d'informer les autorités concernées de la suite donnée à ces injonctions, par opposition à l'exécution des injonctions elles-mêmes, soit soumise aux règles énoncées dans le présent règlement.

(33) Il convient que le fournisseur de services intermédiaires informe l'autorité d'émission de toute suite donnée à ces injonctions, sans retard injustifié, dans le respect des délais prévus par le droit de l'Union ou le droit national applicable.

(34) Les autorités nationales compétentes devraient pouvoir émettre de telles injonctions d'agir contre un contenu considéré comme illicite ou des injonctions de fournir des informations sur la base du droit de l'Union ou du droit national conforme au droit de l'Union, en particulier la Charte, et les adresser aux fournisseurs de services intermédiaires, y compris ceux qui sont établis dans un autre État membre. Le présent règlement devrait toutefois s'entendre sans préjudice du droit de l'Union dans le domaine de la coopération judiciaire en matière civile ou pénale, y compris le règlement (UE) n° 1215/2012 et un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, et du droit de la procédure pénale ou du droit de la procédure civile national. Par conséquent, lorsque ces législations prévoient, dans le cadre de procédures pénales ou civiles, des conditions supplémentaires à celles prévues dans le présent règlement ou incompatibles avec celles-ci en ce qui concerne les injonctions d'agir contre des contenus illicites ou de fournir des informations, les conditions prévues dans le présent règlement pourraient ne pas s'appliquer ou être adaptées. En particulier, l'obligation faite au coordinateur pour les services numériques de l'État membre de l'autorité d'émission de transmettre une copie des injonctions à tous les autres coordinateurs pour les services numériques pourrait ne pas s'appliquer dans le cadre de procédures pénales ou pourrait être adaptée, lorsque le droit de la procédure pénale national applicable le prévoit.

En outre, l'obligation pour les injonctions de contenir un exposé des motifs expliquant pourquoi l'information constitue un contenu illicite devrait être adaptée, si cela est nécessaire, en vertu du droit de la procédure pénale national applicable à des fins de prévention et de détection des infractions pénales et d'enquêtes et de poursuites en la matière. Enfin, l'obligation pour les fournisseurs de services intermédiaires d'informer le destinataire du service pourrait être différée conformément au droit de l'Union ou

au droit national applicable, en particulier dans le cadre de procédures pénales, civiles ou administratives. En outre, les injonctions devraient être émises dans le respect du règlement (UE) 2016/679 et de l'interdiction des obligations générales de surveillance des informations ou de recherche active des faits ou des circonstances indiquant une activité illégale prévue par le présent règlement. Les conditions et exigences énoncées dans le présent règlement qui s'appliquent aux injonctions d'agir contre des contenus illicites sont sans préjudice d'autres actes de l'Union prévoyant des systèmes similaires visant à agir contre des types spécifiques de contenus illicites, tels que le règlement (UE) 2021/784, le règlement (UE) 2019/1020 ou le règlement (UE) 2017/2394 qui confère aux autorités des États membres chargées de faire respecter la législation en matière de protection des consommateurs des pouvoirs spécifiques pour ordonner la fourniture d'informations. De même, les conditions et exigences qui s'appliquent aux injonctions de fournir des informations sont sans préjudice d'autres actes de l'Union prévoyant des règles pertinentes similaires pour des secteurs spécifiques. Ces conditions et exigences devraient être sans préjudice des règles de conservation et de préservation prévues par le droit national applicable, en conformité avec le droit de l'Union et avec les demandes de traitement confidentiel concernant la non-divulgation d'informations émanant des autorités répressives. Ces conditions et exigences ne devraient pas faire obstacle à la possibilité, pour les États membres, d'exiger d'un fournisseur de services intermédiaires qu'il prévienne une infraction, en conformité avec le droit de l'Union, y compris le présent règlement, et en particulier avec l'interdiction des obligations générales de surveillance.

cf.RGPD

(35) Il convient que les conditions et exigences fixées dans le présent règlement soient remplies au plus tard au moment de la transmission de l'injonction au fournisseur concerné. Par conséquent, l'injonction peut être émise dans l'une des langues officielles de l'autorité d'émission de l'État membre concerné. Toutefois, lorsque cette langue diffère de la langue déclarée par le fournisseur de services intermédiaires ou d'une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et le fournisseur de services intermédiaires, il convient que la transmission de l'injonction soit accompagnée d'une traduction, au minimum, des éléments de l'injonction qui sont prévus dans le présent règlement. Lorsqu'un fournisseur de services intermédiaires et les autorités d'un État membre sont convenus d'utiliser une certaine langue, il convient d'encourager ledit fournisseur à accepter des injonctions émises dans la même langue par les autorités d'autres États membres. Il convient que les injonctions contiennent des éléments qui permettent au destinataire d'identifier l'autorité d'émission, y compris les coordonnées d'un point de contact au sein de ladite autorité, le cas échéant, et de vérifier le caractère authentique de l'injonction.

(36) La portée territoriale de ces injonctions d'agir contre des contenus illicites devrait être clairement définie sur la base du droit de l'Union ou du droit national applicable en vertu duquel l'injonction est émise et ne devrait pas excéder ce qui est strictement nécessaire pour atteindre les objectifs de cette dernière. À cet égard, l'autorité judiciaire ou administrative nationale, qui pourrait être une autorité répressive, qui émet l'injonction devrait mettre en balance l'objectif poursuivi par l'injonction, conformément à la base juridique en vertu de laquelle elle est émise, et les droits et intérêts légitimes de l'ensemble des tiers susceptibles d'être affectés par celle-ci, en particulier leurs droits fondamentaux au titre de la Charte. En particulier dans un contexte transfrontière, l'effet de l'injonction devrait être, en principe, limité au territoire de l'État membre d'émission, à moins que le caractère illicite du contenu découle directement du droit de l'Union ou que l'autorité d'émission considère que les droits en cause requièrent un champ d'application territorial plus large, conformément au droit de l'Union et au droit international, en ce compris les impératifs de courtoisie internationale.

(37) Les injonctions de fournir des informations régies par le présent règlement concernent la production d'informations spécifiques portant sur des destinataires particuliers du service intermédiaire concerné qui sont identifiés dans ces injonctions aux fins de déterminer si les destinataires du service respectent les règles de l'Union ou les règles nationales applicables. Il convient que ces injonctions demandent des informations destinées à permettre l'identification des destinataires du service concerné. Par conséquent, les injonctions relatives à des informations sur un groupe de destinataires du service qui ne sont pas précisément identifiés, y compris les injonctions de fournir des informations agrégées requises à des fins statistiques ou en vue de l'élaboration de politiques fondées sur des éléments factuels, ne sont pas couvertes par les exigences du présent règlement concernant la fourniture d'informations.

(38) Les injonctions d'agir contre des contenus illicites et de fournir des informations ne sont soumises aux règles garantissant la compétence de l'État membre dans lequel le fournisseur de services visé est établi et aux règles prévoyant d'éventuelles dérogations à cette compétence dans certains cas, énoncées à l'article 3 de la directive 2000/31/CE, que si les conditions dudit article sont remplies. Dans la mesure où les injonctions en question portent, respectivement, sur des éléments de contenus illicites et sur des éléments d'information spécifiques, lorsqu'elles sont adressées à des fournisseurs de services intermédiaires établis dans un autre État membre, elles ne restreignent pas en principe la liberté de ces fournisseurs de fournir leurs services par-delà les frontières. Par conséquent, les règles énoncées à l'article 3 de la directive 2000/31/CE, y compris celles qui concernent la nécessité de justifier les mesures dérogeant à la compétence de l'État membre dans lequel le prestataire de services est établi pour certains motifs précis et la notification de ces mesures, ne s'appliquent pas à ces injonctions.

(39) Les obligations de fournir des informations sur les mécanismes de recours dont disposent le fournisseur du service intermédiaire et le destinataire du service qui a fourni le contenu comprennent une obligation de fournir des informations sur les mécanismes administratifs de traitement des plaintes et les voies de recours juridictionnel, y compris les recours contre les injonctions émises par des autorités judiciaires. De plus, les coordinateurs pour les services numériques pourraient élaborer des outils et orientations nationaux en ce qui concerne les mécanismes de plainte et de recours applicables sur leur territoire respectif afin de faciliter l'accès des destinataires du service à ces mécanismes. Enfin, lors de l'application du présent règlement, il convient que les États membres respectent le droit fondamental à un recours juridictionnel effectif et à accéder à un tribunal impartial, comme le prévoit l'article 47 de la Charte. Le présent règlement ne devrait donc pas empêcher les autorités judiciaires ou administratives nationales compétentes, sur la base du droit de l'Union ou du droit national applicable, d'émettre une injonction de rétablir des contenus, lorsque ces contenus étaient conformes aux conditions générales du fournisseur de services intermédiaires, mais ont été considérés par erreur comme illicites par ce fournisseur et ont été retirés.

Obligation de diligence

(40) Afin d'atteindre les objectifs du présent règlement, et notamment d'améliorer le fonctionnement du marché intérieur et de garantir un environnement en ligne sûr et transparent, il est nécessaire d'établir un ensemble clair, efficace, prévisible et équilibré d'obligations harmonisées de diligence pour les fournisseurs de services intermédiaires. Ces obligations devraient notamment viser à garantir différents objectifs de politique publique, comme celui d'assurer la sécurité et la confiance des destinataires du service, y compris les consommateurs, les mineurs et les utilisateurs qui sont particulièrement exposés au risque de faire l'objet de discours haineux, de harcèlement sexuel ou d'autres actions discriminatoires, de protéger les droits fondamentaux concernés inscrits dans la Charte, d'assurer une véritable responsabilisation de ces fournisseurs et de donner les moyens d'agir aux destinataires et autres parties affectées, tout en facilitant le contrôle nécessaire par les autorités compétentes.

(41) À cet égard, il est important que les obligations de diligence soient adaptées au type, à la taille et à la nature du service intermédiaire concerné. Le présent règlement définit donc des obligations de base applicables à tous les fournisseurs de services intermédiaires, ainsi que des obligations supplémentaires pour les fournisseurs de services d'hébergement et, plus particulièrement, pour les fournisseurs de plateformes en ligne et de très grandes plateformes en ligne ainsi que de très grands moteurs de recherche en ligne. Dans la mesure où les fournisseurs de services intermédiaires entrent dans un certain nombre de catégories différentes en raison de la nature de leurs services et de leur taille, ils devraient respecter toutes les obligations correspondantes du présent règlement se rapportant à ces services. Ces obligations harmonisées de diligence, qui devraient être raisonnables et non arbitraires, sont indispensables en vue de répondre aux préoccupations de politique publique déterminées, telles que la sauvegarde des intérêts légitimes des destinataires du service, la lutte contre les pratiques illégales et la protection des droits fondamentaux consacrés dans la Charte. Les obligations de diligence sont indépendantes de la question de la responsabilité des fournisseurs de services intermédiaires, qui doit donc être appréciée séparément.

Point de contact électronique unique

(42) Afin de faciliter une communication bidirectionnelle fluide et efficace, avec, le cas échéant, un accusé de réception de ladite communication, sur les matières relevant du présent règlement, les fournisseurs de services intermédiaires devraient être tenus

de désigner un point de contact électronique unique et de publier et mettre à jour les informations utiles concernant ce point de contact, y compris les langues à utiliser dans cette communication. Le point de contact électronique peut également être utilisé par des signaleurs de confiance et par des entités professionnelles qui ont un lien particulier avec le fournisseur de services intermédiaires. Contrairement au représentant légal, le point de contact électronique devrait avoir une fonction opérationnelle et ne devrait pas être tenu d'avoir une localisation physique. Les fournisseurs de services intermédiaires peuvent désigner le même point de contact unique pour répondre aux exigences du présent règlement et aux fins d'autres actes du droit de l'Union. Lorsqu'ils spécifient les langues de communication, les fournisseurs de services intermédiaires sont encouragés à veiller à ce que les langues choisies ne constituent pas en elles-mêmes un obstacle à la communication. Si nécessaire, il devrait être possible pour les fournisseurs de services intermédiaires et les autorités des États membres de conclure un accord séparé sur la langue de communication, ou de chercher un autre moyen de surmonter la barrière linguistique, y compris en utilisant tous les moyens technologiques ou toutes les ressources humaines internes et externes disponibles.

(43) Les fournisseurs de services intermédiaires devraient également être tenus de désigner un point de contact unique pour les destinataires des services, permettant d'établir une communication rapide, directe et efficace, en particulier par des moyens aisément accessibles, tels que des numéros de téléphone, des adresses de courrier électronique, des formulaires de contact électroniques, des dialogueurs ou des messageries instantanées. Lorsqu'un destinataire du service communique avec des dialogueurs, il convient de l'indiquer explicitement. Les fournisseurs de services intermédiaires devraient permettre aux destinataires des services de choisir des moyens de communication directe et efficace qui ne reposent pas uniquement sur des outils automatisés. Les fournisseurs de services intermédiaires devraient s'efforcer, dans la mesure du raisonnable, de garantir que des ressources humaines et financières suffisantes sont allouées pour que cette communication s'effectue de façon rapide et efficace.

Représentant légal

(44) Il convient que les fournisseurs de services intermédiaires établis dans un pays tiers qui proposent des services dans l'Union désignent un représentant légal doté d'un mandat suffisant dans l'Union et fournissent des informations relatives à leurs représentants légaux aux autorités compétentes et les mettent à la disposition du public. Pour se conformer à cette obligation, ces fournisseurs de services intermédiaires devraient veiller à ce que le représentant légal désigné dispose des pouvoirs et ressources nécessaires pour coopérer avec les autorités compétentes. Cela pourrait être le cas, par exemple, lorsqu'un fournisseur de services intermédiaires désigne une entreprise filiale du même groupe que lui, ou sa société mère, si cette entreprise filiale ou cette société mère est établie dans l'Union. Toutefois, cela pourrait ne pas être le cas, par exemple, lorsque le représentant légal fait l'objet d'une procédure d'assainissement, de faillite ou d'insolvabilité personnelle ou d'entreprise. Cette obligation devrait permettre un contrôle efficace et, si nécessaire, l'exécution du présent règlement à l'égard de ces fournisseurs. Il devrait être possible pour un représentant légal d'être mandaté, conformément au droit national, par plus d'un fournisseur de services intermédiaires. Le représentant légal devrait pouvoir également faire office de point de contact, pour autant que les exigences pertinentes du présent règlement soient respectées.

Modération

(45) Tout en respectant en principe la liberté contractuelle des fournisseurs de services intermédiaires, il convient de fixer certaines règles concernant le contenu, l'application et la mise en application des conditions générales de ces fournisseurs, dans un souci de transparence, de protection des destinataires du service et de prévention de conséquences inéquitables ou arbitraires. Les fournisseurs de services intermédiaires devraient indiquer clairement et tenir à jour dans leurs conditions générales les informations relatives aux motifs au titre desquels ils peuvent restreindre la fourniture de leurs services. Ils devraient en particulier inclure des renseignements ayant trait aux politiques, procédures, mesures et outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain ainsi que le règlement intérieur de leur système interne de traitement des réclamations. Ils devraient également fournir des informations aisément accessibles sur le droit de mettre fin à l'utilisation du service. Les fournisseurs de services intermédiaires peuvent utiliser des éléments graphiques dans leurs conditions générales, tels que des icônes ou des images, pour illustrer les principaux éléments des exigences en matière d'information énoncées dans le présent règlement. Les fournisseurs devraient informer les destinataires de leur service, à l'aide de moyens appropriés, au

sujet des modifications importantes apportées aux conditions générales, par exemple lorsqu'ils modifient les règles relatives aux informations qui sont autorisées sur leur service, ou d'autres modifications de cette nature qui pourraient avoir une influence directe sur la capacité des destinataires à utiliser le service.

(46) Les fournisseurs de services intermédiaires qui s'adressent principalement aux mineurs, par exemple par la conception ou la commercialisation du service, ou qui sont utilisés de manière prédominante par des mineurs, devraient déployer des efforts particuliers pour rendre l'explication de leurs conditions générales aisément compréhensible pour les mineurs.

(47) Lorsqu'ils conçoivent, appliquent et font respecter ces restrictions, les fournisseurs de services intermédiaires devraient agir de manière non arbitraire et non discriminatoire et tenir compte des droits et des intérêts légitimes des destinataires du service, y compris les droits fondamentaux consacrés dans la Charte. Les fournisseurs de très grandes plateformes en ligne devraient, par exemple, en particulier, tenir dûment compte de la liberté d'expression et d'information, notamment la liberté et le pluralisme des médias. Tous les fournisseurs de services intermédiaires devraient également tenir dûment compte des normes internationales pertinentes en matière de protection des droits de l'homme, telles que les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme.

(48) Compte tenu de leur portée et de leur rôle particuliers, il convient d'imposer aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne des exigences supplémentaires en matière d'information et de transparence en ce qui concerne leurs conditions générales. Par conséquent, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne devraient fournir leurs conditions générales dans les langues officielles de tous les États membres dans lesquels ils proposent leurs services et devraient également fournir aux destinataires des services un résumé concis et facilement lisible des principaux éléments des conditions générales. Ces résumés devraient recenser les principaux éléments des exigences en matière d'information, y compris la possibilité de ne pas consentir aux clauses optionnelles.

(49) En vue de garantir un niveau adéquat de transparence et de responsabilisation, les fournisseurs de services intermédiaires devraient publier un rapport annuel dans un format lisible par une machine, conformément aux exigences harmonisées contenues dans le présent règlement, sur la modération des contenus à laquelle ils procèdent, y compris les mesures prises dans le cadre de l'application et de la mise en application de leurs conditions générales. Toutefois, afin d'éviter des charges disproportionnées, les obligations en matière de rapports de transparence ne devraient pas s'appliquer aux fournisseurs qui sont des microentreprises ou des petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission[25] et qui ne sont pas de très grandes plateformes en ligne au sens du présent règlement.

(50) Les fournisseurs de services d'hébergement jouent un rôle particulièrement important dans la lutte contre les contenus illicites en ligne, car ils stockent les informations fournies par les destinataires du service et à la demande de ceux-ci, et permettent généralement à d'autres destinataires d'accéder à ces informations, parfois à grande échelle. Il est important que tous les fournisseurs de services d'hébergement, quelle que soit leur taille, mettent en place des mécanismes de notification et d'action facilement accessibles et faciles à utiliser, qui permettent de notifier aisément au fournisseur de services d'hébergement concerné les éléments d'information spécifiques que la partie notifiante considère comme un contenu illicite ("notification"), notification à la suite de laquelle ce fournisseur peut décider s'il est d'accord ou non avec cette évaluation et s'il souhaite ou non retirer ce contenu ou rendre l'accès à ce contenu impossible ("action"). Ces mécanismes devraient être clairement identifiables, situés à proximité des informations en question et au moins aussi faciles à trouver et à utiliser que les mécanismes de notification pour les contenus qui enfreignent les conditions générales du fournisseur de services d'hébergement. Pour autant que les exigences relatives aux notifications soient respectées, il devrait être possible à des particuliers ou à des entités de notifier plusieurs éléments spécifiques de contenus présumés illi-

25. Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

cites par le biais d'une notification unique afin de permettre la mise en œuvre effective des mécanismes de notification et d'action. Le mécanisme de notification devrait permettre, mais ne pas exiger, l'identification du particulier ou de l'entité soumettant la notification. Pour certains types d'éléments d'information notifiés, l'identité du particulier ou de l'entité soumettant la notification pourrait être nécessaire pour déterminer si les informations en question constituent un contenu illicite, comme il est allégué. L'obligation de mettre en place des mécanismes de notification et d'action devrait s'appliquer, par exemple, aux services de stockage et de partage de fichiers, aux services d'hébergement de sites internet, aux serveurs de publicité et aux "pastebins", dans la mesure où ils peuvent être qualifiés de services d'hébergement couverts par le présent règlement.

(51) Eu égard à la nécessité de tenir dûment compte des droits fondamentaux de toutes les parties concernées garantis par la Charte, toute mesure prise par un fournisseur de services d'hébergement à la suite de la réception d'une notification devrait être strictement ciblée, au sens où elle devrait servir à retirer des éléments d'information spécifiques considérées comme constituant un contenu illicite ou à rendre l'accès à ceux-ci impossible, sans porter indûment atteinte à la liberté d'expression et d'information des destinataires du service. En conséquence, les notifications devraient, en règle générale, être adressées aux fournisseurs de services d'hébergement dont il peut être raisonnablement attendu qu'ils aient la capacité technique et opérationnelle d'agir contre ces éléments spécifiques. Les fournisseurs de services d'hébergement qui reçoivent une notification relative à un élément d'information spécifique qu'ils ne peuvent retirer, pour des raisons techniques ou opérationnelles, devraient en informer la personne ou l'entité qui a soumis la notification.

(52) Il convient que les règles relatives à ces mécanismes de notification et d'action soient harmonisées au niveau de l'Union, de manière à permettre un traitement en temps utile, diligent et non arbitraire des notifications sur la base de règles uniformes, transparentes et claires et qui comportent des garanties solides protégeant les droits et intérêts légitimes de toutes les parties affectées, en particulier leurs droits fondamentaux garantis par la Charte, indépendamment de l'État membre dans lequel ces parties sont établies ou résident et du domaine juridique en cause. Ces droits fondamentaux comprennent notamment, sans s'y limiter: pour les destinataires du service, le droit à la liberté d'expression et d'information, le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel, le droit à la non-discrimination et le droit à un recours effectif; pour les fournisseurs de services, la liberté d'entreprise, y compris la liberté contractuelle; pour les parties affectées par un contenu illicite, le droit à la dignité humaine, les droits de l'enfant, le droit à la protection de la propriété, y compris la propriété intellectuelle, et le droit à la non-discrimination. Les fournisseurs de services d'hébergement devraient réagir rapidement aux notifications, notamment en tenant compte du type de contenu illicite notifié et de l'urgence d'agir. Il peut, par exemple, être attendu de ces fournisseurs qu'ils agissent sans retard en cas de notification d'un contenu présumé illicite comportant une menace pour la vie ou la sécurité des personnes. Le fournisseur de services d'hébergement devrait informer le particulier ou l'entité ayant notifié le contenu spécifique, sans retard injustifié après avoir pris la décision d'agir ou non à la suite de la notification.

(53) Les mécanismes de notification et d'action devraient permettre la soumission de notifications suffisamment précises et dûment motivées pour permettre au fournisseur de services d'hébergement concerné de prendre une décision éclairée et diligente, compatible avec la liberté d'expression et d'information, en ce qui concerne le contenu auquel la notification se rapporte, en particulier la question de savoir si ce contenu doit ou non être considéré comme un contenu illicite et s'il doit être retiré ou si l'accès à ce contenu doit être rendu impossible. Ces mécanismes devraient être conçus de manière à faciliter l'envoi de notifications qui contiennent une explication des raisons pour lesquelles le particulier ou l'entité soumettant la notification considère le contenu comme un contenu illicite et une indication claire de l'emplacement du contenu en question. Lorsqu'une notification contient suffisamment d'informations pour permettre à un fournisseur diligent de services d'hébergement de déterminer, sans examen juridique détaillé, que le contenu est clairement illicite, la notification devrait être réputée donner lieu à la connaissance ou à la prise de conscience effective de l'illégalité. À l'exception de la soumission de notifications relatives aux infractions visées aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil[26], ces mécanismes devraient demander au particulier ou à l'entité soumettant la notification de divulguer son identité afin d'éviter toute utilisation abusive.

(54) Lorsqu'un fournisseur de services d'hébergement décide, au motif que les informations fournies par le destinataire du service constituent du contenu illicite ou sont incompatibles avec ses conditions générales, de retirer des informations fournies par un destinataire du service ou de rendre impossible l'accès à de telles informations, ou de restreindre d'une autre manière leur visibilité ou leur monétisation, par exemple à la suite de la réception d'une notification ou de sa propre initiative, y compris par l'utilisation exclusive d'outils automatisés, il convient que ce fournisseur informe le destinataire, de manière claire et facilement compréhensible, de sa décision, des raisons de celle-ci et des possibilités de recours disponibles pour la contester, compte tenu des conséquences négatives que de telles décisions peuvent avoir pour le destinataire, y compris en ce qui concerne l'exercice de son droit fondamental à la liberté d'expression. Cette obligation devrait s'appliquer quelles que soient les raisons de la décision, en particulier si l'action a été engagée parce que les informations notifiées sont considérées comme un contenu illicite ou sont incompatibles avec les conditions générales applicables au service. Lorsque la décision a été prise à la suite de la réception d'une notification, le fournisseur de services d'hébergement ne devrait révéler l'identité de la personne ou de l'entité qui a soumis la notification au destinataire du service que lorsque cette information est nécessaire pour déterminer l'illicéité du contenu, par exemple en cas de violation des droits de propriété intellectuelle.

(55) La restriction de la visibilité peut prendre la forme d'une rétrogradation dans les systèmes de classement ou de recommandation, ainsi que d'une limitation de l'accessibilité pour un ou plusieurs destinataires du service ou du blocage de l'utilisateur sur une communauté en ligne à l'insu de ce dernier ("bannissement par l'ombre"). La monétisation via les recettes publicitaires générées par les informations fournies par le destinataire du service peut être restreinte au moyen de la suspension ou la fin des paiements monétaires ou des recettes associées aux informations concernées. L'obligation de fournir un exposé des motifs ne devrait toutefois pas s'appliquer aux contenus commerciaux trompeurs et de grande diffusion diffusés par manipulation intentionnelle du service, en particulier l'utilisation non authentique du service, comme l'utilisation de robots ou de faux comptes ou d'autres utilisations trompeuses du service. Quelles que soient les autres possibilités de contester la décision du fournisseur de services d'hébergement, le destinataire du service devrait toujours disposer d'un droit de recours effectif devant une juridiction, conformément au droit national.

(56) Un fournisseur de services d'hébergement peut, dans certains cas, avoir connaissance, à la suite de la notification d'une partie notifiante ou des mesures qu'il a lui-même volontairement adoptées, d'informations relatives à certaines activités d'un destinataire du service, telles que la fourniture de certains types de contenus illicites, qui donnent lieu à des motifs raisonnables de soupçonner, compte tenu de toutes les circonstances pertinentes dont le fournisseur de services d'hébergement a connaissance, que ce destinataire peut avoir commis, peut être en train de commettre ou est susceptible de commettre une infraction pénale impliquant une menace pour la vie ou la sécurité d'une ou de plusieurs personnes, telles que des infractions définies dans la directive 2011/36/UE du Parlement européen et du Conseil[27], dans la directive 2011/93/UE ou dans la directive (UE) 2017/541 du Parlement européen et du Conseil[28]. À titre d'exemple, des éléments spécifiques de contenus peuvent conduire à soupçonner l'existence d'une menace pour le public, telle que la provocation à commettre une infraction terroriste au sens de l'article 21 de la directive (UE) 2017/541. Dans de tels cas, le fournisseur de services d'hébergement devrait informer sans retard les autorités répressives compétentes de tels soupçons. Le fournisseur de services d'hébergement devrait fournir toutes les informations pertinentes dont il dispose, en particulier, le cas échéant, le contenu en question et, s'il est connu, le moment où il a été publié, y compris le fuseau horaire désigné, une explication quant à ses soupçons et les informations nécessaires pour localiser et identifier le destinataire du service concerné. Le présent

26. Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).
27. Directive 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil (JO L 101 du 15.4.2011, p. 1).
28. Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

règlement n'offre pas de base juridique pour le profilage des destinataires des services aux fins de la détection éventuelle d'infractions pénales par les fournisseurs de services d'hébergement. Les fournisseurs de services d'hébergement devraient également respecter les autres dispositions applicables du droit de l'Union ou du droit national relatives à la protection des droits et libertés des personnes lorsqu'ils informent les autorités répressives.

(57) Pour éviter d'imposer des contraintes disproportionnées, les obligations supplémentaires imposées au titre du présent règlement aux fournisseurs de plateformes en ligne, y compris les plateformes permettant aux consommateurs de conclure des contrats à distance avec des professionnels, ne devraient pas s'appliquer aux fournisseurs qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE. Pour la même raison, ces obligations supplémentaires ne devraient pas non plus s'appliquer aux fournisseurs de plateformes en ligne qui étaient qualifiés précédemment de microentreprises ou de petites entreprises, pendant une période de douze mois suivant la perte de ce statut. Ces fournisseurs ne devraient pas être exclus de l'obligation de fournir des informations sur la moyenne mensuelle des destinataires actifs du service à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission. Toutefois, étant donné que les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne ont une plus grande portée et une plus grande influence sur la manière dont les destinataires du service obtiennent des informations et communiquent en ligne, ces fournisseurs ne devraient pas bénéficier de cette exclusion, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises ou qu'ils aient été récemment qualifiés comme tels. Les règles de consolidation fixées dans la recommandation 2003/361/CE contribuent à prévenir tout contournement de ces obligations supplémentaires. Aucune disposition du présent règlement n'empêche les fournisseurs de plateformes en ligne couverts par cette exclusion de mettre en place, sur une base volontaire, un système qui respecte une ou plusieurs de ces obligations.

(58) Les destinataires du service devraient pouvoir contester facilement et efficacement certaines décisions des fournisseurs de plateformes en ligne, relatives à l'illicéité d'un contenu ou à son incompatibilité avec les conditions générales, qui ont une incidence négative pour eux. Il convient donc que les fournisseurs de plateformes en ligne soient tenus de prévoir des systèmes internes de traitement des réclamations, qui remplissent certaines conditions visant à garantir la facilité d'accès à ces systèmes ainsi que leur capacité d'aboutir à des résultats rapides, non discriminatoires, non arbitraires et équitables, et à garantir que ces systèmes fassent l'objet d'un réexamen par un être humain lorsque des moyens automatisés sont utilisés. Ces systèmes devraient permettre à tous les destinataires du service d'introduire une réclamation et ne devraient pas fixer d'exigences formelles, telles que le renvoi à des dispositions juridiques spécifiques pertinentes ou à des explications juridiques compliquées. Les destinataires du service qui ont soumis une notification, au moyen du mécanisme de notification et d'action prévu par le présent règlement ou par l'intermédiaire du mécanisme de notification des contenus qui enfreignent les conditions générales du fournisseur de plateformes en ligne, devraient être autorisés à utiliser le mécanisme de réclamation pour contester la décision du fournisseur de plateformes en ligne concernant leurs notifications, y compris lorsqu'ils estiment que les mesures prises par ce fournisseur n'étaient pas adéquates. La possibilité d'introduire une réclamation visant à obtenir l'annulation de la décision contestée devrait être disponible pendant au moins six mois, à compter du moment auquel le fournisseur de plateformes en ligne a informé le destinataire du service de la décision.

(59) En outre, il convient de prévoir la possibilité de participer de bonne foi à un règlement extrajudiciaire de ces litiges, y compris de ceux qui n'ont pas pu être résolus de manière satisfaisante par les systèmes internes de traitement des réclamations, par des organes certifiés qui disposent de l'indépendance, des moyens et de l'expertise nécessaires pour s'acquitter de leur mission d'une manière équitable, rapide et économiquement avantageuse. L'indépendance des organes de règlement extrajudiciaire des litiges devrait également être garantie au niveau des personnes physiques chargées de régler les litiges, y compris au moyen de règles sur les conflits d'intérêts. Les frais facturés par les organes de règlement extrajudiciaire des litiges devraient être raisonnables, abordables, attrayants, peu coûteux pour les consommateurs et proportionnés et devraient être évalués au cas par cas. Lorsqu'un organe de règlement extrajudiciaire des litiges est certifié par le coordinateur pour les services numériques compétent, ce

certificat devrait être valide dans tous les États membres. Les fournisseurs de plateformes en ligne devraient pouvoir refuser de participer à des procédures de règlement extrajudiciaire des litiges au titre du présent règlement lorsque le même litige, en particulier en ce qui concerne les informations concernées et les motifs de la décision attaquée, les effets de la décision et les motifs invoqués pour contester la décision, a déjà été résolu par une procédure en cours devant la juridiction compétente ou devant un autre organe de règlement extrajudiciaire des litiges compétent ou fait déjà l'objet d'une procédure en cours devant une telle juridiction ou un tel organe. Les destinataires du service devraient pouvoir choisir entre le mécanisme interne de traitement des réclamations, un règlement extrajudiciaire des litiges et la possibilité d'engager, à tout moment, une procédure juridictionnelle. Étant donné que l'issue de la procédure de règlement extrajudiciaire des litiges n'est pas contraignante, les parties ne devraient pas être empêchées d'engager une procédure judiciaire concernant le même litige. Les possibilités de contester les décisions des fournisseurs de plateformes en ligne ne devraient altérer en aucune manière la possibilité de former un recours juridictionnel conformément à la législation de l'État membre concerné, et ne sauraient donc porter atteinte à l'exercice du droit à un recours juridictionnel effectif tel qu'il est prévu à l'article 47 de la Charte. Les dispositions du présent règlement relatives au règlement extrajudiciaire des litiges ne devraient pas obliger les États membres à mettre en place de tels organes de règlement extrajudiciaire des litiges.

(60) Pour les litiges contractuels entre consommateurs et entreprises concernant l'achat de biens ou de services, la directive 2013/11/UE garantit que les consommateurs et les entreprises de l'Union ont accès à des entités de règlement extrajudiciaire des litiges dont la qualité est certifiée. À cet égard, il convient de préciser que les règles du présent règlement relatives au règlement extrajudiciaire des litiges sont sans préjudice de ladite directive, y compris du droit qu'elle confère aux consommateurs de se retirer de la procédure à tout moment s'ils sont insatisfaits du déroulement ou du fonctionnement de la procédure.

(61) Il est possible d'agir plus rapidement et de manière plus fiable contre les contenus illicites lorsque les fournisseurs de plateformes en ligne prennent les mesures nécessaires pour faire en sorte que les notifications soumises par des signaleurs de confiance, qui agissent dans leur domaine d'expertise désigné, par l'intermédiaire des mécanismes de notification et d'action requis par le présent règlement soient traitées en priorité, sans préjudice de l'obligation de traiter et de statuer sur toutes les notifications soumises dans le cadre de ces mécanismes, en temps utile, avec diligence et de manière non arbitraire. Ce statut de signaleur de confiance devrait être attribué par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, et il devrait être reconnu par tous les fournisseurs de plateformes en ligne relevant du champ d'application du présent règlement. Ce statut de signaleur de confiance ne devrait être attribué qu'aux entités, et non aux particuliers, qui ont démontré, entre autres, qu'elles possèdent une expertise et une compétence particulières dans la lutte contre les contenus illicites et qu'elles travaillent de manière diligente, précise et objective. Il peut s'agir d'entités publiques, comme, en ce qui concerne les contenus terroristes, les unités de signalement des contenus sur l'internet des autorités répressives nationales ou de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), ou il peut s'agir d'organisations non gouvernementales et d'organismes privés ou semi-publics, tels que les organisations faisant partie du réseau INHOPE de permanences téléphoniques pour le signalement de matériel pédopornographique et les organisations ayant pour objectif de signaler les expressions racistes et xénophobes illégales en ligne. Pour éviter de diminuer la valeur ajoutée d'un tel mécanisme, le nombre total de signaleurs de confiance reconnus conformément au présent règlement devrait être limité. En particulier, les associations professionnelles représentant les intérêts de leurs membres sont encouragées à demander le statut de signaleurs de confiance, sans préjudice du droit des entités privées ou des particuliers de conclure des accords bilatéraux avec les fournisseurs de plateformes en ligne.

(62) Les signaleurs de confiance devraient publier des rapports facilement compréhensibles et détaillés sur les notifications soumises conformément au présent règlement. Ces rapports devraient indiquer des informations telles que le nombre de notifications classées par fournisseur de services d'hébergement, type de contenu et action entreprise par le fournisseur. Étant donné que les signaleurs de confiance ont fait la preuve de leur expertise et de leur compétence, il peut être escompté que le traitement des notifications provenant de signaleurs de confiance soit moins contraignant et donc

plus rapide que celui des notifications émanant d'autres destinataires du service. Cependant, le temps moyen nécessaire pour traiter les notifications peut toujours varier en fonction de facteurs tels que le type de contenu illicite, la qualité des notifications et les procédures techniques concrètes mises en place pour la soumission de ces notifications.

Par exemple, si le code de conduite pour la lutte contre les discours haineux illégaux en ligne de 2016 fixe un critère de référence pour les entreprises participantes en ce qui concerne le temps nécessaire au traitement des notifications valides en vue du retrait de discours haineux illégaux, d'autres types de contenus illicites peuvent prendre des délais de traitement très différents, en fonction des faits et circonstances spécifiques et des types de contenus illicites en jeu. Afin d'éviter les abus du statut de signaleur de confiance, il devrait être possible de suspendre ce statut lorsqu'un coordinateur pour les services numériques de l'État membre d'établissement a ouvert une enquête pour des raisons légitimes. Les dispositions du présent règlement relatives aux signaleurs de confiance ne devraient pas être interprétées comme empêchant les fournisseurs de plateformes en ligne de traiter de la même manière les notifications soumises par des entités ou des particuliers auxquels le statut de signaleur de confiance prévu par le présent règlement n'a pas été accordé, ou de coopérer d'une autre manière avec d'autres entités, conformément au droit applicable, notamment le présent règlement et le règlement (UE) 2016/794 du Parlement européen et du Conseil[29]. Les dispositions du présent règlement ne devraient pas empêcher les fournisseurs de plateformes en ligne d'utiliser ce mécanisme de signaleurs de confiance ou des mécanismes similaires pour prendre des mesures rapides et fiables contre les contenus qui sont incompatibles avec leurs conditions générales, en particulier contre les contenus qui sont préjudiciables aux destinataires vulnérables du service, tels que les mineurs.

Utilisation abusive

(63) Utiliser de manière abusive les plateformes en ligne en fournissant fréquemment des contenus manifestement illicites ou en soumettant souvent des notifications ou des réclamations manifestement infondées dans le cadre, respectivement, des mécanismes et systèmes mis en place en vertu du présent règlement nuit à la confiance et porte atteinte aux droits et intérêts légitimes des parties concernées. Il est donc nécessaire de mettre en place des garanties appropriées, proportionnées et efficaces contre de tels abus, garanties qui doivent respecter les droits et les intérêts légitimes de toutes les parties concernées, y compris les libertés et droits fondamentaux applicables consacrés par la Charte, en particulier la liberté d'expression. Il convient de considérer des informations comme des contenus manifestement illicites et des notifications ou réclamations comme manifestement infondées lorsqu'il est évident pour un profane, sans aucune analyse de fond, que le contenu est illicite ou que les notifications ou réclamations sont infondées, respectivement.

(64) Sous certaines conditions, les fournisseurs de plateformes en ligne devraient suspendre temporairement leurs activités pertinentes concernant la personne ayant un comportement abusif. Cela s'entend sans préjudice de la liberté des fournisseurs de plateformes en ligne de déterminer leurs conditions générales et d'établir des mesures plus strictes dans le cas de contenus manifestement illicites liés à des infractions graves, tels que le matériel pédopornographique. Pour des raisons de transparence, il convient que les conditions générales des plateformes en ligne fassent clairement état, et de manière suffisamment détaillée, de cette possibilité. Les décisions prises à cet égard par les fournisseurs de plateformes en ligne devraient toujours être susceptibles de recours et elles devraient être soumises au contrôle du coordinateur pour les services numériques compétent. Avant de décider de procéder à une suspension, les fournisseurs de plateformes en ligne devraient envoyer un avertissement préalable, qui devrait préciser les motifs de l'éventuelle suspension et les voies de recours disponibles contre leur décision. Lorsqu'ils décident de procéder à une suspension, les fournisseurs de plateformes en ligne devraient envoyer l'exposé des motifs conformément aux dispositions énoncées dans le présent règlement. Les règles du présent règlement relatives aux utilisations abusives ne devraient pas empêcher les fournisseurs de plateformes en ligne de prendre d'autres mesures pour lutter contre la fourniture de contenus illicites par les destinataires de leurs services ou contre tout autre usage abusif de leurs services, y compris par la violation de leurs conditions générales, conformément

29. Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

au droit de l'Union et au droit national applicables. Ces règles ne portent pas atteinte à la possibilité de tenir les personnes se livrant à une utilisation abusive pour responsables, notamment des dommages, conformément au droit de l'Union ou au droit national.

Transparence

(65) Compte tenu des responsabilités et obligations particulières des fournisseurs de plateformes en ligne, il convient de les soumettre à des obligations en matière de rapports de transparence, qui s'appliquent en sus des obligations en matière de rapports de transparence imposées à tous les fournisseurs de services intermédiaires par le présent règlement. Afin de déterminer si des plateformes en ligne et des moteurs de recherche en ligne sont susceptibles d'être, respectivement, de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne soumis à certaines obligations supplémentaires par le présent règlement, les obligations en matière de rapports de transparence applicables aux plateformes en ligne et aux moteurs de recherche en ligne devraient inclure certaines obligations relatives à la publication et à la communication d'informations sur le nombre mensuel moyen de destinataires actifs du service dans l'Union.

(66) En vue de garantir la transparence et de permettre le contrôle des décisions relatives à la modération des contenus des fournisseurs de plateformes en ligne et le suivi de la diffusion de contenus illicites en ligne, il convient que la Commission gère et publie une base de données contenant les décisions et les exposés des motifs des fournisseurs de plateformes en ligne lorsqu'ils retirent des informations ou limitent d'une autre manière la disponibilité d'informations et l'accès à des informations. Afin de maintenir la base de données constamment à jour, les fournisseurs de plateformes en ligne devraient soumettre, dans un format standard, les décisions et les exposés des motifs sans retard injustifié après avoir pris une décision, afin de permettre des mises à jour en temps réel lorsque cela est techniquement possible et proportionné aux moyens de la plateforme en ligne en question. La base de données structurée devrait permettre d'accéder aux informations pertinentes et de les rechercher, notamment en ce qui concerne le type de contenus présumés illicites en jeu.

Interface trompeuse

(67) Les interfaces en ligne trompeuses de plateformes en ligne sont des pratiques qui ont pour objectif ou pour effet d'altérer ou d'entraver sensiblement la capacité des destinataires du service de prendre une décision ou de faire un choix, de manière autonome et éclairée. Ces pratiques peuvent être utilisées pour persuader les destinataires du service de se livrer à des comportements non désirés ou de prendre des décisions non souhaitées qui ont des conséquences négatives pour eux. Par conséquent, il devrait être interdit pour les fournisseurs de plateformes en ligne de tromper ou d'encourager dans un sens les destinataires du service et d'altérer ou d'entraver l'autonomie, la prise de décision ou le choix des destinataires du service par la structure, la conception ou les fonctionnalités d'une interface en ligne ou d'une partie de celle-ci. Cela devrait comprendre, sans s'y limiter, les choix de conception abusifs destinés à amener le destinataire à exécuter des actions qui profitent au fournisseur de plateformes en ligne mais qui ne sont pas nécessairement dans l'intérêt du destinataire, en lui présentant des choix de manière biaisée, par exemple en accordant davantage d'importance à certains choix au moyen de composantes visuelles, auditives ou autres, lorsqu'il est demandé au destinataire du service de prendre une décision.

Cela devrait également inclure le fait de demander à plusieurs reprises à un destinataire du service de faire un choix lorsque ce choix a déjà été fait, de rendre la procédure d'annulation d'un service nettement plus compliquée que celle de s'y inscrire, de rendre certains choix plus difficiles ou plus longs que d'autres, de rendre excessivement difficile l'interruption des achats ou le fait de quitter une plateforme en ligne donnée permettant aux consommateurs de conclure des contrats à distance avec des professionnels, de tromper les destinataires du service en les incitant à prendre des décisions sur des transactions, ou d'appliquer des paramètres par défaut très difficiles à modifier, et d'influencer ainsi de manière excessive la prise de décision des destinataires du service, d'une manière qui altère et entrave leur autonomie, leur prise de décision et leur choix. Toutefois, les règles qui empêchent les interfaces trompeuses ne devraient pas être interprétées comme empêchant les fournisseurs d'interagir directement avec les destinataires du service et de leur proposer des services nouveaux ou supplémentaires. Les pratiques légitimes, par exemple dans le domaine de la publicité, qui sont conformes au droit de l'Union ne devraient pas en elles-mêmes être considérées comme constituant des interfaces trompeuses. Ces règles relatives aux interfaces trompeuses devraient être interprétées comme couvrant les pratiques interdites rele-

vant du champ d'application du présent règlement dans la mesure où ces pratiques ne sont pas déjà couvertes par la directive 2005/29/CE ou le règlement (UE) 2016/679.

cf. RGPD

Publicité en ligne

(68) La publicité en ligne joue un rôle important dans l'environnement en ligne, notamment en ce qui concerne la fourniture de plateformes en ligne, où la fourniture du service est parfois rémunérée, en tout ou en partie, directement ou indirectement, au moyen de recettes publicitaires. La publicité en ligne peut présenter des risques importants, qu'il s'agisse de messages publicitaires constituant eux-mêmes un contenu illicite, de la contribution à des incitations financières en faveur de la publication ou de l'amplification de contenus et d'activités illégales ou autrement préjudiciables en ligne, ou encore de la présentation discriminatoire de publicités ayant une incidence sur l'égalité de traitement et des chances des citoyens. Outre les exigences découlant de l'article 6 de la directive 2000/31/CE, il convient donc que les fournisseurs de plateformes en ligne soient tenus de veiller à ce que les destinataires du service disposent de certaines informations individualisées qui leur sont nécessaires pour comprendre quand et pour le compte de qui la publicité est présentée. Ils devraient veiller à ce que les informations soient bien visibles, notamment grâce à des signes visuels ou sonores standardisés, clairement identifiables et dépourvues d'ambiguïté pour le destinataire moyen du service, et à ce qu'elles soient adaptées à la nature de l'interface en ligne du service individuel. De plus, les destinataires du service devraient disposer d'informations, directement accessibles depuis l'interface en ligne lorsque la publicité est présentée, relatives aux principaux paramètres utilisés pour déterminer qu'une publicité spécifique leur est présentée, accompagnées d'explications judicieuses sur la logique utilisée à cette fin, notamment lorsque celle-ci est fondée sur le profilage.

Ces explications devraient comprendre des informations sur la méthode utilisée pour présenter la publicité, par exemple préciser s'il s'agit d'une publicité contextuelle ou d'un autre type de publicité et, le cas échéant, les principaux critères de profilage utilisés; elles devraient également informer le destinataire de tout moyen dont il dispose pour modifier ces critères. Les exigences du présent règlement concernant la fourniture d'informations relatives à la publicité sont sans préjudice de l'application des dispositions pertinentes du règlement (UE) 2016/679, en particulier celles relatives au droit d'opposition, à la prise de décision individuelle automatisée, y compris le profilage, et en particulier à la nécessité d'obtenir le consentement de la personne concernée avant de traiter des données à caractère personnel à des fins de publicité ciblée. De même, elles sont sans préjudice des dispositions prévues par la directive 2002/58/CE, notamment celles qui concernent le stockage d'informations dans les équipements terminaux et l'accès aux informations qui y sont stockées. Enfin, le présent règlement complète l'application de la directive 2010/13/UE, qui impose des mesures pour permettre aux utilisateurs de déclarer les communications commerciales audiovisuelles figurant dans les vidéos qu'ils ont créées. Il complète également les obligations imposées aux professionnels en vertu de la directive 2005/29/CE concernant la divulgation des communications commerciales.

cf. RGPD

(69) Lorsque les destinataires du service reçoivent des publicités fondées sur des techniques de ciblage optimisées pour répondre à leurs intérêts et potentiellement exploiter leurs vulnérabilités, cela peut avoir des effets négatifs particulièrement graves. Dans certains cas, les techniques de manipulation peuvent avoir une incidence négative sur des groupes entiers et amplifier les préjudices sociétaux, par exemple en contribuant à des campagnes de désinformation ou en pratiquant des discriminations à l'égard de certains groupes. Les plateformes en ligne sont des environnements particulièrement sensibles pour de telles pratiques et présentent un risque plus élevé pour la société. Par conséquent, les fournisseurs de plateformes en ligne ne devraient pas présenter de publicité sur la base d'un profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679, en utilisant les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, dudit règlement, y compris en utilisant des catégories de profilage fondées sur ces catégories particulières. Cette interdiction est sans préjudice des obligations applicables aux fournisseurs de plateformes en ligne ou à tout autre fournisseur de services ou annonceur participant à la diffusion des publicités en vertu du droit de l'Union en matière de protection des données à caractère personnel.

cf. RGPD

(70) La manière dont les informations sont hiérarchisées et présentées sur l'interface en ligne d'une plateforme en ligne afin de faciliter et d'optimiser l'accès aux informations pour les destinataires du service occupe une place essentielle dans les activités de la plateforme. Cela consiste, par exemple, à suggérer, classer et hiérarchiser les infor-

mations de manière algorithmique, en les distinguant par le texte ou par d'autres représentations visuelles, ou en organisant de toute autre manière les informations fournies par les destinataires. Ces systèmes de recommandation peuvent avoir une incidence significative sur la capacité des destinataires à récupérer les informations en ligne et à interagir avec elles, y compris pour faciliter la recherche d'informations pertinentes pour les destinataires du service et contribuer à améliorer l'expérience utilisateur. Ils jouent également un rôle important dans l'amplification de certains messages, la diffusion virale de l'information et la stimulation du comportement en ligne. Par conséquent, les plateformes en ligne devraient veiller en permanence à ce que les destinataires de leur service soient correctement informés de la manière dont les systèmes de recommandation ont un effet sur la manière dont l'information est affichée et peuvent influencer la manière dont les informations leur sont présentées. Elles devraient présenter clairement les paramètres de ces systèmes de recommandation d'une manière facilement compréhensible afin que les destinataires du service comprennent comment l'information est hiérarchisée à leur intention. Ces paramètres devraient inclure au moins les critères les plus importants utilisés pour déterminer les informations suggérées au destinataire du service et les raisons de leur importance respective, y compris lorsque les informations sont hiérarchisées sur la base du profilage et du comportement en ligne des destinataires.

Protection des mineurs

(71) La protection des mineurs est un objectif stratégique important de l'Union. Une plateforme en ligne peut être considérée comme accessible aux mineurs lorsque ses conditions générales permettent aux mineurs d'utiliser le service, lorsque son service s'adresse aux mineurs ou est utilisé de manière prédominante par des mineurs, ou lorsque le fournisseur sait par ailleurs que certains des destinataires de son service sont des mineurs, par exemple parce qu'il traite déjà des données à caractère personnel des destinataires de son service révélant leur âge à d'autres fins. Les fournisseurs de plateformes en ligne utilisées par des mineurs devraient prendre des mesures appropriées et proportionnées pour protéger les mineurs, par exemple en concevant leurs interfaces en ligne ou des parties de celles-ci avec le plus haut niveau de protection de la vie privée, de sécurité et de sûreté des mineurs par défaut, s'il y a lieu, ou en adoptant des normes de protection des mineurs, ou en participant à des codes de conduite pour la protection des mineurs. Ils devraient tenir compte des bonnes pratiques et des orientations disponibles, telles que celles fournies dans la communication de la Commission intitulée "Une décennie numérique pour les enfants et les jeunes: la nouvelle stratégie européenne pour un internet mieux adapté aux enfants". Les fournisseurs de plateformes en ligne ne devraient pas présenter de publicité qui repose sur le profilage utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils savent avec une certitude raisonnable que le destinataire du service est un mineur. Conformément au règlement (UE) 2016/679, et notamment au principe de minimisation des données prévu à l'article 5, paragraphe 1, point c), dudit règlement, cette interdiction ne devrait pas conduire le fournisseur de la plateforme en ligne à conserver, à acquérir ou à traiter davantage de données à caractère personnel qu'il n'en détient déjà afin d'évaluer si le destinataire du service est un mineur. Par conséquent, cette obligation ne devrait pas inciter les fournisseurs de plateformes en ligne à recueillir l'âge du destinataire du service avant l'utilisation de ces plateformes. Ceci devrait s'appliquer sans préjudice du droit de l'Union en matière de protection des données à caractère personnel.

cf. RGPD

Traçabilité des contrats en ligne

(72) Afin de contribuer à un environnement en ligne sûr, fiable et transparent pour les consommateurs, ainsi que pour les autres parties intéressées telles que les professionnels concurrents et les titulaires de droits de propriété intellectuelle, et de dissuader les professionnels de vendre des produits ou des services en violation des règles applicables, il convient que les plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels garantissent la traçabilité de ces derniers. Le professionnel devrait donc être tenu de fournir certaines informations essentielles aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, notamment aux fins de la promotion de messages concernant des produits ou l'offre de produits. Cette exigence devrait également être applicable aux professionnels qui font la promotion de messages concernant des produits ou des services pour le compte de marques, sur la base d'accords sous-jacents. Il convient que ces fournisseurs de plateformes en ligne conservent toutes les informations de manière sécurisée pendant la durée de leur relation contractuelle avec le professionnel et six mois après la fin de celle-ci, afin que toute réclamation à l'encontre du professionnel puisse être déposée ou que les injonctions le concernant puissent être respectées.

Cette obligation est nécessaire et proportionnée, de manière à ce que les autorités publiques et les parties privées ayant un intérêt légitime puissent avoir accès aux informations, dans le respect du droit applicable, y compris en matière de protection des données à caractère personnel, notamment au moyen des injonctions de fournir des informations prévues par le présent règlement. Cette obligation ne modifie en rien les éventuelles obligations de préserver des contenus déterminés pendant des périodes plus longues, sur la base d'autres dispositions du droit de l'Union ou d'autres dispositions du droit national conforme au droit de l'Union. Sans préjudice de la définition figurant dans le présent règlement, tout professionnel, qu'il s'agisse d'une personne physique ou morale, identifié sur la base de l'article 6 bis, paragraphe 1, point b), de la directive 2011/83/UE et de l'article 7, paragraphe 4, point f), de la directive 2005/29/CE devrait être traçable lorsqu'il propose un produit ou un service par l'intermédiaire d'une plateforme en ligne. La directive 2000/31/CE impose à tous les prestataires de services de la société de l'information de rendre possible un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, à certaines informations permettant l'identification de tous les prestataires. Les exigences en matière de traçabilité applicables aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, énoncées dans le présent règlement, n'affectent pas l'application de la directive (UE) 2021/514 du Conseil[30], qui poursuit d'autres objectifs légitimes d'intérêt public.

(73) Pour que cette obligation soit appliquée de manière efficace et adéquate, sans imposer de contraintes disproportionnées, les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels devraient déployer tous leurs efforts en vue d'évaluer la fiabilité des informations fournies par les professionnels concernés, notamment en utilisant des bases de données en ligne et des interfaces en ligne officielles librement accessibles, telles que les registres du commerce nationaux et le système d'échange d'informations sur la TVA, ou demander aux professionnels concernés de fournir des documents justificatifs fiables, telles que des copies de documents d'identité, des relevés de comptes de paiement certifiés, des certificats d'entreprise et des certificats d'immatriculation au registre du commerce. Ils peuvent également utiliser d'autres sources, disponibles pour une utilisation à distance, qui présentent un degré équivalent de fiabilité aux fins du respect de cette obligation. Toutefois, les fournisseurs de plateformes en ligne concernés ne devraient pas être tenus de se livrer à des recherches de faits en ligne excessives ou coûteuses ou de procéder à des vérifications disproportionnées sur place. Les fournisseurs qui ont déployé tous les efforts requis par le présent règlement ne devraient pas non plus être réputés garantir la fiabilité des informations à l'égard du consommateur ou d'autres parties intéressées.

(74) Il convient également que les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels conçoivent et organisent leur interface en ligne de manière à permettre aux professionnels de respecter les obligations qui leur incombent en vertu du droit de l'Union applicable, en particulier les exigences énoncées aux articles 6 et 8 de la directive 2011/83/UE, à l'article 7 de la directive 2005/29/CE, aux articles 5 et 6 de la directive 2000/31/CE et à l'article 3 de la directive 98/6/CE du Parlement européen et du Conseil[31]. À cette fin, les fournisseurs de plateformes en ligne concernés devraient déployer tous leurs efforts en vue d'examiner si les professionnels utilisant leurs services ont téléchargé des informations complètes sur leurs interfaces en ligne, conformément au droit de l'Union applicable pertinent. Les fournisseurs de plateformes en ligne devraient veiller à ce que les produits ou services ne soient pas proposés tant que ces informations ne sont pas complètes. Cela ne devrait pas équivaloir pour les fournisseurs de plateformes en ligne concernés à une obligation générale de surveillance des produits ou des services proposés par les professionnels par l'intermédiaire de leurs services ni à une obligation générale de recherche des faits, notamment aux fins de vérifier l'exactitude des informations fournies par les professionnels. Les interfaces en ligne devraient être faciles d'accès et faciles à utiliser pour les professionnels et les consommateurs. En outre, une fois qu'ils ont autorisé le professionnel à proposer un produit ou service, les

30. Directive (UE) 2021/514 du Conseil du 22 mars 2021 modifiant la directive 2011/16/UE relative à la coopération administrative dans le domaine fiscal (JO L 104 du 25.3.2021, p. 1).
31. Directive 98/6/CE du Parlement européen et du Conseil du 16 février 1998 relative à la protection des consommateurs en matière d'indication des prix des produits offerts aux consommateurs (JO L 80 du 18.3.1998, p. 27).

fournisseurs de plateformes en ligne concernés s'efforcent, dans la mesure du raisonnable, de contrôler aléatoirement si les produits ou services proposés ont été signalés comme étant illégaux dans des bases de données en ligne ou des interfaces en ligne officielles, librement accessibles et lisibles par une machine, disponibles dans un État membre ou dans l'Union. La Commission devrait également encourager la traçabilité des produits au moyen de solutions technologiques telles que des codes à réponse rapide signés numériquement (ou "codes QR") ou des jetons non fongibles. La Commission devrait promouvoir l'élaboration de normes et, en l'absence de ces dernières, l'élaboration de solutions fondées sur le marché qui peuvent être acceptables pour les parties concernées.

(75) Compte tenu du rôle important que jouent les très grandes plateformes en ligne, en raison de leur portée, exprimée notamment en nombre de destinataires du service, s'agissant de faciliter le débat public, les transactions économiques, et la diffusion au public d'informations, d'opinions et d'idées, et d'influencer la manière dont les destinataires obtiennent et communiquent des informations en ligne, il est nécessaire d'imposer aux fournisseurs de ces plateformes des obligations spécifiques venant s'ajouter aux obligations applicables à toutes les plateformes en ligne. En raison de leur rôle essentiel dans la localisation et la possibilité de récupérer des informations en ligne, il est également nécessaire d'imposer ces obligations, dans la mesure où elles sont applicables, aux fournisseurs de très grands moteurs de recherche en ligne. Ces obligations supplémentaires imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont nécessaires pour répondre aux considérations de politique publique, dans la mesure où il n'existe pas d'autres mesures moins restrictives qui permettraient d'atteindre effectivement le même résultat.

(76) Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne peuvent engendrer des risques pour la société, qui diffèrent, par leur ampleur et leur incidence, de ceux qui sont imputables aux plateformes de plus petite taille. Les fournisseurs de ces très grandes plateformes en ligne et de ces très grands moteurs de recherche en ligne devraient donc être soumis aux normes les plus strictes en matière d'obligations de diligence, proportionnellement à leurs effets sur la société. Lorsque le nombre de destinataires actifs d'une plateforme en ligne ou de destinataires actifs d'un moteur de recherche en ligne, calculé comme une moyenne sur une période de six mois, représente une part significative de la population de l'Union, les risques systémiques présentés par la plateforme en ligne ou le moteur de recherche en ligne peuvent produire des effets disproportionnés dans l'Union. On peut considérer qu'une portée significative est atteinte lorsque ce nombre dépasse un seuil opérationnel fixé à 45 millions, c'est-à-dire un nombre équivalent à 10 % de la population de l'Union. Ce seuil opérationnel devrait être maintenu à jour et, par conséquent, la Commission devrait être habilitée à compléter les dispositions du présent règlement en adoptant des actes délégués, si nécessaire.

cf. Actes délégués

(77) Afin de déterminer la portée d'une plateforme en ligne ou d'un moteur de recherche en ligne donné, il est nécessaire d'établir le nombre moyen de destinataires actifs de chaque service individuellement. En conséquence, le nombre moyen de destinataires mensuels actifs d'une plateforme en ligne devrait refléter tous les destinataires utilisant effectivement le service au moins une fois au cours d'une période donnée, en étant exposés à des informations diffusées sur l'interface en ligne de la plateforme en ligne, par exemple en les regardant ou en les écoutant, ou en fournissant des informations, comme les professionnels sur des plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels.

Aux fins du présent règlement, l'utilisation active ne se limite pas à interagir avec des informations en cliquant dessus, en les commentant, en les affichant en lien, en les partageant, en procédant à des achats ou en effectuant des transactions sur une plateforme en ligne. Par conséquent, la notion de destinataire actif du service ne coïncide pas nécessairement avec celle d'utilisateur inscrit d'un service. En ce qui concerne les moteurs de recherche en ligne, la notion de destinataires actifs du service devrait comprendre ceux qui consultent les informations sur leur interface en ligne, mais pas, par exemple, les propriétaires des sites internet indexés par un moteur de recherche en ligne, car ils n'utilisent pas activement le service. Le nombre de destinataires actifs d'un service devrait inclure tous les destinataires uniques du service qui utilisent activement ce service spécifique. À cet effet, un destinataire du service qui utilise différentes interfaces en ligne, telles que des sites internet ou des applications, y compris

lorsque les services sont accessibles au moyen de différents localisateurs uniformes de ressources (URL) ou noms de domaine, ne devrait, dans la mesure du possible, être comptabilisé qu'une seule fois. Toutefois, la notion de destinataire actif du service ne devrait pas inclure l'utilisation accessoire du service par les destinataires d'autres fournisseurs de services intermédiaires qui mettent indirectement à disposition des informations hébergées par le fournisseur de plateformes en ligne via la fourniture d'un lien ou l'indexation par un fournisseur de moteur de recherche en ligne.

En outre, le présent règlement n'impose pas aux fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne d'effectuer un pistage spécifique des personnes en ligne. Lorsque ces fournisseurs sont en mesure d'exclure du décompte les utilisateurs automatisés tels que les robots ou les récupérateurs d'informations ("scrapers") sans autre traitement des données à caractère personnel ni pistage, ils peuvent le faire. La détermination du nombre de destinataires actifs du service pouvant être influencée par les évolutions du marché et les évolutions techniques, la Commission devrait être habilitée à compléter les dispositions du présent règlement en adoptant des actes délégués établissant la méthode permettant de déterminer les destinataires actifs d'une plateforme en ligne ou d'un moteur de recherche en ligne, si nécessaire, en tenant compte de la nature du service et de la manière dont les destinataires du service interagissent avec celui-ci.

cf. Actes délégués

(78) Compte tenu des effets de réseau qui caractérisent l'économie des plateformes, la base d'utilisateurs d'une plateforme en ligne ou d'un moteur de recherche en ligne peut rapidement s'accroître et atteindre la dimension d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne, avec une incidence correspondante sur le marché intérieur. Cela peut se produire si une croissance exponentielle est enregistrée sur de courtes périodes, ou si l'importance de la présence et du chiffre d'affaires mondiaux de la plateforme en ligne ou du moteur de recherche en ligne lui permet d'exploiter pleinement les effets de réseau et les économies d'échelle et de gamme. Un chiffre d'affaires annuel important ou une capitalisation boursière annuelle élevée peuvent notamment être des indices de la capacité d'évolution rapide de l'audience. Dans de tels cas, le coordinateur pour les services numériques de l'État membre d'établissement ou la Commission devraient pouvoir demander au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de soumettre plus fréquemment des rapports sur le nombre de destinataires actifs du service afin de pouvoir déterminer à temps le moment à partir duquel cette plateforme ou ce moteur de recherche devrait être désigné comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement, aux fins du présent règlement.

(79) Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne peuvent être utilisés d'une manière qui a une influence considérable sur la sécurité en ligne, sur la formation de l'opinion publique et du discours, ainsi que sur le commerce en ligne. La façon dont ils conçoivent leurs services est généralement optimisée au bénéfice de leurs modèles économiques souvent axés sur la publicité et peut susciter des préoccupations sociétales. Une réglementation et une exécution efficaces sont nécessaires pour déterminer et atténuer efficacement les risques et le préjudice sociétal et économique potentiels. En vertu du présent règlement, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient donc évaluer les risques systémiques découlant de la conception, du fonctionnement et de l'utilisation de leurs services, ainsi que des abus potentiels par les destinataires du service, et devraient prendre des mesures d'atténuation appropriées, dans le respect des droits fondamentaux. Pour déterminer l'ampleur des effets et impact négatifs potentiels, les fournisseurs devraient examiner la gravité de l'impact potentiel et la probabilité de tous ces risques systémiques. Par exemple, ils pourraient évaluer si l'impact négatif potentiel peut toucher un grand nombre de personnes, déterminer son éventuelle irréversibilité ou apprécier à quel point il est difficile de remédier au problème et de revenir à la situation antérieure à l'impact potentiel.

Catégories de risques systémiques

(80) Quatre catégories de risques systémiques devraient être évaluées de manière approfondie par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. Dans la première catégorie figurent les risques associés à la diffusion de contenus illicites, tels que la diffusion de matériel pédopornographique, de discours haineux illégaux ou d'autres types d'usage abusif de leurs services dans le cadre d'infractions pénales, et la poursuite d'activités illégales, telles que la vente de produits ou de services interdits par le droit de l'Union ou le droit national, y compris des produits dangereux ou de contrefaçon, ou des animaux commercialisés

illégalement. Par exemple, cette diffusion ou ces activités peuvent constituer un risque systémique important lorsque l'accès à des contenus illicites peut se propager rapidement et largement grâce à des comptes d'une portée particulièrement large ou à d'autres moyens d'amplification. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient évaluer le risque de diffusion de contenus illicites, que l'information soit ou non également incompatible avec leurs conditions générales. Cette évaluation est sans préjudice de la responsabilité personnelle du destinataire du service de très grandes plateformes en ligne ou des propriétaires de sites internet indexés par de très grands moteurs de recherche en ligne du fait de l'éventuelle illégalité de leur activité au regard du droit applicable.

(81) La deuxième catégorie concerne l'incidence réelle ou prévisible du service sur l'exercice des droits fondamentaux, tels qu'ils sont protégés par la Charte, ce qui comprend, sans s'y limiter, la dignité humaine, la liberté d'expression et d'information, dont la liberté et le pluralisme des médias, le droit à la vie privée, la protection des données, le droit à la non-discrimination, les droits de l'enfant et la protection des consommateurs. De tels risques peuvent découler, par exemple, de la conception des systèmes algorithmiques utilisés par la très grande plateforme en ligne ou par le très grand moteur de recherche en ligne, ou de l'usage abusif de leur service par la soumission de notifications abusives ou d'autres méthodes visant à réduire au silence ou à entraver la concurrence. Lorsqu'ils évaluent les risques pour les droits de l'enfant, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient examiner par exemple à quel point la conception et le fonctionnement du service sont faciles à comprendre pour les mineurs, ainsi que la manière dont ces derniers peuvent être exposés, par le biais de leur service, à des contenus pouvant nuire à leur santé ainsi qu'à leur épanouissement physique, mental et moral. Ces risques peuvent résulter, par exemple, de la conception des interfaces en ligne qui exploitent intentionnellement ou non les faiblesses et l'inexpérience des mineurs ou qui peuvent entraîner un comportement de dépendance.

(82) La troisième catégorie de risques concerne les effets négatifs réels ou prévisibles sur les processus démocratiques, le discours civique et les processus électoraux, ainsi que sur la sécurité publique.

(83) Une quatrième catégorie de risques découle de préoccupations similaires relatives à la conception, au fonctionnement ou à l'utilisation, y compris par manipulation, de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ayant un effet négatif réel ou prévisible sur la protection de la santé publique et des mineurs, ainsi que des conséquences négatives graves sur le bien-être physique et mental d'une personne, ou sur la violence à caractère sexiste. Ces risques peuvent également résulter de campagnes de désinformation coordonnées liées à la santé publique ou de la conception d'interfaces en ligne susceptibles de stimuler les dépendances comportementales des destinataires du service.

(84) Lors de l'évaluation de ces risques systémiques, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient se concentrer sur les systèmes ou autres éléments susceptibles de contribuer aux risques, y compris tous les systèmes algorithmiques qui peuvent être concernés, en particulier leurs systèmes de recommandation et leurs systèmes publicitaires, en étant attentifs aux pratiques connexes en matière de collecte et d'utilisation des données. Ils devraient également évaluer si leurs conditions générales et la mise en application de ces dernières sont appropriées, ainsi que leurs processus de modération des contenus, leurs outils techniques et les ressources affectées. Lors de l'évaluation des risques systémiques recensés dans le présent règlement, ces fournisseurs devraient également se concentrer sur les informations qui ne sont pas illicites mais alimentent les risques systémiques recensés dans le présent règlement. Ces fournisseurs devraient donc accorder une attention particulière à la manière dont leurs services sont utilisés pour diffuser ou amplifier des contenus trompeurs ou mensongers, et notamment à la désinformation. Lorsque l'amplification algorithmique des informations contribue aux risques systémiques, ces fournisseurs devraient en tenir dûment compte dans leurs évaluations des risques. Lorsque les risques sont localisés ou qu'il existe des différences linguistiques, il y a lieu que ces fournisseurs en rendent compte également dans leurs évaluations des risques. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient, en particulier, examiner la manière dont la conception et le fonctionnement de leurs services, ainsi que l'utilisation et la manipulation intentionnelles et, souvent, coordonnées de leurs services, ou la violation systé-

mique de leurs conditions d'utilisation, contribuent à ces risques. Ces risques peuvent résulter, par exemple, de l'utilisation non authentique du service, telle que la création de faux comptes, l'utilisation de robots ou l'utilisation trompeuse d'un service, et d'autres comportements automatisés ou partiellement automatisés, susceptibles de conduire à la diffusion rapide et généralisée au public d'informations qui constituent un contenu illicite ou qui sont incompatibles avec les conditions générales d'une plateforme en ligne ou d'un moteur de recherche en ligne et qui contribuent à des campagnes de désinformation.

(85) Afin que les évaluations des risques ultérieures puissent s'appuyer les unes sur les autres et montrer l'évolution des risques recensés, ainsi que pour faciliter les enquêtes et les mesures d'exécution, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient conserver tous les documents justificatifs relatifs aux évaluations des risques qu'ils ont effectuées, tels que les informations relatives à leur préparation, les données sous-jacentes et les données sur les essais de leurs systèmes algorithmiques.

(86) Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient déployer les moyens nécessaires pour atténuer avec diligence les risques systémiques recensés dans les évaluations des risques, dans le respect des droits fondamentaux. Toute mesure adoptée devrait respecter les exigences de diligence du présent règlement, être raisonnable et atténuer efficacement les risques systémiques spécifiques recensés. Ces mesures devraient être proportionnées à la capacité économique du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et à la nécessité d'éviter des restrictions inutiles à l'utilisation de leur service, compte devant dûment être tenu des effets négatifs potentiels sur les droits fondamentaux. Ces fournisseurs devraient accorder une attention particulière aux répercussions sur la liberté d'expression.

(87) Dans le cadre de ces mesures d'atténuation, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient envisager, par exemple, d'adapter toute conception, toute caractéristique ou tout fonctionnement nécessaires de leur service, comme la conception des interfaces en ligne. Ils devraient adapter et appliquer leurs conditions générales, si nécessaire et conformément aux règles du présent règlement relatives aux conditions générales. D'autres mesures appropriées pourraient comprendre l'adaptation de leurs systèmes de modération des contenus et de leurs processus internes ou l'adaptation de leurs processus décisionnels et de leurs ressources, notamment le personnel chargé de la modération des contenus, leur formation et leur expertise locale. Cela concerne en particulier la rapidité et la qualité du traitement des notifications. À cet égard, par exemple, le code de conduite pour la lutte contre les discours haineux illégaux en ligne de 2016 fixe un critère de référence pour le traitement des notifications valides en vue du retrait des discours haineux illégaux en moins de 24 heures. Les fournisseurs de très grandes plateformes en ligne, en particulier celles qui sont principalement utilisées pour la diffusion au public de contenus pornographiques, devraient s'acquitter avec diligence de toutes les obligations qui leur incombent en vertu du présent règlement en ce qui concerne les contenus illicites constituant de la cyberviolence, en particulier les contenus pornographiques illicites, en veillant plus particulièrement à ce que les victimes puissent effectivement exercer leurs droits en lien avec des contenus constituant un partage non consensuel de contenus intimes ou de matériel manipulé, et ce en traitant rapidement les notifications et en procédant au retrait des contenus en question sans retard injustifié. D'autres types de contenus illicites peuvent nécessiter des délais plus longs ou plus courts pour le traitement des notifications, en fonction des faits, des circonstances et des types de contenus illicites en cause. Ces fournisseurs peuvent également mettre en place une coopération ou renforcer une coopération existante avec des signaleurs de confiance et organiser des sessions de formation et des échanges avec des organisations de signaleurs de confiance.

(88) Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient également faire preuve de diligence dans les mesures qu'ils prennent pour tester et, si nécessaire, adapter leurs systèmes algorithmiques, en particulier leurs systèmes de recommandation. Ils peuvent devoir atténuer les effets négatifs de recommandations personnalisées et à corriger les critères utilisés dans leurs recommandations. Les systèmes publicitaires utilisés par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne peuvent également être un catalyseur pour les risques systémiques. Ces fournisseurs devraient

envisager de prendre des mesures correctives consistant par exemple à mettre fin aux revenus publicitaires pour des informations déterminées ou d'autres mesures, telles que les mesures visant à accroître la visibilité des sources d'information faisant autorité, ou à adapter leurs systèmes publicitaires davantage sur le plan structurel. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne peuvent devoir renforcer leurs processus internes ou la surveillance d'une ou plusieurs de leurs activités, notamment en ce qui concerne la détection des risques systémiques, et procéder à des évaluations des risques plus fréquentes ou plus ciblées liées aux nouvelles fonctionnalités. En particulier, lorsque les risques sont communs à différentes plateformes en ligne ou moteurs de recherche en ligne, ils devraient coopérer avec d'autres fournisseurs de services, notamment en mettant en chantier des codes de conduite ou d'autres mesures d'autorégulation ou en adhérant à des codes de conduite ou à de telles mesures existants. Ils devraient également envisager des actions de sensibilisation, en particulier lorsque les risques sont liés à des campagnes de désinformation.

(89) Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient tenir compte de l'intérêt supérieur des mineurs lorsqu'ils prennent des mesures telles que l'adaptation de la conception de leur service et de leur interface en ligne, plus particulièrement lorsque leurs services s'adressent aux mineurs ou sont utilisés de manière prédominante par ceux-ci. Ils devraient veiller à ce que leurs services soient organisés de manière à permettre aux mineurs d'accéder facilement aux mécanismes prévus par le présent règlement, le cas échéant, y compris aux mécanismes de notification et d'action et aux mécanismes de réclamation. En outre, ils devraient prendre des mesures pour protéger les mineurs contre les contenus susceptibles de nuire à leur épanouissement physique, mental ou moral et fournir des outils permettant un accès conditionnel à ces informations. Lorsqu'ils choisissent les mesures d'atténuation appropriées, les fournisseurs peuvent prendre en compte, le cas échéant, les bonnes pratiques du secteur, y compris celles établies au moyen d'une coopération en matière d'autorégulation, telles que les codes de conduite, et devraient tenir compte des lignes directrices de la Commission.

(90) Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller à ce que leur approche de l'évaluation et de l'atténuation des risques soit fondée sur les meilleures informations et connaissances scientifiques disponibles et à mettre à l'essai leurs hypothèses auprès des groupes les plus affectés par les risques et les mesures prises. Il convient à cette fin que les fournisseurs procèdent, le cas échéant, à leurs évaluations des risques et conçoivent leurs mesures d'atténuation des risques avec la participation de représentants des destinataires du service, de représentants de groupes potentiellement affectés par leurs services, d'experts indépendants et d'organisations de la société civile. Ils devraient s'efforcer d'intégrer ces consultations, comprenant, le cas échéant, des enquêtes, des groupes de réflexion, des tables rondes et d'autres méthodes de consultation et de conception, dans leurs méthodes d'évaluation des risques et de conception des mesures d'atténuation. Lors de l'évaluation du caractère raisonnable, proportionné et efficace d'une mesure, il convient d'accorder une attention particulière au droit à la liberté d'expression.

Situation de crise

(91) En temps de crise, les fournisseurs de très grandes plateformes en ligne pourraient devoir prendre certaines mesures spécifiques d'urgence, en plus des mesures qu'ils prendraient compte tenu de leurs autres obligations au titre du présent règlement. À cet égard, il y a lieu de conclure à une crise lorsque des circonstances extraordinaires peuvent entraîner une menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de l'Union. Ces crises pourraient résulter de conflits armés ou d'actes de terrorisme, existants ou nouveaux, de catastrophes naturelles telles que des tremblements de terre et des ouragans, ainsi que de pandémies et d'autres menaces transfrontières graves pour la santé publique. La Commission devrait être en mesure d'exiger, sur recommandation du comité européen pour les services numériques (ci-après dénommé "comité"), que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne initient d'urgence une réaction aux crises. Les mesures que ces fournisseurs peuvent déterminer et envisager d'appliquer comprennent, par exemple, l'adaptation des processus de modération des contenus et l'augmentation des ressources consacrées à la modération des contenus, l'adaptation des conditions générales, des systèmes algorithmiques et des systèmes publicitaires concernés, l'intensification de la coopération avec les signaleurs de confiance, la prise de mesures de sensibilisation, la promotion d'informations

fiables et l'adaptation de la conception de leurs interfaces en ligne. Il convient de prévoir les exigences nécessaires pour garantir que ces mesures sont prises dans un délai très court et que le mécanisme de réaction aux crises n'est utilisé que lorsque, et dans la mesure où, cela est strictement nécessaire et que toute mesure prise au titre de ce mécanisme est efficace et proportionnée, compte étant dûment tenu des droits et des intérêts légitimes de toutes les parties concernées. Le recours au mécanisme devrait être sans préjudice des autres dispositions du présent règlement, telles que celles relatives à l'évaluation des risques et aux mesures d'atténuation des risques et à leur exécution, ainsi que celles relatives aux protocoles de crise.

Audit

(92) Compte tenu de la nécessité de garantir une vérification par des experts indépendants, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient être tenus de rendre des comptes, dans le cadre d'un audit indépendant, en ce qui concerne leur respect des obligations prévues dans le présent règlement et, le cas échéant, de tout engagement complémentaire pris en vertu de codes de conduite et de protocoles de crise. Afin de garantir que les audits sont réalisés de manière efficace, efficiente et en temps utile, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient fournir la coopération et l'assistance nécessaires aux organisations effectuant les audits, y compris en donnant à l'auditeur l'accès à l'ensemble des données pertinentes et aux locaux nécessaires pour effectuer correctement l'audit, y compris, le cas échéant, aux données relatives aux systèmes algorithmiques, et en répondant aux questions orales ou écrites. Les auditeurs devraient également pouvoir utiliser d'autres sources d'informations objectives, y compris des études réalisées par des chercheurs agréés. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ne sauraient entraver la réalisation de l'audit. Les audits devraient être réalisés conformément aux bonnes pratiques du secteur et en respectant un niveau élevé d'éthique professionnelle et d'objectivité, en tenant dûment compte, le cas échéant, des normes d'audit et des codes de bonnes pratiques. Les auditeurs devraient garantir la confidentialité, la sécurité et l'intégrité des informations, telles que les secrets d'affaires, qu'ils obtiennent dans l'accomplissement de leurs tâches. Cette garantie ne devrait pas être un moyen de contourner l'applicabilité des obligations en matière d'audit prévues par le présent règlement. Les auditeurs devraient disposer de l'expertise nécessaire dans le domaine de la gestion des risques et des compétences techniques pour vérifier les algorithmes. Ils devraient être indépendants, afin de pouvoir accomplir leurs tâches de manière adéquate et fiable. Ils devraient respecter les exigences fondamentales en matière d'indépendance en ce qui concerne les services extérieurs à la mission d'audit interdits, la rotation des cabinets d'audit et les honoraires non conditionnels. Si leur indépendance et leurs compétences techniques ne sont pas incontestables, ils devraient démissionner ou s'abstenir d'effectuer la mission d'audit.

(93) Le rapport d'audit devrait être étayé, afin de rendre compte de manière judicieuse des activités entreprises et des conclusions auxquelles elles ont abouti. Il devrait contribuer à nourrir la réflexion sur les mesures prises par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pour se conformer à leurs obligations au titre du présent règlement et, le cas échéant, suggérer des améliorations de ces mesures. Le rapport d'audit devrait être transmis après réception au coordinateur pour les services numériques de l'État membre d'établissement, à la Commission et au comité. Les fournisseurs devraient également transmettre sans retard injustifié, dès leur achèvement, chacun des rapports sur l'évaluation des risques et les mesures d'atténuation, ainsi que le rapport de mise en œuvre des recommandations de l'audit du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, dans lequel ces derniers indiquent comment ils ont donné suite aux recommandations de l'audit. Le rapport d'audit devrait comprendre un avis d'audit fondé sur les conclusions tirées des éléments probants recueillis dans le cadre de l'audit. Un "avis positif" devrait être rendu lorsque tous les éléments probants montrent que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne respecte les obligations prévues par le présent règlement ou, le cas échéant, les éventuels engagements qu'il ou elle a pris en vertu d'un code de conduite ou d'un protocole de crise, notamment en déterminant, en évaluant et en atténuant les risques systémiques présentés par son système et ses services. L'"avis positif" devrait être assorti de commentaires lorsque l'auditeur souhaite inclure des observations qui n'ont pas d'incidence importante sur le résultat de l'audit. Un "avis négatif" devrait être émis lorsque l'auditeur estime que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ne respecte pas le présent règlement ou les engagements pris. Lorsqu'un avis d'audit n'a pu aboutir à

aucune conclusion sur des éléments spécifiques relevant du champ de l'audit, une explication des raisons du défaut de conclusions devrait être intégrée dans l'avis d'audit. Le cas échéant, le rapport devrait comprendre une description des éléments spécifiques qui n'ont pas pu être audités, et une explication de la raison pour laquelle ils n'ont pas pu l'être.

(94) Les obligations en matière d'évaluation et d'atténuation des risques devraient entraîner, au cas par cas, la nécessité pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne d'évaluer et, si nécessaire, d'ajuster la conception de leurs systèmes de recommandation, par exemple en prenant des mesures pour prévenir et réduire le plus possible les biais qui conduisent à la discrimination de personnes en situation de vulnérabilité, en particulier lorsque cet ajustement est conforme au droit en matière de protection des données et lorsque les informations sont personnalisées en fonction de catégories particulières de données à caractère personnel visées à l'article 9 du règlement (UE) 2016/679. En outre, et en complément des obligations de transparence applicables aux plateformes en ligne en ce qui concerne leurs systèmes de recommandation, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller systématiquement à ce que les destinataires de leur service bénéficient d'autres options qui ne sont pas fondées sur le profilage, au sens du règlement (UE) 2016/679, pour les principaux paramètres de leurs systèmes de recommandation. Ces choix devraient être directement accessibles à partir de l'interface en ligne où les recommandations sont présentées.

cf. RGPD

cf. RGPD

(95) Les systèmes publicitaires utilisés par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne présentent des risques particuliers et nécessitent un contrôle public et réglementaire plus poussé en raison de leur envergure et de leur capacité à cibler et à atteindre les destinataires du service en fonction de leur comportement à l'intérieur et à l'extérieur de l'interface en ligne de cette plateforme ou de ce moteur de recherche. Les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne devraient garantir l'accès du public aux registres des publicités présentées sur leurs interfaces en ligne afin de faciliter la surveillance et les recherches relatifs aux risques émergents engendrés par la diffusion de publicités en ligne, par exemple en ce qui concerne les publicités illégales ou les techniques de manipulation et de désinformation ayant un effet négatif réel et prévisible sur la santé publique, la sécurité publique, le discours civique, la participation politique et l'égalité. Les registres devraient inclure le contenu des publicités, y compris le nom du produit, du service ou de la marque et l'objet de la publicité, et les données connexes concernant l'annonceur et, si elle est différente, la personne physique ou morale qui a financé la publicité, et la diffusion de la publicité, en particulier lorsqu'il s'agit de publicité ciblée. Ces informations devraient comprendre des informations relatives tant aux critères de ciblage qu'aux critères de diffusion, en particulier lorsque les publicités sont diffusées auprès de personnes en situation de vulnérabilité, comme les mineurs.

(96) Afin de surveiller et d'évaluer de manière appropriée le respect par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne des obligations prévues par le présent règlement, le coordinateur pour les services numériques de l'État membre d'établissement ou la Commission peut exiger l'accès à des données spécifiques ou la communication de celles-ci, y compris les données relatives aux algorithmes. Une telle exigence peut porter, par exemple, sur les données nécessaires pour évaluer les risques et les éventuels préjudices causés par les systèmes de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, les données concernant l'exactitude, le fonctionnement et les tests des systèmes algorithmiques de modération des contenus, des systèmes de recommandation ou des systèmes de publicité, y compris, le cas échéant, les données et algorithmes d'entraînement, ou encore les données concernant les processus et les résultats de la modération des contenus ou des systèmes internes de traitement des réclamations au sens du présent règlement. Ces demandes d'accès aux données ne devraient pas comprendre les demandes de production d'informations spécifiques sur des destinataires individuels du service visant à déterminer si ces destinataires respectent d'autres dispositions applicables du droit de l'Union ou du droit national. Les enquêtes menées par des chercheurs sur l'évolution et la gravité des risques systémiques en ligne sont particulièrement importantes pour corriger les asymétries d'information et établir un système résilient d'atténuation des risques, informer les fournisseurs des plateformes en ligne, les fournisseurs des

moteurs de recherche en ligne, les coordinateurs pour les services numériques, les autres autorités compétentes, la Commission et le public.

(97) Le présent règlement fournit donc un cadre permettant de contraindre à donner aux chercheurs agréés affiliés à un organisme de recherche au sens de l'article 2 de la directive (UE) 2019/790, lesquels organismes peuvent comprendre, aux fins du présent règlement, les organisations de la société civile qui mènent des recherches scientifiques dans le but principal de soutenir leur mission d'intérêt public, l'accès aux données provenant des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne. Il convient que l'ensemble des demandes d'accès aux données en vertu de ce cadre soient proportionnées et protègent de manière appropriée les droits et les intérêts légitimes, y compris les données à caractère personnel, les secrets d'affaires et autres informations confidentielles, de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et de toute autre partie concernée, y compris les destinataires du service. Toutefois, aux fins de la réalisation de l'objectif du présent règlement, la prise en compte des intérêts commerciaux des fournisseurs ne devrait pas conduire à un refus d'accès aux données nécessaires à l'objectif de recherche spécifique lié à une demande introduite au titre du présent règlement. À cet égard, sans préjudice de la directive (UE) 2016/943 du Parlement européen et du Conseil[32], les fournisseurs devraient garantir un accès approprié aux chercheurs, y compris, si nécessaire, en prenant des mesures de protection technique, par exemple par l'intermédiaire de coffres de données. Les demandes d'accès aux données pourraient, par exemple, porter sur le nombre de vues ou concerner, le cas échéant, d'autres types d'accès aux contenus par les destinataires du service avant leur retrait par les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne.

(98) En outre, lorsque les données sont accessibles au public, ces fournisseurs ne devraient pas empêcher les chercheurs répondant à un sous-ensemble approprié de critères d'utiliser ces données à des fins de recherche qui contribuent à la détection, à la détermination et à la compréhension des risques systémiques. Ils devraient fournir à ces chercheurs l'accès aux données accessibles au public, y compris, lorsque cela est techniquement possible, en temps réel, par exemple les données relatives aux interactions agrégées avec le contenu de pages publiques, de groupes publics ou de personnalités publiques, y compris les données relatives aux impressions et aux échanges, telles que le nombre de réactions, de partages et de commentaires des destinataires du service. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne devraient être encouragés à coopérer avec les chercheurs et à élargir l'accès aux données pour suivre les préoccupations sociétales grâce à des initiatives volontaires, y compris au moyen d'actions et de procédures convenus dans le cadre de codes de conduite ou de protocoles de crise. Ces fournisseurs et ces chercheurs devraient accorder une attention particulière à la protection des données à caractère personnel et veiller à ce que tout traitement de données à caractère personnel respecte le règlement (UE) 2016/679. Les fournisseurs devraient anonymiser ou pseudonymiser les données à caractère personnel, sauf dans les cas où cela rendrait impossible l'objectif de recherche poursuivi.

cf. RGPD

(99) Compte tenu de la complexité du fonctionnement des systèmes déployés et des risques systémiques qu'ils présentent pour la société, il convient que les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne établissent une fonction de contrôle de la conformité, qui devrait être indépendante des services opérationnels de ces fournisseurs. Le responsable de la fonction de contrôle de la conformité devrait être placé sous la responsabilité directe de l'organe de direction de ces fournisseurs, y compris en ce qui concerne les préoccupations liées au non-respect du présent règlement. Les responsables de la conformité qui font partie de la fonction de contrôle de la conformité devraient avoir les qualifications, les connaissances, l'expérience et les capacités nécessaires pour mettre en œuvre des mesures et contrôler le respect du présent règlement au sein de l'organisation des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devraient veiller à ce que la fonction de contrôle de la conformité

32. Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

soit associée, d'une manière appropriée et en temps utile, au traitement de toutes les questions relatives au présent règlement, y compris à la stratégie et aux mesures spécifiques d'évaluation et d'atténuation des risques ainsi que, le cas échéant, à l'évaluation du respect des engagements pris par ces fournisseurs en vertu des codes de conduite et des protocoles de crise auxquels ils ont adhéré.

(100)Compte tenu des risques accrus liés aux activités des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ainsi qu'aux obligations supplémentaires qui leur incombent en vertu du présent règlement, d'autres obligations en matière de transparence devraient leur être applicables, notamment l'obligation de faire rapport de manière exhaustive sur les évaluations des risques effectuées et les mesures ultérieures adoptées conformément au présent règlement.

Redevance de surveillance

(101)Il convient que la Commission soit en possession de toutes les ressources, quant au personnel, aux compétences et aux moyens financiers, nécessaires à l'exécution de ses missions au titre du présent règlement. Afin d'assurer la disponibilité des ressources nécessaires à une surveillance adéquate au niveau de l'Union au titre du présent règlement, et étant donné que les États membres devraient être autorisés à imposer une redevance de surveillance aux fournisseurs établis sur leur territoire pour les tâches de surveillance et d'exécution exercées par leurs autorités, la Commission devrait imposer une redevance de surveillance, dont le niveau devrait être établi sur une base annuelle, aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne. Le montant global de la redevance de surveillance annuelle imposée devrait être établi sur la base du montant global des coûts supportés par la Commission pour l'exercice de ses missions de surveillance au titre du présent règlement, raisonnablement estimé au préalable. Ce montant devrait englober les coûts liés à l'exercice des compétences et des tâches spécifiques de surveillance, d'enquête, d'exécution et de contrôle à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, notamment les coûts relatifs à la désignation des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne ou à la création, à la maintenance et à l'exploitation des bases de données envisagées au titre du présent règlement.

Il devrait comprendre également les coûts liés à la mise en place, à la maintenance et à l'exploitation de l'infrastructure institutionnelle et d'information de base aux fins de la coopération entre les coordinateurs pour les services numériques, le comité et la Commission, compte tenu du fait qu'en raison de leur taille et de leur portée, les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne ont une incidence importante sur les ressources nécessaires au fonctionnement de ces infrastructures. L'estimation des coûts globaux devrait tenir compte des coûts de surveillance supportés l'année précédente, y compris, le cas échéant, des coûts excédant la redevance de surveillance annuelle individuelle imposée l'année précédente. Les recettes affectées externes résultant de la redevance de surveillance annuelle pourraient être utilisées pour financer des ressources humaines supplémentaires, telles que des agents contractuels et des experts nationaux détachés, ainsi que d'autres dépenses liées à l'accomplissement des tâches confiées à la Commission par le présent règlement. La redevance de surveillance annuelle imposée aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne devrait être proportionnée à la taille du service, telle qu'elle résulte du nombre de destinataires actifs du service dans l'Union. En outre, la redevance de surveillance annuelle individuelle ne devrait pas dépasser un plafond global pour chaque fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, compte devant être tenu de la capacité économique du fournisseur du ou des services concernés.

Normes

(102)Pour faciliter l'application efficace et cohérente des obligations prévues par le présent règlement qui peuvent nécessiter une mise en œuvre par des moyens technologiques, il importe de promouvoir des normes volontaires portant sur certaines procédures techniques, lorsque le secteur peut contribuer à la mise au point de moyens normalisés pour aider les fournisseurs de services intermédiaires à se conformer au présent règlement, par exemple en autorisant la soumission de notifications, y compris par des interfaces de programmation d'application, ou des normes relatives aux conditions générales ou des normes en matière d'audit, ou des normes relatives à l'interopérabilité des registres de publicités. En outre, parmi ces normes pourraient figurer des normes relatives à la publicité en ligne, aux systèmes de recommandation, à l'accessibilité et à la protection des mineurs en ligne. Les fournisseurs de services intermédiaires sont libres d'adopter ces normes, mais l'adoption de celles-ci ne présume pas la

conformité au présent règlement. Dans le même temps, en fournissant de bonnes pratiques, ces normes pourraient, en particulier, être utiles pour les fournisseurs de services intermédiaires de relativement petite taille. En fonction des cas, ces normes pourraient faire la distinction entre différents types de contenus illicites ou différents types de services intermédiaires.

(103)Il convient que la Commission et le comité encouragent l'élaboration de codes de conduite volontaires ainsi que la mise en œuvre des dispositions énoncées dans ces codes pour contribuer à l'application du présent règlement. La Commission et le comité devraient se fixer comme objectif que les codes de conduite définissent clairement la nature des objectifs d'intérêt général visés, qu'ils contiennent des mécanismes d'évaluation indépendante de la réalisation de ces objectifs et que le rôle des autorités concernées soit clairement défini. Il convient d'accorder une attention particulière à la prévention des effets négatifs sur la sécurité et à la protection de la vie privée et des données à caractère personnel, ainsi qu'à l'interdiction d'imposer des obligations générales de surveillance. Bien que la mise en œuvre des codes de conduite devrait être mesurable et soumise à un contrôle public, cela ne devrait cependant pas porter atteinte au caractère volontaire de ces codes, ni à la liberté des parties intéressées de décider d'y participer ou non. Dans certaines circonstances, il est important que les très grandes plateformes en ligne coopèrent à l'élaboration de codes de conduite spécifiques et y adhèrent. Aucune disposition du présent règlement n'empêche d'autres fournisseurs de services d'adhérer aux mêmes normes de diligence, d'adopter les bonnes pratiques et de bénéficier des lignes de conduite fournies par la Commission et le comité, en souscrivant aux mêmes codes de conduite.

(104)Il convient que le présent règlement détermine certains domaines à prendre en considération pour ces codes de conduite. En particulier, des mesures d'atténuation des risques concernant des types spécifiques de contenu illicite devraient être explorées par le biais d'accords d'autorégulation et de corégulation. Un autre domaine à prendre en considération est celui des éventuelles répercussions négatives des risques systémiques sur la société et la démocratie, tels que la désinformation ou les manipulations et les abus, ou tout effet nocif sur les mineurs. Cela concerne notamment les opérations coordonnées visant à amplifier l'information, y compris la désinformation, comme l'utilisation de robots ou de faux comptes pour la création d'informations intentionnellement inexactes ou trompeuses, parfois dans le but d'obtenir un gain économique, opérations qui sont particulièrement préjudiciables aux destinataires vulnérables du service, tels que les mineurs. Dans ces domaines, l'adhésion à un code de conduite donné et son respect par une très grande plateforme en ligne ou un très grand moteur de recherche en ligne peuvent être considérés comme constituant une mesure appropriée d'atténuation des risques. Le refus, sans explications valables, par le fournisseur d'une plateforme en ligne ou d'un moteur de recherche en ligne de l'invitation de la Commission à participer à l'application d'un tel code de conduite pourrait être pris en compte, le cas échéant, pour déterminer si la plateforme en ligne ou le moteur de recherche en ligne a enfreint les obligations prévues dans le présent règlement. Le simple fait d'adhérer à un code de conduite donné et de le mettre en œuvre ne devrait pas en lui-même faire présumer que le présent règlement est respecté.

(105)Les codes de conduite devraient accroître l'accessibilité des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne, dans le respect du droit de l'Union et du droit national, afin de faciliter leur utilisation prévisible par les personnes handicapées. Les codes de conduite pourraient notamment faire en sorte que les informations soient présentées d'une manière perceptible, utilisable, compréhensible et claire et que les formulaires et mesures prévus dans le présent règlement soient faciles à trouver et accessibles aux personnes handicapées.

(106)Les règles relatives aux codes de conduite prévues par le présent règlement pourraient servir de base aux efforts d'autorégulation déjà déployés au niveau de l'Union, notamment l'engagement en matière de sécurité des produits, le protocole d'accord sur la vente de contrefaçons sur l'internet, le code de conduite pour la lutte contre les discours haineux illégaux en ligne ainsi que le code de bonnes pratiques en matière de désinformation. En ce qui concerne ce dernier en particulier, conformément aux orientations de la Commission le code de bonnes pratiques en matière de désinformation a été renforcé, comme annoncé dans le plan d'action pour la démocratie européenne.

(107)La fourniture de publicité en ligne implique généralement plusieurs acteurs, notamment des services intermédiaires qui mettent en relation les éditeurs de publicité

et les annonceurs. Les codes de conduite devraient soutenir et compléter les obligations en matière de transparence relatives à la publicité pesant sur les fournisseurs de plateformes en ligne, de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne énoncées dans le présent règlement afin de prévoir des mécanismes souples et efficaces visant à faciliter et à renforcer le respect de ces obligations, notamment en ce qui concerne les modalités de transmission des informations pertinentes. Il devrait notamment s'agir de faciliter la transmission des informations sur l'annonceur qui paie la publicité lorsqu'il diffère de la personne physique ou morale pour le compte de laquelle la publicité est présentée sur l'interface en ligne d'une plateforme en ligne. Les codes de conduite devraient également comprendre des mesures visant à garantir que des informations utiles sur la monétisation des données sont correctement partagées tout au long de la chaîne de valeur. La participation d'un large éventail de parties prenantes devrait garantir que ces codes de conduite bénéficient d'un large soutien, sont techniquement solides, efficaces et offrent le plus haut niveau de facilité d'utilisation afin que les obligations en matière de transparence atteignent leurs objectifs. Afin de garantir l'efficacité des codes de conduite, la Commission devrait prévoir des mécanismes d'évaluation lors de l'élaboration des codes de conduite. Le cas échéant, la Commission peut inviter l'Agence des droits fondamentaux ou le Contrôleur européen de la protection des données à donner son avis sur le code de conduite qui le concerne.

(108)Outre le mécanisme de réaction aux crises pour les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, la Commission peut entreprendre l'élaboration de protocoles de crise volontaires pour coordonner une réponse rapide, collective et transfrontière dans l'environnement en ligne. Cela peut ainsi être le cas lorsque les plateformes en ligne sont utilisées de manière abusive, par exemple, pour la diffusion rapide de contenus illicites ou de désinformation ou lorsqu'il est nécessaire de diffuser rapidement des informations fiables. Compte tenu du rôle important des très grandes plateformes en ligne dans la diffusion de l'information dans nos sociétés et au-delà des frontières, il convient d'encourager les fournisseurs de ces plateformes à élaborer et à appliquer des protocoles de crise spécifiques. Ces protocoles de crise ne devraient être activés que pour une période limitée et les mesures adoptées devraient également être limitées à ce qui est strictement nécessaire pour faire face à la circonstance extraordinaire considérée. Ces mesures devraient être cohérentes avec le présent règlement et ne devraient pas constituer, pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne participants, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni de rechercher activement des faits ou des circonstances indiquant un contenu illicite.

Autorité de surveillance

(109)Afin de contrôler et de faire respecter de manière adéquate les obligations prévues par le présent règlement, les États membres devraient désigner au moins une autorité qui serait chargée de surveiller l'application du présent règlement et de le faire respecter, sans préjudice de la possibilité de désigner une autorité existante ni de la forme juridique de celle-ci conformément au droit national. En fonction de leur structure constitutionnelle, organisationnelle et administrative nationale, les États membres devraient toutefois pouvoir confier des missions et des pouvoirs spécifiques de surveillance ou d'exécution en ce qui concerne l'application du présent règlement à plusieurs autorités compétentes, par exemple dans des secteurs spécifiques où des autorités existantes peuvent également être chargées de ces tâches, telles que les régulateurs des communications électroniques, les régulateurs des médias ou les autorités chargées de la protection des consommateurs. Dans l'exécution de leurs missions, toutes les autorités compétentes devraient contribuer à la réalisation des objectifs du présent règlement, à savoir le bon fonctionnement du marché intérieur des services intermédiaires, au sein duquel des règles harmonisées pour un environnement en ligne sûr, prévisible et fiable, propice à l'innovation, et en particulier les obligations de diligence applicables aux différentes catégories de fournisseurs de services intermédiaires, font l'objet d'une surveillance et d'une mise en application effectives, aux fins d'une protection efficace des droits fondamentaux consacrés dans la Charte, dont notamment le principe de protection des consommateurs. Le présent règlement n'impose pas aux États membres de confier aux autorités compétentes la mission de se prononcer sur la licéité d'éléments de contenus spécifiques.

(110)Compte tenu de la nature transfrontière des services en cause et de la portée horizontale des obligations introduites par le présent règlement, une autorité désignée pour surveiller l'application du présent règlement et, si nécessaire, le faire respecter devrait

être désignée en tant que coordinateur pour les services numériques dans chaque État membre. Lorsque plusieurs autorités compétentes sont désignées pour surveiller l'application du présent règlement et le faire respecter, une seule autorité dans cet État membre devrait être désignée en tant que coordinateur pour les services numériques. Il convient que le coordinateur pour les services numériques fasse office de point de contact unique concernant toutes les questions liées à l'application du présent règlement pour la Commission, le comité, les coordinateurs pour les services numériques des autres États membres, ainsi que pour les autres autorités compétentes de l'État membre en question. En particulier, lorsque, dans un État membre donné, plusieurs autorités compétentes sont chargées de missions au titre du présent règlement, le coordinateur pour les services numériques devrait assurer la coordination et la coopération avec ces autorités conformément aux dispositions du droit national fixant leurs missions respectives et sans préjudice de l'évaluation indépendante des autres autorités compétentes. Sans que cela ne suppose une supériorité hiérarchique sur d'autres autorités compétentes dans l'exercice de leurs missions, le coordinateur pour les services numériques devrait veiller à une participation effective de toutes les autorités compétentes concernées et faire rapport en temps utile sur leur évaluation dans le cadre de la coopération en matière de surveillance et d'exécution au niveau de l'Union. De plus, en complément des mécanismes spécifiques prévus dans le présent règlement en ce qui concerne la coopération au niveau de l'Union, l'État membre devrait également veiller à la coopération entre le coordinateur pour les services numériques et les autres autorités compétentes désignées au niveau national, le cas échéant, au moyen d'instruments appropriés, tels que la mise en commun des ressources, des groupes de travail communs, des enquêtes communes et des mécanismes d'assistance mutuelle.

(111)Le coordinateur pour les services numériques, de même que les autorités compétentes désignées en vertu du présent règlement, jouent un rôle crucial pour assurer l'effectivité des droits et obligations prévus par le présent règlement et la réalisation de ses objectifs. En conséquence, il est nécessaire de veiller à ce que ces autorités disposent des moyens nécessaires, y compris des ressources financières et humaines, pour surveiller tous les fournisseurs de services intermédiaires relevant de leur compétence, dans l'intérêt de tous les citoyens de l'Union. Compte tenu de la diversité des fournisseurs de services intermédiaires et du fait qu'ils utilisent des technologies avancées pour fournir leurs services, il est également essentiel que le coordinateur pour les services numériques et les autorités compétentes concernées soient dotés du nombre nécessaire d'agents et d'experts possédant des compétences spécialisées et des moyens techniques avancés, et qu'ils gèrent de manière autonome les ressources financières requises pour s'acquitter de leurs missions. En outre, le niveau des ressources devrait être adapté à la taille, à la complexité et à l'impact potentiel sur la société des fournisseurs de services intermédiaires relevant de leur compétence, ainsi qu'à la portée de leurs services dans l'Union. Le présent règlement est sans préjudice de la possibilité pour les États membres d'établir des mécanismes de financement fondés sur une redevance de surveillance imposée aux fournisseurs de services intermédiaires en vertu du droit national en conformité avec le droit de l'Union, pour autant qu'elle soit perçue auprès de fournisseurs de services intermédiaires ayant leur établissement principal dans l'État membre en question, qu'elle soit strictement limitée à ce qui est nécessaire et proportionné pour couvrir les coûts liés à l'accomplissement des tâches confiées aux autorités compétentes en vertu du présent règlement, à l'exclusion des tâches confiées à la Commission, et qu'une transparence suffisante soit assurée quant à la perception et à l'utilisation d'une telle redevance de surveillance.

(112)Les autorités compétentes désignées au titre du présent règlement devraient également agir en toute indépendance par rapport aux organismes privés et publics, sans obligation ni possibilité de solliciter ou de recevoir des instructions, y compris du gouvernement, et sans préjudice des obligations spécifiques de coopérer avec d'autres autorités compétentes, les coordinateurs pour les services numériques, le comité et la Commission. Toutefois, l'indépendance desdites autorités ne devrait pas signifier qu'elles ne peuvent pas être soumises, dans le respect des constitutions nationales et sans que cela mette en péril la réalisation des objectifs du présent règlement, à des mécanismes de responsabilisation proportionnés portant sur les activités générales des coordinateurs pour les services numériques, telles que leurs dépenses financières ou la présentation de rapports aux parlements nationaux. L'exigence d'indépendance ne devrait pas non plus faire obstacle à l'exercice d'un contrôle juridictionnel ni à la possibilité de consulter d'autres autorités nationales, y compris, le cas échéant, les autorités répressives, les autorités de gestion des crises ou les autorités chargées de la protection des consommateurs, ou de procéder à des échanges de vues réguliers avec

ces autorités pour se tenir mutuellement informées des enquêtes en cours, sans porter atteinte à l'exercice de leurs pouvoirs respectifs.

(113)Les États membres peuvent désigner une autorité nationale existante pour assumer la fonction de coordinateur pour les services numériques ou lui confier les missions spécifiques de surveiller l'application du présent règlement et de le faire respecter, à condition que cette autorité désignée respecte les exigences fixées dans le présent règlement, notamment en ce qui concerne son indépendance. En outre, il n'est en principe pas exclu que les États membres puissent procéder à un regroupement de fonctions au sein d'une autorité existante, dans le respect du droit de l'Union. Les mesures à cet effet peuvent comprendre, entre autres, l'interdiction de révoquer le président ou un membre du conseil d'administration d'un organe collégial d'une autorité existante avant l'expiration de leur mandat, au seul motif qu'une réforme institutionnelle a eu lieu impliquant le regroupement de différentes fonctions au sein d'une autorité, en l'absence de règles garantissant que ces révocations ne compromettent pas l'indépendance et l'impartialité de ces membres.

(114)Les États membres devraient doter le coordinateur pour les services numériques, et toute autre autorité compétente désignée en vertu du présent règlement, de pouvoirs et de moyens suffisants pour rendre effectives leurs activités en matière d'enquête et de d'exécution, conformément aux missions qui leur sont confiées. Cela comprend le pouvoir des autorités compétentes d'adopter des mesures provisoires conformément au droit national en cas de risque de préjudice grave. Ces mesures provisoires, qui peuvent inclure des injonctions de mettre fin ou de remédier à une infraction alléguée donnée, ne devraient pas aller au-delà de ce qui est nécessaire pour veiller à ce qu'un préjudice grave soit évité dans l'attente de la décision définitive. Il convient notamment que le coordinateur pour les services numériques puisse rechercher et obtenir des informations qui se trouvent sur le territoire de son État membre, y compris dans le cadre d'enquêtes conjointes, en tenant dûment compte du fait que les mesures de surveillance et d'exécution concernant un fournisseur relevant de la compétence d'un autre État membre ou de la Commission devraient être adoptées par le coordinateur pour les services numériques de cet autre État membre, le cas échéant conformément aux procédures relatives à la coopération transfrontière, ou, selon le cas, par la Commission.

Dispositions en droit national

(115)Conformément au droit de l'Union et en particulier au présent règlement et à la Charte, les États membres devraient définir en détail dans leur droit national les conditions et limites de l'exercice des pouvoirs d'enquête et d'exécution de leurs coordinateurs pour les services numériques, et, le cas échéant, d'autres autorités compétentes au titre du présent règlement.

(116)Dans l'exercice de ces pouvoirs, les autorités compétentes devraient respecter les règles nationales applicables concernant les procédures et les aspects tels que la nécessité de disposer d'une autorisation judiciaire préalable pour pénétrer dans certains locaux ainsi que le secret professionnel. Ces dispositions devraient en particulier garantir le respect des droits fondamentaux à un recours effectif et à un procès équitable, y compris les droits de la défense, ainsi que du droit au respect de la vie privée. À cet égard, les garanties prévues en ce qui concerne les procédures de la Commission en vertu du présent règlement pourraient constituer une référence appropriée. Avant qu'une décision définitive soit prise, il convient de garantir une procédure préalable, équitable et impartiale, y compris le droit des personnes concernées d'être entendues et d'avoir accès au dossier, dans le respect de la confidentialité et du secret professionnel et d'affaires, ainsi que de l'obligation de dûment motiver les décisions. Toutefois, cela ne devrait pas empêcher que des mesures soient prises, dans des cas d'urgence dûment justifiés et sous réserve de conditions et de modalités procédurales appropriées. Il convient que l'exercice de ces pouvoirs soit également proportionné, entre autres, à la nature de l'infraction ou de l'infraction présumée et au préjudice global, réel ou potentiel, qui en découle. Les autorités compétentes devraient tenir compte de tous les faits et circonstances pertinents de l'affaire, y compris des informations recueillies par les autorités compétentes d'autres États membres.

Sanctions

(117)Les États membres devraient veiller à ce que les infractions aux obligations prévues par le présent règlement puissent être sanctionnés d'une manière efficace, proportionnée et dissuasive, en fonction de la nature, de la gravité, de la récurrence et de la durée de l'infraction, compte tenu de l'objectif d'intérêt général poursuivi, de l'ampleur et de la nature des activités menées, ainsi que de la capacité économique de

l'auteur de l'infraction. En particulier, les sanctions devraient tenir compte du fait que le fournisseur de services intermédiaires concerné manque systématiquement ou de manière récurrente aux obligations qui lui incombent en vertu du présent règlement, ainsi que, le cas échéant, du nombre de destinataires du service affectés, du caractère intentionnel ou négligent de l'infraction et du fait que le fournisseur exerce ses activités dans plusieurs États membres. Lorsque le présent règlement prévoit un montant maximal pour les amendes ou les astreintes, ce montant maximal devrait s'appliquer pour chaque infraction au présent règlement et sans préjudice de la modulation des amendes ou des astreintes en ce qui concerne des infractions spécifiques. Les États membres devraient veiller à ce que l'imposition d'amendes ou d'astreintes en cas d'infraction soit effective, proportionnée et dissuasive dans chaque cas particulier en établissant des règles et procédures nationales conformément au présent règlement, en tenant compte de tous les critères concernant les conditions générales d'imposition des amendes ou des astreintes.

(118)Afin de garantir l'exécution effective des obligations fixées dans le présent règlement, il convient que les particuliers ou les organisations représentatives puissent introduire toute plainte relative au respect de ces obligations auprès du coordinateur pour les services numériques du territoire où ils ont été destinataires du service, sans préjudice des règles du présent règlement en matière de répartition des compétences et des règles applicables en matière de traitement des plaintes conformément aux principes nationaux de bonne administration. Les plaintes pourraient donner un aperçu fidèle des préoccupations suscitées par un fournisseur de services intermédiaire déterminé quant au respect du présent règlement et pourraient également informer le coordinateur pour les services numériques de toute autre question de nature transversale. Le coordinateur pour les services numériques devrait impliquer d'autres autorités nationales compétentes ainsi que le coordinateur pour les services numériques d'un autre État membre, et en particulier celui de l'État membre où le fournisseur de services intermédiaires concerné est établi, si la question nécessite une coopération transfrontière.

(119)Les États membres devraient veiller à ce que les coordinateurs pour les services numériques puissent prendre des mesures qui permettent de lutter effectivement contre certaines infractions particulièrement graves et persistantes au présent règlement et qui soient proportionnées auxdites infractions. Il convient d'exiger, en particulier lorsque ces mesures sont susceptibles de porter atteinte aux droits et intérêts de tiers, comme cela peut être le cas notamment lorsque l'accès à des interfaces en ligne est restreint, que lesdites mesures soient assorties de garanties supplémentaires En particulier, les tiers potentiellement affectés devraient avoir la possibilité d'être entendus et ces injonctions ne devraient être émises que lorsqu'il n'est pas raisonnablement possible de recourir aux pouvoirs conférés par d'autres actes du droit de l'Union ou du droit national pour adopter de telles mesures, par exemple pour protéger les intérêts collectifs des consommateurs, pour assurer le retrait rapide des pages internet contenant ou diffusant de la pédopornographie ou pour rendre impossible l'accès à des services qui sont utilisés par un tiers pour porter atteinte à un droit de propriété intellectuelle.

(120)Une telle injonction visant à restreindre l'accès ne devrait pas excéder ce qui est nécessaire pour atteindre l'objectif poursuivi. À cette fin, elle devrait être temporaire et être destinée, en principe à un fournisseur de services intermédiaires, tel que le fournisseur de services d'hébergement concerné, le fournisseur de services internet, le registre du domaine ou le bureau d'enregistrement concerné, qui est raisonnablement en mesure d'atteindre cet objectif sans restreindre indûment l'accès aux informations licites.

(121)Sans préjudice des dispositions relatives à l'exemption de responsabilité prévues dans le présent règlement en ce qui concerne les informations transmises ou stockées à la demande d'un destinataire du service, un fournisseur de services intermédiaires devrait être tenu responsable des préjudices subis par les destinataires du service causés par une violation par ledit fournisseur des obligations énoncées dans le présent règlement. L'indemnisation devrait se faire conformément aux règles et procédures définies dans le droit national applicable et sans préjudice d'autres possibilités de recours prévues par les règles relatives à la protection des consommateurs.

(122)Il convient que le coordinateur pour les services numériques publie régulièrement, par exemple sur son site internet, un rapport sur les activités menées au titre du présent règlement. En particulier, le rapport devrait être publié dans un format lisible

par une machine et comporter un aperçu des plaintes reçues et de leur suivi, notamment le nombre global de plaintes reçues et le nombre de plaintes ayant conduit à l'ouverture d'une enquête formelle ou à une transmission à d'autres coordinateurs pour les services numériques, sans faire référence à des données à caractère personnel. Dans la mesure où le coordinateur pour les services numériques est également informé des injonctions d'agir contre des contenus illicites ou de fournir, par l'intermédiaire du système de partage d'informations, des informations régies par le présent règlement, il devrait inclure dans son rapport annuel le nombre et les catégories d'injonctions de ce type émises à l'encontre des fournisseurs de services intermédiaires par les autorités judiciaires et administratives de son État membre.

(123)Par souci de clarté, de simplicité et d'efficacité, les pouvoirs de surveillance et d'exécution des obligations prévues au présent règlement devraient être conférés aux autorités compétentes de l'État membre dans lequel se trouve l'établissement principal du fournisseur de services intermédiaires, c'est-à-dire dans lequel le fournisseur a son administration centrale ou son siège statutaire au sein duquel sont exercés les principales fonctions financières ainsi que le contrôle opérationnel. En ce qui concerne les fournisseurs qui ne sont pas établis dans l'Union, mais qui proposent des services dans l'Union et relèvent donc du champ d'application du présent règlement, l'État membre dans lequel ces fournisseurs ont désigné leur représentant légal devrait être compétent, compte tenu de la fonction de représentant légal prévue par le présent règlement. Toutefois, dans l'intérêt d'une application effective du présent règlement, lorsqu'un fournisseur n'a pas désigné de représentant légal, tous les États membres ou la Commission, selon le cas, devraient être compétents. Cette compétence peut être exercée par toute autorité compétente ou la Commission, pour autant que le fournisseur ne fasse pas l'objet d'une procédure d'exécution portant sur les mêmes faits par une autre autorité compétente ou la Commission. Afin que le principe non bis in idem soit respecté, et notamment afin d'éviter que la même infraction aux obligations définies dans le présent règlement ne soit sanctionnée plus d'une fois, chaque État membre qui entend exercer sa compétence à l'égard de tels fournisseurs devrait, sans retard injustifié, en informer toutes les autres autorités, y compris la Commission, au moyen du système de partage d'informations mis en place aux fins du présent règlement.

(124)Compte tenu de leur effet potentiel et des difficultés que comporte leur surveillance effective, des règles spéciales de surveillance et d'exécution sont nécessaires à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. La Commission devrait être chargée, le cas échéant avec le concours des autorités nationales compétentes, de surveiller et de faire respecter par les autorités publiques l'obligation de gérer les questions systémiques, notamment les questions ayant un impact important sur les intérêts collectifs des destinataires du service. Par conséquent, la Commission devrait disposer de pouvoirs exclusifs de surveillance et d'exécution des obligations supplémentaires de gestion des risques systémiques imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne par le présent règlement. Les pouvoirs exclusifs de la Commission devraient s'entendre sans préjudice de certaines tâches administratives confiées par le présent règlement aux autorités compétentes des États membres d'établissement, telles que l'agrément des chercheurs.

(125)Les pouvoirs de surveillance et d'exécution des obligations de diligence, autres que les obligations supplémentaires de gestion des risques systémiques imposées par le présent règlement aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, devraient être partagés par la Commission et les autorités nationales compétentes. D'une part, la Commission pourrait très souvent être mieux placée pour remédier aux infractions systémiques commises par ces fournisseurs, comme les infractions qui touchent plusieurs États membres, les infractions graves répétées ou l'absence de mise en place des mécanismes efficaces requis par le présent règlement. D'autre part, les autorités compétentes de l'État membre dans lequel se trouve l'établissement principal d'un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne pourraient être mieux placées pour remédier aux infractions particulières commises par ces fournisseurs lorsqu'elles ne soulèvent pas de questions systémiques ou transfrontières. Dans un souci d'efficience, afin d'éviter les doubles emplois et de veiller au respect du principe non bis in idem, c'est à la Commission qu'il devrait appartenir d'évaluer si elle juge approprié d'exercer ces compétences partagées dans un cas donné et, lorsqu'elle a engagé la procédure, les États membres ne devraient plus avoir la faculté de le faire. Les États membres devraient coopérer étroitement à la fois entre eux et avec la Com-

mission et la Commission devrait coopérer étroitement avec les États membres afin d'assurer le bon fonctionnement et l'efficacité du système de surveillance et d'exécution mis en place par le présent règlement.

(126)Les règles de répartition des compétences prévues par le présent règlement devraient s'appliquer sans préjudice des dispositions du droit de l'Union et des règles nationales de droit international privé relatives à la juridiction et à la loi applicable en matière civile et commerciale, telles que les procédures engagées par des consommateurs devant les juridictions de l'État membre où ils sont domiciliés conformément aux dispositions pertinentes du droit de l'Union. En ce qui concerne les obligations, imposées aux fournisseurs de services intermédiaires par le présent règlement, d'informer l'autorité d'émission de la suite donnée aux injonctions d'agir contre des contenus illicites et aux injonctions de fournir des informations, les règles de répartition des compétences ne devraient s'appliquer qu'à la surveillance du respect de ces obligations, mais pas aux autres aspects de l'injonction, telle que la compétence d'émettre l'injonction.

(127)Compte tenu de l'aspect transfrontière et transsectoriel des services intermédiaires, une coopération à haut niveau est nécessaire pour veiller à l'application cohérente du présent règlement et à la disponibilité des informations pertinentes pour l'exercice des tâches d'exécution par l'intermédiaire du système de partage d'informations. La coopération peut prendre différentes formes en fonction des questions en jeu, sans préjudice des exercices d'enquêtes communes. Il est en tout état de cause nécessaire que le coordinateur pour les services numériques de l'État membre d'établissement d'un fournisseur de services intermédiaires informe les autres coordinateurs pour les services numériques des questions et des enquêtes concernant un fournisseur et des mesures qui vont être prises à l'égard de ce fournisseur. En outre, lorsqu'une autorité compétente d'un État membre détient des informations pertinentes pour une enquête menée par les autorités compétentes de l'État membre d'établissement, ou est en mesure de recueillir sur son territoire de telles informations auxquelles les autorités compétentes de l'État membre d'établissement n'ont pas accès, le coordinateur pour les services numériques de l'État membre de destination devrait prêter son concours en temps utile au coordinateur pour les services numériques de l'État membre d'établissement, y compris dans le cadre de l'exercice de ses pouvoirs d'enquête conformément aux procédures nationales applicables et à la Charte. Le destinataire de ces mesures d'enquête devrait s'y conformer et être tenu responsable en cas de manquement, et les autorités compétentes de l'État membre d'établissement devraient pouvoir se fier aux informations recueillies dans le cadre de l'assistance mutuelle, afin de garantir le respect du présent règlement.

(128)Le coordinateur pour les services numériques de l'État membre de destination, en particulier sur la base de plaintes reçues ou, le cas échéant, de la contribution d'autres autorités nationales compétentes ou du comité, dans le cas de questions concernant plus de trois États membres, devrait pouvoir demander au coordinateur pour les services numériques de l'État membre d'établissement de prendre des mesures d'enquête ou d'exécution à l'égard d'un fournisseur relevant de sa compétence. Ces demandes de mesures devraient reposer sur des éléments de preuve bien étayés démontrant l'existence d'une infraction alléguée ayant une incidence négative sur les intérêts collectifs des destinataires du service dans son État membre ou ayant une incidence négative pour la société. Le coordinateur pour les services numériques de l'État membre d'établissement devrait pouvoir recourir à l'assistance mutuelle ou inviter le coordinateur pour les services numériques demandeur à participer à une enquête commune si des informations supplémentaires sont nécessaires pour prendre une décision, sans qu'il soit fait obstacle à la possibilité d'inviter la Commission à évaluer le cas s'il a des raisons de soupçonner qu'une infraction systémique commise par une très grande plateforme en ligne ou un très grand moteur de recherche en ligne puisse être en cause.

(129)Il convient que le comité puisse saisir la Commission s'il n'est pas d'accord avec les évaluations ou les mesures prises ou proposées ou si aucune mesure n'a été prise conformément au présent règlement à la suite d'une demande de coopération transfrontière ou d'enquête commune. Lorsque la Commission, sur la base des informations mises à disposition par les autorités concernées, considère que les mesures proposées, y compris le niveau des amendes proposé, ne permettent pas de garantir l'exécution effective des obligations prévues dans le présent règlement, elle devrait par conséquent pouvoir exprimer ses sérieux doutes et demander au coordinateur pour

les services numériques compétent de réévaluer la question et de prendre, dans un délai déterminé, les mesures nécessaires pour assurer le respect du présent règlement. Cette possibilité est sans préjudice de l'obligation générale faite à la Commission de surveiller l'application du droit de l'Union et, si nécessaire, de le faire respecter, sous le contrôle de la Cour de justice de l'Union européenne, conformément aux traités.

(130)Afin de faciliter la surveillance et les enquêtes transfrontières portant sur les obligations fixées dans le présent règlement impliquant plusieurs États membres, les coordinateurs pour les services numériques de l'État membre d'établissement devraient pouvoir, par l'intermédiaire du système de partage d'informations, inviter d'autres coordinateurs pour les services numériques à participer à une enquête commune concernant une infraction alléguée au présent règlement. D'autres coordinateurs pour les services numériques et, le cas échéant, d'autres autorités compétentes devraient pouvoir prendre part à l'enquête proposée par le coordinateur pour les services numériques de l'État membre d'établissement, à moins que ce dernier ne considère qu'un nombre excessif d'autorités participantes risque de nuire à l'efficacité de l'enquête compte tenu des caractéristiques de l'infraction alléguée et de l'absence d'effets directs sur les destinataires du service dans ces États membres. Les activités menées dans le cadre des enquêtes communes peuvent comprendre des mesures très diverses qui doivent être coordonnées par le coordinateur pour les services numériques de l'État membre d'établissement conformément aux disponibilités des autorités participantes, telles que des exercices de collecte coordonnée de données, la mise en commun des ressources, des groupes de travail, des demandes coordonnées d'informations ou des inspections communes de locaux. Toutes les autorités compétentes participant à une enquête commune devraient coopérer avec le coordinateur pour les services numériques de l'État membre d'établissement, notamment en exerçant leurs pouvoirs d'enquête sur leur territoire, conformément aux procédures nationales applicables. L'enquête commune devrait se conclure dans un délai déterminé par un rapport final tenant compte de la contribution de toutes les autorités compétentes participantes. Le comité peut également, à la demande d'au moins trois coordinateurs pour les services numériques d'États membres de destination, recommander à un coordinateur pour les services numériques d'un État membre d'établissement de lancer une telle enquête commune et donner des indications sur son organisation. Afin d'éviter les blocages, le comité devrait pouvoir saisir la Commission dans des cas précis, notamment lorsque le coordinateur pour les services numériques de l'État membre d'établissement refuse de lancer l'enquête et que le comité n'est pas d'accord avec la justification donnée.

(131)Afin d'assurer une application cohérente du présent règlement, il est nécessaire de créer un groupe consultatif indépendant au niveau de l'Union, un comité européen pour les services numériques, qui devrait soutenir la Commission et aider à coordonner les actions des coordinateurs pour les services numériques. Le comité devrait être composé des coordinateurs pour les services numériques, lorsque ceux-ci ont été désignés, sans préjudice de la possibilité pour ces derniers d'inviter à ses réunions ou de nommer des délégués ad hoc d'autres autorités compétentes chargées de tâches spécifiques au titre du présent règlement, lorsque cela est nécessaire en vertu de la répartition nationale des tâches et des compétences. Si plusieurs participants d'un État membre sont présents, le droit de vote devrait rester limité à une voix par État membre.

(132)Le comité devrait contribuer à définir une vision commune de l'Union concernant l'application cohérente du présent règlement et à la coopération entre les autorités compétentes, notamment en conseillant la Commission et les coordinateurs pour les services numériques sur les mesures d'enquête et d'exécution appropriées, en particulier à l'égard des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et compte tenu, notamment, de la liberté des fournisseurs de services intermédiaire de fournir des services dans toute l'Union. Le comité devrait également contribuer à l'élaboration de modèles et de codes de conduite pertinents et à l'analyse des nouvelles tendances générales qui se dessinent dans le développement des services numériques dans l'Union, notamment en émettant des avis ou des recommandations sur les questions ayant trait aux normes.

(133)À cette fin, le comité devrait pouvoir adopter des avis, des demandes et des recommandations adressés aux coordinateurs pour les services numériques ou à d'autres autorités nationales compétentes. Bien que ces actes ne soient pas juridiquement contraignants, toute décision de s'en écarter devrait être assortie d'une explica-

tion adéquate et pourrait être prise en compte par la Commission lors de l'évaluation du respect du présent règlement par l'État membre concerné.

(134)Le comité devrait réunir les représentants des coordinateurs pour les services numériques et éventuellement d'autres autorités compétentes sous la présidence de la Commission, en vue de garantir, pour l'évaluation des questions qui lui sont soumises, une dimension pleinement européenne. Eu égard à d'éventuels éléments de nature transversale susceptibles de présenter un intérêt pour d'autres cadres réglementaires au niveau de l'Union, le comité devrait être autorisé à coopérer avec d'autres organes, organismes, agences et groupes consultatifs de l'Union ayant des responsabilités dans des domaines tels que l'égalité, y compris l'égalité des genres, la non-discrimination, la protection des données, les communications électroniques, les services audiovisuels, la détection des fraudes au détriment du budget de l'Union en matière de droits de douane et les enquêtes en la matière, la protection des consommateurs ou le droit de la concurrence, dans la mesure où cela est nécessaire à l'accomplissement de ses tâches.

(135)La Commission, par l'intermédiaire du président, devrait participer au comité sans droit de vote. Par l'intermédiaire du président, la Commission devrait veiller à ce que l'ordre du jour des réunions soit établi conformément aux demandes des membres du comité, comme le prévoit le règlement intérieur, et conformément aux tâches du comité telles qu'elles sont définies dans le présent règlement.

(136)Ses activités devant bénéficier d'un soutien, il convient que le comité puisse s'appuyer sur les compétences et les ressources humaines de la Commission et des autorités nationales compétentes. Il y a lieu de préciser les modalités opérationnelles spécifiques du fonctionnement interne du comité dans le règlement intérieur de celui-ci.

(137)Compte tenu de l'importance des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne, eu égard à leur portée et à leur poids, leur manquement aux obligations spécifiques qui leur sont applicables est susceptible d'affecter un nombre substantiel de destinataires des services dans différents États membres et peut causer des préjudices importants à la société, alors même qu'il peut aussi être particulièrement complexe de détecter ces manquements et d'y remédier. Pour ce motif, la Commission devrait, en coopération avec les coordinateurs pour les services numériques et le comité, développer l'expertise et les capacités de l'Union en ce qui concerne la surveillance des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne. Le Commission devrait donc être en mesure de coordonner et d'utiliser l'expertise et les ressources de ces autorités, par exemple en analysant, à titre permanent ou temporaire, les tendances spécifiques ou les questions qui émergent en ce qui concerne une ou plusieurs très grandes plateformes en ligne ou un ou plusieurs très grands moteurs de recherche en ligne. Les États membres devraient coopérer avec la Commission au développement de ces capacités, notamment par le détachement de personnel, le cas échéant, et la contribution à la mise en place d'une capacité commune de surveillance propre à l'Union. Afin de développer l'expertise et les capacités de l'Union, la Commission peut également recourir à l'expertise et aux capacités de l'Observatoire de l'économie des plateformes en ligne, institué par la décision de la Commission du 26 avril 2018 relative à la création du groupe d'experts de l'Observatoire de l'économie des plateformes en ligne, d'organismes spécialisés pertinents et de centres d'excellence. La Commission peut inviter des experts possédant une expertise spécifique, y compris des chercheurs agréés, des représentants d'agences et d'organismes de l'Union, des représentants du secteur, des associations représentant les utilisateurs ou la société civile, des organisations internationales, des experts du secteur privé ainsi que d'autres parties prenantes.

(138)La Commission devrait pouvoir enquêter de sa propre initiative sur les infractions conformément aux pouvoirs prévus dans le présent règlement, y compris en demandant à avoir accès à des données, en exigeant des informations ou en menant des inspections, ainsi qu'en faisant appel au soutien des coordinateurs pour les services numériques. Lorsque la surveillance exercée par les autorités nationales compétentes à l'égard de certaines infractions particulières alléguées, commises par des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne révèle des questions systémiques, telles que des questions ayant un impact important sur les intérêts collectifs des destinataires du service, les coordinateurs pour les services numériques devraient pouvoir, sur la base d'une demande

dûment motivée, saisir la Commission de ces questions. Cette demande devrait comprendre, au minimum, tous les faits et circonstances nécessaires à l'appui de l'infraction alléguée et de son caractère systémique. En fonction du résultat de sa propre évaluation, la Commission devrait pouvoir également prendre les mesures d'enquête et d'exécution nécessaires au titre du présent règlement, y compris, s'il y a lieu, lancer une enquête ou prendre des mesures provisoires.

(139)Pour pouvoir s'acquitter efficacement de ses tâches, la Commission devrait conserver une marge d'appréciation en ce qui concerne la décision d'engager une procédure à l'encontre de fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne. Dès lors que la Commission a engagé la procédure, les coordinateurs pour les services numériques des États membres d'établissement concernés devraient être mis dans l'impossibilité d'exercer leurs pouvoirs d'enquête et d'exécution en ce qui concerne le comportement en cause du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, afin d'éviter les doubles emplois, les incohérences et les risques du point de vue du principe non bis in idem. La Commission devrait toutefois pouvoir demander aux coordinateurs pour les services numériques une contribution individuelle ou commune à l'enquête. Conformément au principe de coopération loyale, il convient que le coordinateur pour les services numériques mette tout en œuvre pour satisfaire les demandes justifiées et proportionnées adressées par la Commission dans le cadre d'une enquête. En outre, le coordinateur pour les services numériques de l'État membre d'établissement, ainsi que le comité et tout autre coordinateur pour les services numériques le cas échéant, devraient fournir à la Commission toutes les informations et l'assistance nécessaires pour lui permettre de s'acquitter efficacement de ses tâches, y compris les informations recueillies dans le cadre d'une collecte de données ou d'exercices d'accès aux données, dans la mesure où cela n'est pas interdit par la base juridique en vertu de laquelle les informations ont été recueillies. Réciproquement, la Commission devrait tenir le coordinateur pour les services numériques de l'État membre d'établissement et le comité informés de l'exercice de ses pouvoirs, en particulier lorsqu'elle a l'intention d'engager la procédure et d'exercer ses pouvoirs d'enquête. Par ailleurs, lorsque la Commission communique ses conclusions préliminaires, y compris toute question sur laquelle elle exprime des griefs, aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne concernés, elle devrait également les communiquer au comité. Le comité devrait faire connaître son point de vue sur les griefs et l'appréciation émis par la Commission, qui devrait prendre en compte cet avis dans la motivation sous-tendant sa décision définitive.

(140)Compte tenu à la fois des difficultés particulières qui peuvent surgir dans le cadre de la vérification du respect des règles par les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et de l'importance de procéder efficacement à cette vérification, eu égard à leur taille, à leur poids et au préjudice qu'ils peuvent causer, la Commission devrait disposer de pouvoirs d'enquête et d'exécution solides pour lui permettre d'enquêter sur le respect des règles établies dans le présent règlement, de les faire appliquer et de contrôler leur respect, dans le plein respect du droit fondamental d'être entendu et d'avoir accès au dossier dans le cadre de procédures d'exécution, du principe de proportionnalité et des droits et intérêts des parties affectées.

(141)La Commission devrait pouvoir demander les informations nécessaires aux fins de veiller à la mise en œuvre et au respect effectifs des obligations fixées dans le présent règlement, dans l'ensemble de l'Union. En particulier, la Commission devrait avoir accès à tous les documents, données et informations pertinents nécessaires pour ouvrir et mener des enquêtes et pour contrôler le respect des obligations pertinentes prévues par le présent règlement, quelle que soit la personne qui détient les documents, données ou informations en question, et quels que soient la forme ou le format de ceux-ci, leur support de stockage ou le lieu précis où ils sont stockés. La Commission devrait pouvoir exiger directement, au moyen d'une demande d'informations dûment motivée, que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause, ainsi que toute autre personne physique ou morale agissant pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale et raisonnablement susceptible d'avoir connaissance d'informations relatives à l'infraction présumée ou à l'infraction, selon le cas, fournisse tout élément de preuve, toute donnée et toute information pertinents. En outre, la Commission devrait pouvoir demander toute information pertinente à toute autorité publique, tout

organisme ou toute agence au sein de l'État membre aux fins du présent règlement. La Commission devrait pouvoir exiger, par l'exercice de pouvoirs d'enquête, tels que des demandes d'informations ou des auditions, l'accès aux documents, aux données, aux informations, aux bases de données et aux algorithmes des personnes concernées ainsi que des explications y afférentes, interroger, avec son consentement, toute personne physique ou morale susceptible d'être en possession d'informations utiles et enregistrer les déclarations correspondantes par tout moyen technique. La Commission devrait également être habilitée à effectuer les inspections nécessaires pour faire respecter les dispositions pertinentes du présent règlement. Ces pouvoirs d'enquête visent à compléter la possibilité pour la Commission de demander l'assistance des coordinateurs pour les services numériques et des autorités d'autres États membres, par exemple par la fourniture d'informations ou dans l'exercice de ces pouvoirs.

(142)Les mesures provisoires peuvent être un outil important pour s'assurer que, pendant qu'une enquête est en cours, l'infraction faisant l'objet de l'enquête n'entraîne pas de risque de préjudices graves pour les destinataires du service. Cet instrument joue un rôle important pour éviter une évolution qu'il serait très difficile d'inverser par une décision prise par la Commission à la fin de la procédure. La Commission devrait par conséquent avoir le pouvoir de décider d'imposer des mesures provisoires dans le cadre d'une procédure engagée en vue de l'adoption éventuelle d'une décision constatant un manquement. Ce pouvoir devrait s'appliquer dans les cas où la Commission a conclu à première vue à l'existence d'une violation d'obligations prévues au présent règlement par le fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne. Une décision imposant des mesures provisoires ne devrait s'appliquer que pour une durée déterminée, soit jusqu'au terme de la procédure engagée par la Commission, soit pour une période déterminée, qui peut être renouvelée dans la mesure où cela est nécessaire et opportun.

(143)La Commission devrait pouvoir prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs des obligations prévues par le présent règlement. Au titre de ces mesures, elle devrait avoir la capacité de nommer des experts externes indépendants et des auditeurs chargés de l'assister dans ce processus, y compris, le cas échéant, issus des autorités compétentes des États membres, par exemple les autorités chargées de la protection des données ou de la protection des consommateurs. Lors de la désignation des auditeurs, la Commission devrait veiller à une rotation suffisante.

(144)Le non-respect des obligations pertinentes imposées en vertu du présent règlement devrait pouvoir être sanctionné au moyen d'amendes et d'astreintes. À cette fin, il convient également de fixer des niveaux appropriés d'amendes et d'astreintes en cas de non-respect des obligations et de violation des règles de procédure, sous réserve de délais de prescription appropriés conformément aux principes de proportionnalité et non bis in idem. La Commission et les autorités nationales compétentes devraient coordonner leurs efforts en matière d'exécution afin de veiller au respect desdits principes. En particulier, la Commission devrait tenir compte de toutes les amendes et astreintes imposées à la même personne morale pour les mêmes faits par une décision finale dans le cadre d'une procédure relative à une infraction à d'autres règles nationales ou de l'Union, de manière à veiller à ce que l'ensemble des amendes et astreintes imposées soient proportionnées et correspondent à la gravité des infractions commises. Toutes les décisions prises par la Commission au titre du présent règlement sont soumises au contrôle de la Cour de justice de l'Union européenne conformément au traité sur le fonctionnement de l'Union européenne. La Cour de justice de l'Union européenne devrait disposer d'une compétence de pleine juridiction en ce qui concerne les amendes et les astreintes conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne.

(145)Eu égard aux effets potentiellement importants pour la société que peut avoir une violation des obligations supplémentaires de gestion des risques systémiques qui s'appliquent exclusivement aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne, et afin de répondre à ces préoccupations de politique publique, il est nécessaire de prévoir un système de surveillance renforcée de toute mesure prise pour mettre fin efficacement aux violations du présent règlement et pour y remédier. Par conséquent, dès qu'une infraction à l'une des dispositions du présent règlement qui s'appliquent exclusivement aux très grandes plateformes en ligne ou aux très grands moteurs de recherche en ligne a été constatée et, s'il y a lieu, sanctionnée, la Commission devrait demander au fournisseur de la plateforme ou du moteur de

recherche en cause d'établir un plan d'action détaillé pour remédier à tout effet futur de l'infraction et de communiquer ce plan d'action, dans un délai fixé par la Commission, aux coordinateurs pour les services numériques, à la Commission et au comité. La Commission, tenant compte de l'avis du comité, devrait déterminer si les mesures prévues dans le plan d'action sont suffisantes pour remédier à l'infraction, en prenant également en considération le fait que l'adhésion au code de conduite pertinent figure ou non parmi les mesures proposées. La Commission devrait en outre vérifier toute mesure ultérieure prise par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause conformément à son plan d'action, en tenant compte aussi d'un audit indépendant du fournisseur. Si, à la suite de la mise en œuvre du plan d'action, la Commission considère toujours qu'il n'a pas été pleinement remédié à l'infraction, ou si le plan d'action n'a pas été fourni ou n'est pas considéré comme adéquat, elle devrait pouvoir utiliser tout pouvoir d'enquête ou d'exécution prévu par le présent règlement, y compris le pouvoir d'imposer des astreintes et l'ouverture d'une procédure visant à rendre impossible l'accès au service fourni en violation du présent règlement.

(146)Il convient que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en cause ainsi que les autres personnes soumises à l'exercice des pouvoirs de la Commission dont les intérêts peuvent être affectés par une décision, aient la possibilité de présenter leurs observations au préalable, et une large publicité des décisions prises devrait être assurée. Tout en garantissant les droits de la défense des parties concernées, et notamment le droit d'accès au dossier, il est indispensable de préserver la confidentialité des informations. En outre, tout en respectant la confidentialité des informations, la Commission devrait veiller à ce que toute information invoquée aux fins de sa décision soit divulguée dans une mesure permettant au destinataire de la décision de comprendre les faits et considérations qui ont conduit à celle-ci.

(147)Afin de garantir que le présent règlement est appliqué et exécuté de façon harmonisée, il importe de veiller à ce que les autorités nationales, y compris les juridictions nationales, disposent de toutes les informations nécessaires pour garantir que leurs décisions ne soient pas contraires à une décision adoptée par la Commission en vertu du présent règlement. Cette disposition est sans préjudice de l'article 267 du traité sur le fonctionnement de l'Union européenne.

(148)L'exécution et le contrôle effectifs du présent règlement nécessitent un échange d'informations fluide et en temps réel entre les coordinateurs pour les services numériques, le comité et la Commission, sur la base des flux d'informations et des procédures prévus dans le présent règlement. Cela peut également justifier, s'il y a lieu, l'accès à ce système par d'autres autorités compétentes. Dans le même temps, compte tenu du fait que les informations échangées peuvent être confidentielles ou comporter des données à caractère personnel, elles devraient rester protégées contre tout accès non autorisé, conformément aux finalités pour lesquelles elles ont été recueillies. Pour cette raison, toutes les communications entre ces autorités devraient avoir lieu sur la base d'un système de partage d'informations fiable et sécurisé, dont les détails devraient être fixés dans un acte d'exécution. Le système de partage d'informations peut être fondé sur des outils existants du marché intérieur, dans la mesure où ceux-ci permettent d'atteindre les objectifs du présent règlement de manière économiquement avantageuse.

(149)Sans préjudice du droit des destinataires de services de s'adresser à un représentant conformément à la directive (UE) 2020/1828 du Parlement européen et du Conseil[33] ou à tout autre type de représentation au titre du droit national, les destinataires des services devraient également avoir le droit de mandater une personne morale ou un organisme public pour exercer les droits qui leur sont conférés par le présent règlement. Ces droits peuvent inclure les droits liés à la soumission de notifications, à la contestation des décisions prises par les fournisseurs de services intermédiaires et à l'introduction de plaintes contre les fournisseurs pour violation du présent règlement. Certains organismes, organisations et associations disposent d'une expertise et de compétences particulières pour la détection et le signalement des décisions relatives à

33. Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

la modération des contenus erronées ou injustifiés et les réclamations qu'ils adressent au nom des destinataires du service peuvent avoir un impact positif sur la liberté d'expression et d'information en général; par conséquent, les fournisseurs de plateformes en ligne devraient traiter ces réclamations sans retard injustifié.

(150)Dans un souci d'efficacité et d'efficience, la Commission devrait procéder à une évaluation générale du présent règlement. En particulier, cette évaluation générale devrait, entre autres, porter sur l'étendue des services couverts par le présent règlement, les interactions avec d'autres actes juridiques, l'impact du présent règlement sur le fonctionnement du marché intérieur, notamment en ce qui concerne les services numériques, la mise en œuvre des codes de conduite, l'obligation de désigner un représentant légal établi dans l'Union, l'effet des obligations sur les petites entreprises et les microentreprises, l'efficacité du mécanisme de surveillance de d'exécution et l'impact sur le droit à la liberté d'expression et d'information. En outre, afin d'éviter des charges disproportionnées et de garantir le maintien de l'efficacité du présent règlement, la Commission devrait procéder à une évaluation de l'impact des obligations énoncées dans le présent règlement sur les petites et moyennes entreprises dans les trois ans à compter du début de son application ainsi qu'à une évaluation de l'étendue des services couverts par le présent règlement, notamment pour les très grandes plateformes en ligne et les très grands moteurs de recherche, et les interactions avec d'autres actes juridiques dans les trois ans à compter de son entrée en vigueur.

(151)Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports sur la modération des contenus, établir le montant de la redevance de surveillance annuelle imposée aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, fixer les modalités pratiques des procédures, des auditions et de la divulgation négociée d'informations effectuées dans le cadre de la surveillance, des enquêtes, de l'exécution et du contrôle à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, ainsi que pour fixer les modalités pratiques et opérationnelles du fonctionnement du système de partage d'informations et de son interopérabilité avec d'autres systèmes pertinents. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil[34].

(152)Afin de réaliser les objectifs du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne pour compléter ledit règlement en ce qui concerne les critères d'identification des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne, les étapes procédurales, les méthodologies et les modèles de rapport pour les audits, les spécifications techniques des demandes d'accès ainsi que la méthodologie et les procédures détaillées pour fixer la redevance de surveillance. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"[35]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(153)Le présent règlement respecte les droits fondamentaux reconnus par la Charte et les droits fondamentaux qui constituent des principes généraux du droit de l'Union. Par conséquent, il convient d'interpréter le présent règlement et de l'appliquer conformément à ces droits fondamentaux, y compris la liberté d'expression et d'information et la liberté et le pluralisme des médias. Dans l'exercice des pouvoirs énoncés dans le présent règlement, toute autorité publique concernée devrait parvenir, dans les situations où les droits fondamentaux pertinents entrent en conflit, à un juste équilibre entre les droits concernés, conformément au principe de proportionnalité.

34. Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).
35. JO L 123 du 12.5.2016, p. 1.

(154)Compte tenu de la portée et de l'incidence des risques pour la société pouvant être causés par les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne, de la nécessité de répondre à ces risques de manière prioritaire et de la capacité à prendre les mesures nécessaires, il est justifié de limiter la période après laquelle le présent règlement commence à s'appliquer aux fournisseurs de ces services.

(155)Étant donné que les objectifs du présent règlement, à savoir contribuer au bon fonctionnement du marché intérieur et garantir un environnement en ligne sûr, prévisible et fiable dans lequel les droits fondamentaux consacrés par la Charte sont dûment protégés, ne peuvent pas être atteints de manière suffisante par les États membres en raison de l'impossibilité d'assurer l'harmonisation et la coopération nécessaires en agissant de manière isolée, mais peuvent, en raison du champ d'application territorial et personnel, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(156)Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[36] et a rendu son avis le 10 février 2021[37],

cf. CEPD/EDPS

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet

1. Le présent règlement a pour objectif de contribuer au bon fonctionnement du marché intérieur des services intermédiaires en établissant des règles harmonisées pour un environnement en ligne sûr, prévisible et fiable qui facilite l'innovation et dans lequel les droits fondamentaux consacrés par la Charte, y compris le principe de protection des consommateurs, sont efficacement protégés.

2. Le présent règlement établit des règles harmonisées applicables à la fourniture de services intermédiaires au sein du marché intérieur. En particulier, il établit:
a) un cadre pour l'exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires;
b) des règles relatives à des obligations de diligence spécifiques, adaptées à certaines catégories spécifiques de fournisseurs de services intermédiaires;
c) des règles relatives à la mise en œuvre et à l'exécution du présent règlement, y compris en ce qui concerne la coopération et la coordination entre les autorités compétentes.

Article 2
Champ d'application

1. Le présent règlement s'applique aux services intermédiaires proposés aux destinataires du service dont le lieu d'établissement est situé dans l'Union ou qui sont situés dans l'Union, quel que soit le lieu d'établissement des fournisseurs de ces services intermédiaires.

2. Le présent règlement ne s'applique pas aux services qui ne sont pas des services intermédiaires ou aux exigences imposées à l'égard de tels services, que ces services soient ou non fournis par le biais d'un service intermédiaire.

36. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).
37. JO C 149 du 27.4.2021, p. 3.

3. Le présent règlement n'a pas d'incidence sur l'application de la directive 2000/31/CE.

4. Le présent règlement s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union régissant d'autres aspects de la fourniture de services intermédiaires dans le marché intérieur ou précisant et complétant le présent règlement, en particulier les actes suivants:
a) la directive 2010/13/UE;
b) le droit de l'Union sur le droit d'auteur et les droits voisins;
c) le règlement (UE) 2021/784;
d) le règlement (UE) 2019/1148;
e) le règlement (UE) 2019/1150;
f) le droit de l'Union en matière de protection des consommateurs et de sécurité des produits, notamment les règlements (UE) 2017/2394 et (UE) 2019/1020 et les directives 2001/95/CE et 2013/11/UE;
g) le droit de l'Union en matière de protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 et la directive 2002/58/CE;
h) le droit de l'Union dans le domaine de la coopération judiciaire en matière civile, en particulier le règlement (UE) n° 1215/2012 ou tout acte juridique de l'Union fixant les règles relatives à la loi applicable aux obligations contractuelles et non contractuelles;
i) le droit de l'Union dans le domaine de la coopération judiciaire en matière pénale, en particulier un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale;
j) une directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale.

cf. RGPD

Article 3
Définitions

Aux fins du présent règlement, on entend par:

a) "service de la société de l'information": un service tel qu'il est défini à l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535;

b) "destinataire du service": toute personne physique ou morale utilisant un service intermédiaire, notamment pour rechercher une information ou la rendre accessible;

c) "consommateur": toute personne physique agissant à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

d) "proposer des services dans l'Union": permettre aux personnes physiques ou morales dans un ou plusieurs États membres d'utiliser les services d'un fournisseur de services intermédiaires qui a un lien étroit avec l'Union;

e) "lien étroit avec l'Union": un lien qu'un fournisseur de services intermédiaires a avec l'Union résultant soit de son établissement dans l'Union, soit de critères factuels spécifiques, tels que:

— un nombre significatif de destinataires du service dans un ou plusieurs États membres par rapport à sa ou à leur population; ou

— le ciblage des activités sur un ou plusieurs États membres;

f) "professionnel": toute personne physique, ou toute personne morale qu'elle soit privée ou publique, qui agit, y compris par l'intermédiaire d'une personne agissant en son nom ou pour son compte, à des fins entrant dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

g) "service intermédiaire": un des services de la société de l'information suivants:

i) un service de "simple transport", consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service ou à fournir l'accès à un réseau de communication;

ii) un service de “mise en cache”, consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, impliquant le stockage automatique, intermédiaire et temporaire de ces informations, effectué dans le seul but de rendre plus efficace la transmission ultérieure de ces informations à d’autres destinataires à leur demande;

iii) un service d’”hébergement”, consistant à stocker des informations fournies par un destinataire du service à sa demande;

h) “contenu illicite”: toute information qui, en soi ou par rapport à une activité, y compris la vente de produits ou la fourniture de services, n’est pas conforme au droit de l’Union ou au droit d’un État membre qui est conforme au droit de l’Union, quel que soit l’objet précis ou la nature précise de ce droit;

i) “plateforme en ligne”: un service d’hébergement qui, à la demande d’un destinataire du service, stocke et diffuse au public des informations, à moins que cette activité ne soit une caractéristique mineure et purement accessoire d’un autre service ou une fonctionnalité mineure du service principal qui, pour des raisons objectives et techniques, ne peut être utilisée sans cet autre service, et pour autant que l’intégration de cette caractéristique ou de cette fonctionnalité à l’autre service ne soit pas un moyen de contourner l’applicabilité du présent règlement;

j) “moteur de recherche en ligne”: un service intermédiaire qui permet aux utilisateurs de formuler des requêtes afin d’effectuer des recherches sur, en principe, tous les sites internet ou tous les sites internet dans une langue donnée, sur la base d’une requête lancée sur n’importe quel sujet sous la forme d’un mot-clé, d’une demande vocale, d’une expression ou d’une autre entrée, et qui renvoie des résultats dans quelque format que ce soit dans lesquels il est possible de trouver des informations en rapport avec le contenu demandé;

k) “diffusion au public”: le fait de mettre des informations à la disposition d’un nombre potentiellement illimité de tiers, à la demande du destinataire du service ayant fourni ces informations;

l) “contrat à distance”: le “contrat à distance” tel qu’il est défini à l’article 2, point 7), de la directive 2011/83/UE;

m) “interface en ligne”: tout logiciel, y compris un site internet ou une section de site internet, et des applications, notamment des applications mobiles;

n) “coordinateur pour les services numériques de l’État membre d’établissement”: le coordinateur pour les services numériques de l’État membre dans lequel l’établissement principal d’un fournisseur d’un service intermédiaire est situé, ou dans lequel son représentant légal réside ou est établi;

o) “coordinateur pour les services numériques de l’État membre de destination”: le coordinateur pour les services numériques d’un État membre dans lequel le service intermédiaire est fourni;

p) “destinataire actif d’une plateforme en ligne”: un destinataire du service qui a été en contact avec une plateforme en ligne, soit en demandant à la plateforme en ligne d’héberger des informations, soit en étant exposé aux informations hébergées par la plateforme en ligne et diffusées via son interface en ligne;

q) “destinataire actif d’un moteur de recherche en ligne”: un destinataire du service qui a soumis une requête à un moteur de recherche en ligne et a été exposé aux informations indexées et présentées sur son interface en ligne;

r) “publicité”: les informations destinées à promouvoir le message d’une personne physique ou morale, qu’elles aient des visées commerciales ou non commerciales, et présentées par une plateforme en ligne sur son interface en ligne, moyennant rémunération, dans le but spécifique de promouvoir ces informations;

s) “système de recommandation”: un système entièrement ou partiellement automatisé utilisé par une plateforme en ligne pour suggérer sur son interface en ligne des informations spécifiques aux destinataires du service ou pour hiérarchiser ces informa-

tions, notamment à la suite d'une recherche lancée par le destinataire du service ou en déterminant de toute autre manière l'ordre relatif ou d'importance des informations affichées;

t) "modération des contenus": les activités, qu'elles soient automatisées ou non, entreprises par des fournisseurs de services intermédiaires qui sont destinées, en particulier, à détecter et à identifier les contenus illicites ou les informations incompatibles avec leurs conditions générales, fournis par les destinataires du service, et à lutter contre ces contenus ou ces informations, y compris les mesures prises qui ont une incidence sur la disponibilité, la visibilité et l'accessibilité de ces contenus ou ces informations, telles que leur rétrogradation, leur démonétisation, le fait de rendre l'accès à ceux-ci impossible ou leur retrait, ou qui ont une incidence sur la capacité des destinataires du service à fournir ces informations, telles que la suppression ou la suspension du compte d'un destinataire;

u) "conditions générales": toutes les clauses, quelle que soit leur dénomination ou leur forme, qui régissent la relation contractuelle entre le fournisseur de services intermédiaires et les destinataires du service;

v) "personnes handicapées": les "personnes handicapées" visées à l'article 3, point 1), de la directive (UE) 2019/882 du Parlement européen et du Conseil[38];

w) "communication commerciale": la "communication commerciale" telle qu'elle est définie à l'article 2, point f), de la directive 2000/31/CE;

x) "chiffre d'affaires": le montant atteint par une entreprise au sens de l'article 5, paragraphe 1, du règlement (CE) n° 139/2004 du Conseil[39].

CHAPITRE II
RESPONSABILITE DES FOURNISSEURS DE SERVICES INTERMÉDIAIRES

Article 4
"Simple transport"

1. En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service ou à fournir un accès à un réseau de communication, le fournisseur de services n'est pas responsable des informations transmises ou auxquelles l'accès est fourni, à condition que le fournisseur:
a) ne soit pas à l'origine de la transmission;
b) ne sélectionne pas le destinataire de la transmission; et
c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

3. Le présent article n'affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d'un État membre, d'exiger du fournisseur de services qu'il mette fin à une infraction ou qu'il prévienne une infraction.

Article 5
"Mise en cache"

1. En cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire

38. Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).
39. Règlement (CE) n° 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises (JO L 24 du 29.1.2004, p. 1).

du service, le fournisseur de services n'est pas responsable du stockage automatique, intermédiaire et temporaire de ces informations réalisé dans le seul but de rendre plus efficace ou plus sûre la transmission ultérieure des informations à d'autres destinataires du service à leur demande, à condition que le fournisseur:
a) ne modifie pas les informations;
b) respecte les conditions d'accès aux informations;
c) respecte les règles concernant la mise à jour des informations, indiquées d'une manière largement reconnue et utilisées par le secteur;
d) n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par le secteur, dans le but d'obtenir des données sur l'utilisation des informations; et
e) agisse promptement pour retirer les informations qu'il a stockées ou pour rendre l'accès à ces informations impossible dès qu'il a effectivement connaissance du fait que les informations à l'origine de la transmission ont été retirées du réseau ou que l'accès aux informations a été rendu impossible, ou du fait qu'une autorité judiciaire ou administrative a ordonné de retirer les informations ou de rendre l'accès à ces informations impossible.

2. Le présent article n'affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d'un État membre, d'exiger du fournisseur de services qu'il mette fin à une infraction ou qu'il prévienne une infraction.

Article 6
Hébergement

1. En cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le fournisseur de services n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que le fournisseur:
a) n'ait pas effectivement connaissance de l'activité illégale ou du contenu illicite et, en ce qui concerne une demande en dommages et intérêts, n'ait pas conscience de faits ou de circonstances selon lesquels l'activité illégale ou le contenu illicite est apparent; ou
b) dès le moment où il en prend connaissance ou conscience, agisse promptement pour retirer le contenu illicite ou rendre l'accès à celui-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur.

3. Le paragraphe 1 ne s'applique pas en ce qui concerne la responsabilité au titre de la législation relative à la protection des consommateurs applicable aux plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, lorsqu'une telle plateforme en ligne présente l'information spécifique ou permet de toute autre manière la transaction spécifique en question de telle sorte qu'un consommateur moyen peut être amené à croire que les informations, le produit ou service faisant l'objet de la transaction sont fournis soit directement par la plateforme en ligne, soit par un destinataire du service agissant sous son autorité ou son contrôle.

4. Le présent article n'affecte pas la possibilité, pour une autorité judiciaire ou administrative, conformément au système juridique d'un État membre, d'exiger du fournisseur de services qu'il mette fin à une infraction ou qu'il prévienne une infraction.

Article 7
Enquêtes d'initiative volontaires et respect de la législation

Les fournisseurs de services intermédiaires ne sont pas réputés être exclus du bénéfice des exemptions de responsabilité prévues aux articles 4, 5 et 6 du simple fait qu'ils procèdent de leur propre initiative, de bonne foi et avec diligence, à des enquêtes volontaires ou prennent d'autres mesures destinées à détecter, à identifier et à retirer des contenus illicites, ou à rendre l'accès à ces contenus impossible, ou qu'ils prennent les mesures nécessaires pour se conformer aux exigences du droit de l'Union et du droit national conforme au droit de l'Union, y compris les exigences énoncées dans le présent règlement.

Article 8
Absence d'obligation générale de surveillance ou de recherche active des faits

Les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales.

Article 9
Injonctions d'agir contre des contenus illicites

1. Dès réception d'une injonction d'agir contre un ou plusieurs éléments spécifiques de contenu illicite, émise par les autorités judiciaires ou administratives nationales compétentes sur la base du droit de l'Union ou du droit national conforme au droit de l'Union applicable, le fournisseur de services intermédiaires informe dans les meilleurs délais l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, de la suite éventuelle donnée à l'injonction, en précisant si et quand une suite a été donnée à l'injonction.

2. Lorsqu'une injonction visée au paragraphe 1 est transmise au fournisseur, les États membres veillent à ce qu'elle remplisse au minimum les conditions suivantes:

a) ladite injonction comprend les éléments suivants:

i) une référence à la base juridique au titre du droit de l'Union ou du droit national pour l'injonction;

ii) un exposé des motifs expliquant pourquoi les informations constituent un contenu illicite, en référence à une ou plusieurs dispositions spécifiques du droit de l'Union ou du droit national conforme au droit de l'Union;

iii) des informations permettant d'identifier l'autorité d'émission;

iv) des informations claires permettant au fournisseur de services intermédiaires d'identifier et de localiser le contenu illicite concerné, telles qu'un ou plusieurs URL exacts et, si nécessaire, des informations supplémentaires;

v) des informations relatives aux mécanismes de recours dont disposent le fournisseur de services intermédiaires et le destinataire du service ayant fourni le contenu;

vi) le cas échéant, des informations sur l'autorité qui doit recevoir les informations relatives aux suites données aux injonctions;

b) le champ d'application territorial de ladite injonction, sur la base des règles applicables du droit de l'Union et du droit national, y compris de la Charte, et, le cas échéant, des principes généraux du droit international, est limité à ce qui est strictement nécessaire pour atteindre son objectif;

c) ladite injonction est transmise dans l'une des langues déclarées par le fournisseur de services intermédiaires en vertu de l'article 11, paragraphe 3, ou dans une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et ce fournisseur, et elle est envoyée au point de contact électronique désigné par ce fournisseur, conformément à l'article 11; lorsque l'injonction n'est pas rédigée dans la langue déclarée par le fournisseur de services intermédiaires ou dans une autre langue convenue de manière bilatérale, l'injonction peut être transmise dans la langue de l'autorité qui l'a émise, à condition qu'elle soit accompagnée d'une traduction, dans la langue déclarée ou convenue de manière bilatérale, au minimum des éléments mentionnés aux points a) et b) du présent paragraphe.

3. L'autorité qui a émis l'injonction ou, le cas échéant, l'autorité spécifiée dans l'injonction, transmet l'injonction ainsi que toute information reçue du fournisseur de services intermédiaires concernant la suite donnée à cette injonction au coordinateur pour les services numériques de l'État membre de l'autorité d'émission.

4. Après avoir reçu l'injonction de l'autorité judiciaire ou administrative, le coordinateur pour les services numériques de l'État membre concerné transmet, dans les meilleurs délais, une copie de l'injonction visée au paragraphe 1 du présent article à tous les autres coordinateurs pour les services numériques par l'intermédiaire du système établi conformément à l'article 85.

5. Au plus tard lorsqu'une suite est donnée à l'injonction ou, le cas échéant, au moment indiqué par l'autorité d'émission dans son injonction, les fournisseurs de services intermédiaires informent le destinataire du service concerné de l'injonction reçue et de la suite qui lui est donnée. Les informations communiquées au destinataire du service comprennent un exposé des motifs, les possibilités de recours qui existent et une description du champ d'application territorial de l'injonction, conformément au paragraphe 2.

6. Les conditions et exigences établies dans le présent article sont sans préjudice du droit national applicable en matière de procédure civile et de procédure pénale.

Article 10
Injonctions de fournir des informations

1. Dès réception de l'injonction de fournir des informations spécifiques concernant un ou plusieurs destinataires spécifiques du service, émise par les autorités judiciaires ou administratives nationales compétentes sur la base du droit de l'Union ou du droit national conforme au droit de l'Union applicable, le fournisseur de services intermédiaires informe, dans les meilleurs délais, l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, de la réception de l'injonction et de la suite qui y est donnée, en précisant si et quand une suite a été donnée à l'injonction.

2. Lorsqu'une injonction visée au paragraphe 1 est transmise au fournisseur, les États membres veillent à ce qu'elle remplisse au minimum les conditions suivantes:

a) ladite injonction comprend les éléments suivants:

i) une référence à la base juridique au titre du droit de l'Union ou du droit national pour l'injonction;

ii) des informations permettant d'identifier l'autorité d'émission;

iii) des informations claires permettant au fournisseur de services intermédiaires d'identifier le ou les destinataires spécifiques au sujet desquels des informations sont demandées, telles qu'un ou plusieurs noms de compte ou identifiants uniques;

iv) un exposé des motifs expliquant dans quel but les informations sont requises et pourquoi la demande de fourniture d'informations est nécessaire et proportionnée pour déterminer si les destinataires des services intermédiaires respectent le droit de l'Union ou le droit national conforme au droit de l'Union applicable, à moins qu'un tel exposé ne puisse être fourni pour des raisons liées à la prévention et à la détection des infractions pénales et aux enquêtes et poursuites en la matière;

v) des informations relatives aux mécanismes de recours dont disposent le fournisseur et les destinataires du service concerné;

vi) le cas échéant, des informations relatives à l'autorité qui doit recevoir les informations relatives aux suites données aux injonctions;

b) ladite injonction exige uniquement du fournisseur qu'il communique des informations déjà collectées aux fins de fournir le service et dont il a le contrôle;

c) ladite injonction est transmise dans l'une des langues déclarées par le fournisseur de services intermédiaires en vertu de l'article 11, paragraphe 3, ou dans une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et le fournisseur, et elle est envoyée au point de contact électronique désigné par ce fournisseur, conformément à l'article 11; lorsque l'injonction n'est pas rédigée dans la langue déclarée par le fournisseur de services intermédiaires ou dans une autre langue convenue de manière bilatérale, l'injonction peut être transmise dans la langue de l'autorité qui l'a émise, à condition qu'elle soit accompagnée d'une traduction, dans

cette langue déclarée ou convenue de manière bilatérale, au minimum des éléments mentionnés aux points a) et b) du présent paragraphe.

3. L'autorité qui a émis l'injonction ou, le cas échéant, l'autorité spécifiée dans l'injonction, transmet l'injonction ainsi que toute information reçue du fournisseur de services intermédiaires concernant la suite donnée à cette injonction au coordinateur pour les services numériques de l'État membre de l'autorité d'émission.

4. Après avoir reçu l'injonction de l'autorité judiciaire ou administrative, le coordinateur pour les services numériques de l'État membre concerné transmet, dans les meilleurs délais, une copie de l'injonction visée au paragraphe 1 du présent article à tous les coordinateurs pour les services numériques par l'intermédiaire du système établi conformément à l'article 85.

5. Au plus tard lorsqu'une suite est donnée à l'injonction ou, le cas échéant, au moment indiqué par l'autorité d'émission dans son injonction, les fournisseurs de services intermédiaires informent le destinataire du service concerné de l'injonction reçue et de la suite qui lui est donnée. Les informations communiquées au destinataire du service comprennent un exposé des motifs et les possibilités de recours qui existent, conformément au paragraphe 2.

6. Les conditions et exigences énoncées dans le présent article sont sans préjudice du droit national applicable en matière de procédure civile et de procédure pénale.

CHAPITRE III
OBLIGATIONS DE DILIGENCE POUR UN ENVIRONNEMENT EN LIGNE SÛR ET TRANSPARENT

SECTION 1
Dispositions applicables à tous les fournisseurs de services intermédiaires

Article 11
Points de contact pour les autorités des États membres, la Commission et le comité

1. Les fournisseurs de services intermédiaires désignent un point de contact unique pour leur permettre de communiquer directement, par voie électronique, avec les autorités des États membres, la Commission et le comité visé à l'article 61 en vue de l'application du présent règlement.

2. Les fournisseurs de services intermédiaires rendent publiques les informations nécessaires pour faciliter l'identification de leurs points de contact uniques et la communication avec ces derniers. Ces informations sont aisément accessibles et sont tenues à jour.

3. Les fournisseurs de services intermédiaires précisent, dans les informations visées au paragraphe 2, la ou les langues officielles des États membres qui, en plus d'une langue largement comprise par le plus grand nombre possible de citoyens de l'Union, peuvent être utilisées pour communiquer avec leurs points de contact, et qui comprennent au minimum une des langues officielles de l'État membre dans lequel le fournisseur de services intermédiaires a son établissement principal ou dans lequel son représentant légal réside ou est établi.

Article 12
Points de contact pour les destinataires du service

1. Les fournisseurs de services intermédiaires désignent un point de contact unique pour permettre aux destinataires du service de communiquer directement et rapidement avec eux, par voie électronique et de manière conviviale, y compris en permettant aux destinataires du service de choisir les moyens de communication, lesquels ne s'appuient pas uniquement sur des outils automatisés.

2. Outre les obligations prévues dans la directive 2000/31/CE, les fournisseurs de services intermédiaires rendent publiques les informations nécessaires pour que les destinataires du service puissent facilement identifier leurs points de contact uniques et communiquer avec eux. Ces informations sont aisément accessibles et sont tenues à jour.

Article 13
Représentants légaux

1. Les fournisseurs de services intermédiaires qui n'ont pas d'établissement au sein de l'Union, mais qui proposent des services dans l'Union désignent, par écrit, une personne morale ou physique pour agir comme leur représentant légal dans un des États membres dans lequel le fournisseur propose ses services.

2. Les représentants légaux sont chargés par les fournisseurs de services intermédiaires de répondre, en sus ou à la place de ces fournisseurs, à toutes les questions des autorités compétentes des États membres, de la Commission et du comité nécessaires en vue de la réception, du respect et de l'exécution des décisions prises en lien avec le présent règlement. Les fournisseurs de services intermédiaires donnent à leur représentant légal les pouvoirs nécessaires et les ressources suffisantes pour garantir une coopération efficace et en temps utile avec les autorités compétentes des États membres, la Commission et le comité, et pour se conformer à ces décisions.

3. Le représentant légal désigné peut être tenu pour responsable du non-respect des obligations prévues dans le présent règlement, sans préjudice de la responsabilité du fournisseur de services intermédiaires et des actions en justice qui pourraient être intentées contre lui.

4. Les fournisseurs de services intermédiaires communiquent le nom, l'adresse postale, l'adresse de courrier électronique et le numéro de téléphone de leur représentant légal au coordinateur pour les services numériques de l'État membre dans lequel le représentant légal réside ou est établi. Ils veillent à ce que ces informations soient mises à la disposition du public, facilement accessibles, exactes et tenues à jour.

5. La désignation d'un représentant légal au sein de l'Union en vertu du paragraphe 1 ne constitue pas un établissement dans l'Union.

Article 14
Conditions générales

1. Les fournisseurs de services intermédiaires incluent dans leurs conditions générales des renseignements relatifs aux éventuelles restrictions qu'ils imposent en ce qui concerne l'utilisation de leur service vis-à-vis des informations fournies par les destinataires du service. Ces renseignements comprennent des informations sur les politiques, procédures, mesures et outils utilisés à des fins de modération des contenus, y compris la prise de décision fondée sur des algorithmes et le réexamen par un être humain, ainsi que sur le règlement intérieur de leur système interne de traitement des réclamations. Ils sont énoncés dans un langage clair, simple, intelligible, aisément abordable et dépourvu d'ambiguïté, et sont mis à la disposition du public dans un format facilement accessible et lisible par une machine.

2. Les fournisseurs de services intermédiaires informent les destinataires du service de toute modification importante des conditions générales.

3. Lorsqu'un service intermédiaire s'adresse principalement à des mineurs ou est utilisé de manière prédominante par des mineurs, le fournisseur de ce service intermédiaire explique les conditions et les éventuelles restrictions relatives à l'utilisation du service d'une manière compréhensible pour les mineurs.

4. Lorsqu'ils appliquent et font respecter les restrictions visées au paragraphe 1, les fournisseurs de services intermédiaires agissent de manière diligente, objective et proportionnée en tenant dûment compte des droits et des intérêts légitimes de toutes les parties impliquées, et notamment des droits fondamentaux des destinataires du service, tels que la liberté d'expression, la liberté et le pluralisme des médias et d'autres libertés et droits fondamentaux tels qu'ils sont consacrés dans la Charte.

5. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne fournissent aux destinataires des services un résumé des conditions générales, y compris des mécanismes de recours et de réparation disponibles, concis, facilement accessible et lisible par une machine, dans un langage clair et dépourvu d'ambiguïté.

6. Les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne au sens de l'article 33 publient leurs conditions générales dans les langues officielles de tous les États membres dans lesquels ils proposent leurs services.

Article 15
Obligations en matière de rapports de transparence incombant aux fournisseurs de services intermédiaires

1. Les fournisseurs de services intermédiaires mettent à la disposition du public, dans un format lisible par une machine et d'une manière facilement accessible, au moins une fois par an, des rapports clairs et facilement compréhensibles sur les éventuelles activités de modération des contenus auxquelles ils se sont livrés au cours de la période concernée. Ces rapports comprennent, en particulier, des informations sur les points suivants, selon le cas:

a) pour les fournisseurs de services intermédiaires, le nombre d'injonctions reçues des autorités des États membres, y compris les injonctions émises conformément aux articles 9 et 10, classées par type de contenu illicite concerné, l'État membre qui a émis l'injonction et le délai médian nécessaire pour informer de sa réception l'autorité qui a émis l'injonction, ou toute autre autorité spécifiée dans l'injonction, et pour donner suite à l'injonction;

b) pour les fournisseurs de services d'hébergement, le nombre de notifications soumises conformément à l'article 16, classées par type de contenu présumé illicite concerné, le nombre de notifications soumises par les signaleurs de confiance, toute action entreprise au titre des notifications en précisant si l'action a été entreprise sur la base de la législation ou des conditions générales du fournisseur, le nombre de notifications traitées de manière automatisée et le délai médian nécessaire pour entreprendre l'action;

c) pour les fournisseurs de services intermédiaires, des informations utiles et compréhensibles sur les activités de modération des contenus auxquelles se sont livrés les fournisseurs de leur propre initiative, y compris l'utilisation d'outils automatisés, les mesures prises pour dispenser une formation et une assistance aux personnes chargées de la modération des contenus, le nombre et le type de mesures prises qui affectent la disponibilité, la visibilité et l'accessibilité des informations fournies par les destinataires du service et sur la capacité des destinataires à fournir des informations par l'intermédiaire du service, ainsi que d'autres restrictions connexes du service; les informations communiquées sont classées par type de contenu illicite ou d'infraction aux conditions générales du fournisseur de services, par méthode de détection et par type de restrictions appliquées;

d) pour les fournisseurs de services intermédiaires, le nombre de réclamations reçues par l'intermédiaire des systèmes internes de traitement des réclamations conformément aux conditions générales du fournisseur et, en outre, pour les fournisseurs de plateformes en ligne, conformément à l'article 20, le fondement de ces réclamations, les décisions prises concernant ces réclamations, le délai médian nécessaire pour prendre ces décisions et le nombre de cas dans lesquels ces décisions ont été infirmées;

e) tout recours à des moyens automatisés à des fins de modération des contenus, y compris une description qualitative, une indication des objectifs précis, des indicateurs de la précision et du taux d'erreur possible des moyens automatisés utilisés pour atteindre ces objectifs, et les éventuelles mesures de sauvegarde appliquées.

2. Le paragraphe 1 du présent article ne s'applique pas aux fournisseurs de services intermédiaires qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE et qui ne sont pas de très grandes plateformes en ligne au sens de l'article 33 du présent règlement.

3. La Commission peut adopter des actes d'exécution pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports au titre du paragraphe 1 du présent article, y compris des périodes harmonisées pour l'établissement des rapports. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

SECTION 2
Dispositions supplémentaires applicables aux fournisseurs de services d'hébergement, y compris les plateformes en ligne

Article 16
Mécanismes de notification et d'action

1. Les fournisseurs de services d'hébergement mettent en place des mécanismes permettant à tout particulier ou à toute entité de leur signaler la présence au sein de leur service d'éléments d'information spécifiques que le particulier ou l'entité considère comme du contenu illicite. Ces mécanismes sont faciles d'accès et d'utilisation et permettent la soumission de notifications exclusivement par voie électronique.

2. Les mécanismes prévus au paragraphe 1 sont de nature à faciliter la soumission de notifications suffisamment précises et dûment étayées. À cette fin, les fournisseurs de services d'hébergement prennent les mesures nécessaires pour permettre et faciliter la soumission de notifications contenant l'ensemble des éléments suivants:
a) une explication suffisamment étayée des raisons pour lesquelles le particulier ou l'entité allègue que les informations en question sont du contenu illicite;
b) une indication claire de l'emplacement électronique exact de ces informations, comme l'URL ou les URL exact(s), et, le cas échéant, des informations complémentaires permettant d'identifier le contenu illicite en fonction du type de contenu et du type spécifique de service d'hébergement;
c) le nom et l'adresse de courrier électronique du particulier ou de l'entité soumettant la notification, sauf dans le cas d'informations considérées comme impliquant une des infractions visées aux articles 3 à 7 de la directive 2011/93/UE;
d) une déclaration confirmant que le particulier ou l'entité soumettant la notification pense, de bonne foi, que les informations et les allégations qu'elle contient sont exactes et complètes.

3. Les notifications visées au présent article sont réputées donner lieu à la connaissance ou à la prise de conscience effective aux fins de l'article 6 de l'élément d'information spécifique concerné lorsqu'elles permettent à un fournisseur diligent de services d'hébergement d'identifier l'illégalité de l'activité ou de l'information concernée sans examen juridique détaillé.

4. Lorsque la notification contient les coordonnées électroniques du particulier ou de l'entité qui l'a soumise, le fournisseur de services d'hébergement envoie, dans les meilleurs délais, un accusé de réception de la notification à ce particulier ou cette entité.

5. Le fournisseur notifie également, dans les meilleurs délais, à ce particulier ou cette entité sa décision concernant les informations auxquelles la notification se rapporte, tout en fournissant des informations sur les possibilités de recours à l'égard de cette décision.

6. Les fournisseurs de services d'hébergement traitent les notifications qu'ils reçoivent au titre des mécanismes prévus au paragraphe 1 et prennent leurs décisions concernant les informations auxquelles les notifications se rapportent en temps opportun, de manière diligente, non arbitraire et objective. Lorsqu'ils font appel à des moyens automatisés aux fins de ce traitement ou de cette prise de décisions, ils incluent des informations sur cette utilisation dans la notification visée au paragraphe 5.

Article 17
Exposé des motifs

1. Les fournisseurs de services d'hébergement fournissent à tous les destinataires du service affectés un exposé des motifs clair et spécifique pour l'une ou l'autre des restrictions suivantes imposées au motif que les informations fournies par le destinataire du service constituent un contenu illicite ou sont incompatibles avec leurs conditions générales:

a) toute restriction de la visibilité d'éléments d'information spécifiques fournis par le destinataire du service, y compris le retrait de contenus, le fait de rendre l'accès à des contenus impossible ou le déclassement de contenus;

b) la suspension, la fin ou autre restriction des paiements monétaires;

c) la suspension ou la fin, en tout ou en partie, de la fourniture du service;

d) la suspension ou la suppression du compte du destinataire du service.

2. Le paragraphe 1 s'applique uniquement lorsque les coordonnées électroniques pertinentes sont connues du fournisseur. Il s'applique au plus tard à compter de la date à laquelle la restriction est imposée, indépendamment de la raison pour laquelle ou de la manière dont elle a été imposée.

Le paragraphe 1 ne s'applique pas lorsque les informations constituent un contenu commercial trompeur et de grande diffusion.

3. L'exposé des motifs visé au paragraphe 1 comprend au minimum les informations suivantes:

a) des informations indiquant si la décision implique soit de retirer des informations, de rendre l'accès à celles-ci impossible, de les déclasser, ou de restreindre leur visibilité, soit de suspendre ou de mettre fin aux paiements monétaires liés à ces informations, ou impose d'autres mesures visées au paragraphe 1 en ce qui concerne lesdites informations, et, le cas échéant, le champ d'application territorial de la décision et sa durée;

b) les faits et circonstances sur base desquels la décision a été prise, y compris, le cas échéant, des informations indiquant si la décision a été prise en vertu d'une notification soumise conformément à l'article 16 ou sur la base d'enquêtes d'initiative volontaires et, lorsque cela est strictement nécessaire, l'identité de la personne à l'origine de la notification;

c) le cas échéant, des informations relatives à l'utilisation de moyens automatisés pour prendre la décision, y compris des informations indiquant si la décision a été prise à l'égard de contenus détectés ou identifiés par des moyens automatisés;

d) lorsque la décision concerne des contenus présumés illicites, une référence au fondement juridique sous-jacent et des explications quant aux raisons pour lesquelles ces informations sont considérées comme des contenus illicites sur ce fondement;

e) lorsque la décision se fonde sur l'incompatibilité alléguée des informations avec les conditions générales du fournisseur de services d'hébergement, une référence aux clauses contractuelles sous-jacentes et des explications quant aux raisons pour lesquelles ces informations sont considérées comme incompatibles avec ces clauses;

f) des informations claires et aisément compréhensibles relatives aux possibilités de recours à la disposition du destinataire du service en ce qui concerne cette décision, notamment, le cas échéant, par l'intermédiaire de mécanismes internes de traitement des réclamations, d'un règlement extrajudiciaire des litiges et d'un recours juridictionnel.

4. Les informations fournies par les fournisseurs de services d'hébergement conformément au présent article sont claires et faciles à comprendre et aussi précises et détaillées que cela est raisonnablement possible compte tenu des circonstances données. En particulier, les informations sont de nature à permettre raisonnablement au destinataire du service concerné d'exercer les possibilités de recours visées au paragraphe 3, point f), de manière effective.

5. Le présent article ne s'applique pas aux injonctions visées à l'article 9.

Article 18
Notification des soupçons d'infraction pénale

1. Lorsqu'un fournisseur de services d'hébergement a connaissance d'informations conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une ou de plusieurs personnes a été commise, est en train d'être commise ou est susceptible d'être commise, il informe promptement les autorités répressives ou judiciaires de l'État membre ou des États membres concernés de son soupçon et fournit toutes les informations pertinentes disponibles.

2. Lorsque le fournisseur de services d'hébergement n'est pas en mesure de déterminer avec une certitude raisonnable l'État membre concerné, il informe les autorités répressives de l'État membre dans lequel il est établi ou dans lequel son représentant légal réside ou est établi ou informe Europol, ou les deux.

Aux fins du présent article, l'État membre concerné est l'État membre dans lequel l'infraction est suspectée d'avoir été commise, d'être commise ou est susceptible d'être commise, ou l'État membre dans lequel l'auteur présumé de l'infraction réside ou se trouve, ou l'État membre dans lequel la victime de l'infraction suspectée réside ou se trouve.

SECTION 3
Dispositions supplémentaires applicables aux fournisseurs de plateformes en ligne

Article 19
Exclusion des microentreprises et petites entreprises

1. La présente section, à l'exception de son article 24, paragraphe 3, ne s'applique pas aux fournisseurs de plateformes en ligne qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE.

La présente section, à l'exception de son article 24, paragraphe 3, ne s'applique pas aux fournisseurs de plateformes en ligne qui étaient qualifiés précédemment de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE, pendant les douze mois qui suivent la perte de ce statut en vertu de l'article 4, paragraphe 2, de ladite recommandation, sauf lorsqu'il s'agit de très grandes plateformes en ligne conformément à l'article 33.

2. Par dérogation au paragraphe 1 du présent article, la présente section s'applique aux fournisseurs de plateformes en ligne qui ont été désignés comme des très grandes plateformes en ligne conformément à l'article 33, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises.

Article 20
Système interne de traitement des réclamations

1. Les fournisseurs de plateformes en ligne fournissent aux destinataires du service, y compris aux particuliers ou aux entités qui ont soumis une notification, pour une période d'au moins six mois suivant la décision visée dans le présent paragraphe, l'accès à un système interne de traitement des réclamations efficace qui leur permet d'introduire, par voie électronique et gratuitement, des réclamations contre la décision prise par le fournisseur de la plateforme en ligne à la suite de la réception d'une notification ou contre les décisions suivantes prises par le fournisseur de la plateforme en ligne au motif que les informations fournies par les destinataires constituent un contenu illicite ou qu'elles sont incompatibles avec ses conditions générales:
a) les décisions sur la question de savoir s'il y a lieu ou non de retirer les informations, de rendre l'accès à celles-ci impossible ou de restreindre leur visibilité;
b) les décisions sur la question de savoir s'il y a lieu ou non de suspendre ou de mettre fin, en tout ou en partie, à la fourniture du service aux destinataires;
c) les décisions sur la question de savoir s'il y a lieu ou non de suspendre ou de supprimer le compte des destinataires;

d) les décisions sur la question de savoir s'il y a lieu ou non de suspendre la capacité de monétiser les informations fournies par les destinataires, de mettre fin à cette capacité ou de restreindre d'une autre manière cette capacité.

2. La période d'au moins six mois visée au paragraphe 1 du présent article court à partir du jour où le destinataire du service est informé de la décision, conformément à l'article 16, paragraphe 5, ou à l'article 17.

3. Les fournisseurs de plateformes en ligne veillent à ce que leurs systèmes internes de traitement des réclamations soient d'un accès et d'une utilisation aisés et permettent et facilitent la soumission de réclamations suffisamment précises et dûment étayées.

4. Les fournisseurs de plateformes en ligne traitent les réclamations soumises par l'intermédiaire de leurs systèmes internes de traitement des réclamations en temps opportun, de manière non discriminatoire, diligente et non arbitraire. Lorsqu'une réclamation contient suffisamment de motifs pour que le fournisseur de la plateforme en ligne considère que sa décision de ne pas agir à la suite de la notification est infondée ou que les informations auxquelles la réclamation se rapporte ne sont pas illicites et ne sont pas incompatibles avec ses conditions générales, ou lorsqu'elle contient des informations indiquant que la conduite du plaignant ne justifie pas la mesure prise, le fournisseur infirme sa décision visée au paragraphe 1 dans les meilleurs délais.

5. Les fournisseurs de plateformes en ligne informent les plaignants dans les meilleurs délais de la décision motivée qu'ils prennent en ce qui concerne les informations auxquelles la réclamation se rapporte et de la possibilité d'avoir accès à un règlement extrajudiciaire des litiges prévue à l'article 21 et des autres possibilités de recours disponibles.

6. Les fournisseurs de plateformes en ligne veillent à ce que les décisions visées au paragraphe 5 soient prises sous le contrôle de collaborateurs dûment qualifiés, et pas uniquement par des moyens automatisés.

Article 21
Règlement extrajudiciaire des litiges

1. Les destinataires du service, y compris les particuliers ou les entités qui ont soumis des notifications, qui sont destinataires des décisions visées à l'article 20, paragraphe 1, ont le droit de choisir tout organe de règlement extrajudiciaire des litiges qui a été certifié conformément au paragraphe 3 du présent article en vue de résoudre les litiges relatifs à ces décisions, y compris pour les réclamations qui n'ont pas été résolues par le système interne de traitement des réclamations visé audit article.

Les fournisseurs de plateformes en ligne veillent à ce que les informations relatives à la possibilité pour les destinataires du service d'avoir accès à un règlement extrajudiciaire des litiges, conformément au premier alinéa, soient facilement accessibles sur leur interface en ligne, claires et aisément compréhensibles.

Le premier alinéa est sans préjudice du droit du destinataire du service concerné d'engager, à tout moment, une procédure pour contester lesdites décisions prises par les fournisseurs de plateformes en ligne devant une juridiction conformément au droit applicable.

2. Les deux parties s'engagent, de bonne foi, avec l'organe de règlement extrajudiciaire des litiges certifié qui est choisi en vue de résoudre le litige.

Les fournisseurs de plateformes en ligne peuvent refuser de s'engager avec cet organe de règlement extrajudiciaire des litiges si un litige concernant les mêmes informations et les mêmes motifs d'illégalité ou d'incompatibilité alléguée du contenu a déjà été résolu.

L'organe de règlement extrajudiciaire des litiges certifié n'a pas le pouvoir d'imposer aux parties un règlement du litige contraignant.

3. Le coordinateur pour les services numériques de l'État membre dans lequel est établi l'organe de règlement extrajudiciaire des litiges certifie cet organe, à sa

demande, pour une période maximale de cinq ans, qui peut être renouvelée, lorsque l'organe a démontré qu'il remplit l'ensemble des conditions suivantes:
a) il est impartial et indépendant, y compris financièrement indépendant, des fournisseurs de plateformes en ligne et des destinataires du service fourni par les fournisseurs de plateformes en ligne, y compris des particuliers ou des entités qui ont soumis des notifications;
b) il dispose de l'expertise nécessaire en ce qui concerne les questions liées à un ou plusieurs domaines particuliers de contenu illicite, ou en ce qui concerne l'application et la mise en application des conditions générales d'un ou de plusieurs types de plateformes en ligne, lui permettant de contribuer efficacement au règlement d'un litige;
c) ses membres ne sont pas rémunérés en fonction de l'issue de la procédure;
d) le processus de règlement extrajudiciaire des litiges qu'il propose est facilement accessible au moyen d'une technologie des communications électroniques et prévoit la possibilité d'engager le processus de règlement des litiges et de soumettre les documents justificatifs nécessaires en ligne;
e) il est en mesure de régler des litiges de manière rapide, efficace et économiquement avantageuse, et dans au minimum une des langues officielles des institutions de l'Union;
f) le processus de règlement extrajudiciaire des litiges qu'il propose se déroule conformément à des règles de procédure claires et équitables, qui sont aisément et publiquement accessibles et qui respectent le droit applicable, y compris le présent article.

Le cas échéant, le coordinateur pour les services numériques précise dans le certificat:

a) les questions particulières sur lesquelles porte l'expertise de l'organe, visées au premier alinéa, point b); et

b) la ou les langues officielles des institutions de l'Union dans laquelle ou lesquelles l'organe est en mesure de régler des litiges, comme il est prévu au premier alinéa, point e).

4. Les organes de règlement extrajudiciaire des litiges certifiés font rapport, une fois par an, au coordinateur pour les services numériques qui les a certifiés, sur leur fonctionnement, en précisant au moins le nombre de litiges qu'ils ont reçus, les informations sur l'issue de ces litiges, le laps de temps moyen nécessaire à leur résolution et les éventuelles lacunes ou difficultés rencontrées. Ils fournissent des informations supplémentaires à la demande dudit coordinateur pour les services numériques.

Les coordinateurs pour les services numériques établissent tous les deux ans un rapport sur le fonctionnement des organes de règlement extrajudiciaire des litiges qu'ils ont certifiés. En particulier, ce rapport:

a) indique le nombre de litiges que chaque organe de règlement extrajudiciaire des litiges certifié a reçus chaque année;

b) indique l'issue des procédures portées devant ces organes et le laps de temps moyen nécessaire à la résolution des litiges;

c) recense et explique les éventuelles lacunes ou difficultés systématiques ou sectorielles rencontrées en rapport avec le fonctionnement de ces organes;

d) recense les bonnes pratiques concernant ce fonctionnement;

e) formule, le cas échéant, des recommandations sur la manière d'améliorer ce fonctionnement.

Les organes de règlement extrajudiciaire des litiges certifiés mettent leurs décisions à la disposition des parties dans un délai raisonnable et au plus tard 90 jours civils après la réception de la plainte. En cas de litiges très complexes, l'organe de règlement extrajudiciaire des litiges certifié peut, de sa propre initiative, prolonger le délai de 90 jours civils, pour une période supplémentaire n'excédant pas 90 jours, dans la limite d'une durée totale maximale de 180 jours.

5. Lorsque l'organe de règlement extrajudiciaire des litiges se prononce sur le litige en faveur du destinataire du service, y compris le particulier ou l'entité qui a soumis

une notification, le fournisseur de la plateforme en ligne supporte tous les frais facturés par l'organe de règlement extrajudiciaire des litiges et rembourse à ce destinataire, y compris le particulier ou l'entité, toute autre dépense raisonnable qu'il a effectuée en lien avec le règlement du litige. Lorsque l'organe de règlement extrajudiciaire des litiges se prononce sur le litige en faveur du fournisseur de la plateforme en ligne, le destinataire du service, y compris le particulier ou l'entité, n'est pas tenu de rembourser les frais ou autres dépenses que le fournisseur de la plateforme en ligne a engagés ou dont il est redevable en lien avec le règlement du litige, à moins que l'organe de règlement extrajudiciaire des litiges constate que ce destinataire a manifestement agi de mauvaise foi.

Les frais facturés par l'organe de règlement extrajudiciaire des litiges aux fournisseurs de plateformes en ligne pour le règlement du litige sont raisonnables et n'excèdent en aucun cas les coûts engagés par l'organe. Pour les destinataires du service, le règlement du litige est accessible gratuitement ou moyennant une somme symbolique.

Les organes de règlement extrajudiciaire des litiges certifiés informent le destinataire du service, y compris les particuliers ou les entités qui ont soumis une notification, et le fournisseur de la plateforme en ligne concerné, des frais ou des mécanismes employés pour calculer les frais, avant le début du processus de règlement du litige.

6. Les États membres peuvent établir des organes de règlement extrajudiciaire des litiges aux fins du paragraphe 1 ou apporter un soutien aux activités de certains ou de tous les organes de règlement extrajudiciaire des litiges qu'ils ont certifiés conformément au paragraphe 3.

Les États membres veillent à ce qu'aucune des activités qu'ils entreprennent au titre du premier alinéa ne nuise à la capacité de leurs coordinateurs pour les services numériques à certifier les organes concernés conformément au paragraphe 3.

7. Le coordinateur pour les services numériques qui a certifié un organe de règlement extrajudiciaire des litiges révoque cette certification s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, que l'organe de règlement extrajudiciaire des litiges ne remplit plus les conditions énoncées au paragraphe
3. Avant de révoquer cette certification, le coordinateur pour les services numériques donne à cet organe la possibilité de réagir aux conclusions de son enquête et à son intention de révoquer la certification de l'organe de règlement extrajudiciaire des litiges.

8. Les coordinateurs pour les services numériques notifient à la Commission la liste des organes de règlement extrajudiciaire des litiges qu'ils ont certifiés conformément au paragraphe 3, y compris, le cas échéant, les spécifications visées au second alinéa dudit paragraphe, ainsi que la liste des organes de règlement extrajudiciaire des litiges dont ils ont révoqué la certification. La Commission publie et tient à jour une liste de ces organes, comprenant ces spécifications, sur un site internet dédié, facilement accessible, prévu à cet effet.

9. Le présent article est sans préjudice de la directive 2013/11/UE et des procédures et entités de règlement extrajudiciaire des litiges de consommation qu'elle établit.

Article 22
Signaleurs de confiance

1. Les fournisseurs de plateformes en ligne prennent les mesures techniques et organisationnelles nécessaires pour veiller à ce que les notifications soumises par des signaleurs de confiance, agissant dans leur domaine d'expertise désigné, par l'intermédiaire des mécanismes visés à l'article 16, soient prioritaires et soient traitées et donnent lieu à des décisions dans les meilleurs délais.

2. Le statut de signaleur de confiance au titre du présent règlement est attribué, sur demande présentée par une entité, quelle qu'elle soit, par le coordinateur pour les services numériques de l'État membre dans lequel l'entité présentant la demande est établie, à l'entité présentant la demande qui a démontré qu'elle remplit l'ensemble des conditions suivantes:

a) elle dispose d'une expertise et de compétences particulières aux fins de détecter, d'identifier et de notifier des contenus illicites;
b) elle est indépendante de tout fournisseur de plateformes en ligne;
c) elle exerce ses activités aux fins de la soumission des notifications de manière diligente, précise et objective.

3. Les signaleurs de confiance publient, au minimum une fois par an, des rapports détaillés et facilement compréhensibles sur les notifications soumises conformément à l'article 16 pendant la période concernée. Le rapport indique au moins le nombre de notifications, classées selon les critères suivants:
a) l'identité du fournisseur de services d'hébergement;
b) le type de contenu présumé illicite notifié;
c) l'action entreprise par le fournisseur.

Ces rapports comprennent une explication des procédures mises en place pour garantir que le signaleur de confiance conserve son indépendance.

Les signaleurs de confiance envoient ces rapports au coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance et les mettent à la disposition du public. Les informations figurant dans ces rapports ne contiennent pas de données à caractère personnel.

4. Les coordinateurs pour les services numériques communiquent à la Commission et au comité les noms, adresses postales et adresses de courrier électronique des entités auxquelles ils ont attribué le statut de signaleur de confiance conformément au paragraphe 2 ou dont ils ont suspendu le statut de signaleur de confiance conformément au paragraphe 6 ou révoqué ledit statut conformément au paragraphe 7.

5. La Commission publie les informations visées au paragraphe 4 dans une base de données mise à la disposition du public, dans un format facilement accessible et lisible par une machine, et tient à jour cette base de données.

6. Lorsqu'un fournisseur de plateformes en ligne dispose d'informations indiquant qu'un signaleur de confiance a soumis, par l'intermédiaire des mécanismes visés à l'article 16, un nombre significatif de notifications manquant de précision, inexactes ou insuffisamment étayées, notamment des informations recueillies en lien avec le traitement de réclamations par des systèmes internes de traitement des réclamations visés à l'article 20, paragraphe 4, il communique ces informations au coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance à l'entité concernée, en fournissant les explications et les documents justificatifs nécessaires. Dès réception des informations fournies par le fournisseur de plateformes en ligne et si le coordinateur pour les services numériques estime qu'il existe des raisons légitimes d'ouvrir une enquête, le statut de signaleur de confiance est suspendu pendant la durée de l'enquête. Cette enquête est menée dans les meilleurs délais.

7. Le coordinateur pour les services numériques qui a attribué le statut de signaleur de confiance à une entité révoque ce statut s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, y compris les informations fournies par un fournisseur de plateformes en ligne en vertu du paragraphe 6, que l'entité ne remplit plus les conditions énoncées au paragraphe 2. Avant de révoquer ce statut, le coordinateur pour les services numériques donne à l'entité la possibilité de réagir aux conclusions de son enquête et à son intention de révoquer le statut de signaleur de confiance de l'entité.

8. La Commission, après avoir consulté le comité, publie, si nécessaire, des lignes directrices pour aider les fournisseurs de plateformes en ligne et les coordinateurs pour les services numériques à appliquer les paragraphes 2, 6 et 7.

Article 23
Mesures de lutte et de protection contre les utilisations abusives

1. Les fournisseurs de plateformes en ligne suspendent, pendant une période raisonnable et après avoir émis un avertissement préalable, la fourniture de leurs services aux destinataires du service qui fournissent fréquemment des contenus manifestement illicites.

2. Les fournisseurs de plateformes en ligne suspendent, pendant une période raisonnable et après avoir émis un avertissement préalable, le traitement des notifications et des réclamations soumises par l'intermédiaire des mécanismes de notification et d'action et des systèmes internes de traitement des réclamations prévus aux articles 16 et 20, respectivement, par des particuliers, des entités ou des plaignants qui soumettent fréquemment des notifications ou des réclamations manifestement infondées.

3. Lorsqu'ils décident d'une suspension, les fournisseurs de plateformes en ligne apprécient au cas par cas et en temps opportun, de manière diligente et objective, si le destinataire du service, le particulier, l'entité ou le plaignant se livre aux utilisations abusives visées aux paragraphes 1 et 2, en tenant compte de l'ensemble des faits et circonstances pertinents qui ressortent des informations dont ils disposent. Ces circonstances comprennent au moins les éléments suivants:

a) le nombre, en valeur absolue, d'éléments de contenus manifestement illicites ou de notifications ou de réclamations manifestement infondées, soumis au cours d'une période donnée;

b) la proportion relative de ces éléments par rapport au nombre total d'éléments d'information fournis ou de notifications soumises au cours d'une période donnée;

c) la gravité des utilisations abusives, y compris la nature des contenus illicites, et de leurs conséquences;

d) lorsqu'il est possible de la déterminer, l'intention du destinataire du service, du particulier, de l'entité ou du plaignant.

4. Les fournisseurs de plateformes en ligne énoncent de manière claire et détaillée, dans leurs conditions générales, leur politique relative aux utilisations abusives visées aux paragraphes 1 et 2, et donnent des exemples des faits et circonstances dont ils tiennent compte pour apprécier si certains comportements constituent des utilisations abusives et déterminer la durée de la suspension.

Article 24
Obligations en matière de rapports de transparence incombant aux fournisseurs de plateformes en ligne

1. En plus des informations visées à l'article 15, les fournisseurs de plateformes en ligne intègrent aux rapports visés dans cet article des informations sur les points suivants:
a) le nombre de litiges transmis aux organes de règlement extrajudiciaire des litiges visés à l'article 21, les résultats du règlement des litiges, le délai médian nécessaire pour mener à bien les procédures de règlement des litiges et la proportion de litiges pour lesquels le fournisseur de la plateforme en ligne a mis en œuvre les décisions de l'organe;
b) le nombre de suspensions imposées au titre de l'article 23, en faisant la distinction entre les suspensions prononcées en raison de la fourniture de contenus manifestement illicites, de la soumission de notifications manifestement infondées et de la soumission de réclamations manifestement infondées.

2. Au plus tard le 17 février 2023 et au moins tous les six mois par la suite, les fournisseurs publient pour chaque plateforme en ligne ou chaque moteur de recherche en ligne, dans une section de leur interface en ligne accessible au public, des informations relatives à la moyenne mensuelle des destinataires actifs du service dans l'Union, calculée sous forme de moyenne au cours des six derniers mois et conformément à la méthodologie établie dans les actes délégués visés à l'article 33, paragraphe 3, lorsque ces actes délégués ont été adoptés.

cf. Actes délégués

3. Les fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne communiquent au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, à leur demande et dans les meilleurs délais, les informations visées au paragraphe 2, mises à jour jusqu'au moment de la demande. Ledit coordinateur pour les services numériques ou la Commission peuvent demander au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de fournir des informations complémentaires concernant le calcul visé audit paragraphe, y compris

des explications et des justifications quant aux données utilisées. Ces informations ne contiennent pas de données à caractère personnel.

4. Lorsque le coordinateur pour les services numériques de l'État membre d'établissement a des raisons de considérer, sur la base des informations reçues en application des paragraphes 2 et 3 du présent article, qu'un fournisseur de plateformes en ligne ou de moteurs de recherche en ligne atteint le seuil du nombre mensuel moyen de destinataires actifs du service dans l'Union fixé à l'article 33, paragraphe 1, il en informe la Commission.

5. Les fournisseurs de plateformes en ligne soumettent à la Commission, dans les meilleurs délais, les décisions et les exposés des motifs visés à l'article 17, paragraphe 1, en vue de leur inclusion dans une base de données accessible au public, lisible par une machine, et gérée par la Commission. Les fournisseurs de plateformes en ligne veillent à ce que les informations soumises ne contiennent pas de données à caractère personnel.

6. La Commission peut adopter des actes d'exécution pour établir des modèles concernant la forme, le contenu et d'autres détails des rapports au titre du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

Article 25
Conception et organisation des interfaces en ligne

1. Les fournisseurs de plateformes en ligne ne conçoivent, n'organisent ni n'exploitent leurs interfaces en ligne de façon à tromper ou à manipuler les destinataires de leur service ou de toute autre façon propre à altérer ou à entraver substantiellement la capacité des destinataires de leur service à prendre des décisions libres et éclairées.

2. L'interdiction contenue dans le paragraphe 1 ne s'applique pas aux pratiques couvertes par la directive 2005/29/CE ou le règlement (UE) 2016/679.

cf. RGPD

3. La Commission peut publier des lignes directrices sur la manière dont le paragraphe 1 s'applique à des pratiques spécifiques, notamment:
a) accorder davantage d'importance à certains choix au moment de demander au destinataire du service de prendre une décision;

b) demander de façon répétée au destinataire du service de faire un choix lorsque ce choix a déjà été fait, notamment en faisant apparaître une fenêtre contextuelle qui perturbe l'expérience de l'utilisateur;
c) rendre la procédure de désinscription d'un service plus compliquée que l'inscription à celui-ci.

Article 26
Publicité sur les plateformes en ligne

1. Les fournisseurs de plateformes en ligne qui présentent de la publicité sur leurs interfaces en ligne veillent à ce que, pour chaque publicité spécifique présentée à chaque destinataire individuel, les destinataires du service puissent de manière claire, précise, non ambiguë et en temps réel:
a) se rendre compte que les informations sont de la publicité, y compris au moyen de marquages bien visibles qui pourraient suivre des normes en vertu de l'article 44;
b) identifier la personne physique ou morale pour le compte de laquelle la publicité est présentée;
c) identifier la personne physique ou morale qui a payé pour la publicité, si cette personne est différente de la personne physique ou morale visée au point b); et
d) déterminer les informations utiles, qui doivent être directement et facilement accessibles à partir de la publicité, concernant les principaux paramètres utilisés pour déterminer le destinataire auquel la publicité est présentée et, le cas échéant, la manière dont ces paramètres peuvent être modifiés.

2. Les fournisseurs de plateformes en ligne fournissent aux destinataires du service une fonctionnalité leur permettant de déclarer si le contenu qu'ils fournissent constitue une communication commerciale ou s'il contient une telle communication.

Lorsque le destinataire du service soumet une déclaration en vertu du présent paragraphe, le fournisseur de plateformes en ligne veille à ce que les autres destinataires du service puissent se rendre compte de manière claire, non ambiguë et en temps réel, y compris au moyen de marquages bien visibles, qui pourraient suivre des normes en vertu de l'article 44, que le contenu fourni par le destinataire du service constitue une communication commerciale ou contient une telle communication, telle qu'elle est décrite dans cette déclaration.

3. Les fournisseurs de plateformes en ligne ne présentent pas aux destinataires du service de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679, en utilisant les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679.

profilage interdit sur données sensibles

cf. RGPD

Article 27
Transparence du système de recommandation

1. Les fournisseurs de plateformes en ligne qui utilisent des systèmes de recommandation établissent dans leurs conditions générales, dans un langage simple et compréhensible, les principaux paramètres utilisés dans leurs systèmes de recommandation, ainsi que les options dont disposent les destinataires du service pour modifier ou influencer ces principaux paramètres.

2. Les principaux paramètres visés au paragraphe 1 expliquent pourquoi certaines informations sont suggérées au destinataire du service. Ils précisent, au minimum:
a) les critères les plus importants pour déterminer les informations suggérées au destinataire du service;
b) les raisons de l'importance relative de ces paramètres.

3. Lorsque plusieurs options sont disponibles conformément au paragraphe 1 pour les systèmes de recommandation qui déterminent l'ordre relatif des informations présentées aux destinataires du service, les fournisseurs de plateformes en ligne prévoient également une fonctionnalité permettant aux destinataires du service de sélectionner et de modifier à tout moment leur option favorite. Cette fonctionnalité est directement et aisément accessible dans la rubrique spécifique de l'interface de la plateforme en ligne où les informations sont hiérarchisées.

Article 28
Protection des mineurs en ligne

1. Les fournisseurs de plateformes en ligne accessibles aux mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service.

2. Les fournisseurs de plateformes en ligne ne présentent pas sur leur interface de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679 en utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils ont connaissance avec une certitude raisonnable que le destinataire du service est un mineur.

profilage publicitaire interdit pour les mineurs

cf. RGPD

3. Le respect des obligations énoncées dans le présent article n'impose pas aux fournisseurs de plateformes en ligne de traiter des données à caractère personnel supplémentaires afin de déterminer si le destinataire du service est un mineur.

4. La Commission, après avoir consulté le comité, peut publier des lignes directrices pour aider les fournisseurs de plateformes en ligne à appliquer le paragraphe 1.

SECTION 4
Dispositions supplémentaires applicables aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels

Article 29
Exclusion des microentreprises et petites entreprises

1. La présente section ne s'applique pas aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels qui peuvent être qualifiés de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE.

La présente section ne s'applique pas aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels qui étaient qualifiés précédemment de microentreprises ou de petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE, pendant les douze mois qui suivent la perte de ce statut en vertu de l'article 4, paragraphe 2, de ladite recommandation, sauf s'il s'agit de très grandes plateformes en ligne conformément à l'article 33.

2. Par dérogation au paragraphe 1 du présent article, la présente section s'applique aux fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels qui ont été désignés comme des très grandes plateformes en ligne conformément à l'article 33, indépendamment du fait qu'ils soient qualifiés de microentreprises ou de petites entreprises.

Article 30
Traçabilité des professionnels

1. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels veillent à ce que ces derniers puissent uniquement utiliser ces plateformes en ligne pour promouvoir des messages relatifs à des produits ou services ou proposer des produits ou services à des consommateurs situés dans l'Union si, avant l'utilisation de leurs services à ces fins, ils ont obtenu les informations suivantes, lorsque cela s'applique au professionnel:
a) le nom, l'adresse, le numéro de téléphone et l'adresse de courrier électronique du professionnel;
b) un exemplaire du document d'identification du professionnel ou toute autre identification électronique telle qu'elle est définie à l'article 3 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil[40];
c) les coordonnées du compte de paiement du professionnel;
d) lorsque le professionnel est inscrit à un registre commercial ou un registre public similaire, le registre du commerce auquel le professionnel est inscrit et son numéro d'enregistrement ou un moyen équivalent d'identification dans ce registre;
e) une autocertification du professionnel par laquelle il s'engage à ne fournir que des produits ou services conformes aux règles applicables du droit de l'Union.

2. Lorsqu'il reçoit les informations visées au paragraphe 1, et avant d'autoriser le professionnel concerné à utiliser ses services, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels déploie tous ses efforts pour évaluer si les informations visées au paragraphe 1, points a) à e), sont fiables et complètes, au moyen de toute base de données ou interface en ligne officielle, libre d'accès, mise à disposition par un État membre ou l'Union, ou en demandant au professionnel de fournir des documents justificatifs provenant de sources fiables. Aux fins du présent règlement, les professionnels sont responsables de l'exactitude des informations fournies.

Pour ce qui concerne les professionnels qui utilisent déjà les services de fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, aux fins visées au paragraphe 1, à la date du 17 février

40. Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

2024, le fournisseur déploie tous ses efforts pour obtenir du professionnel concerné les informations énumérées dans un délai de douze mois. Lorsque le professionnel concerné ne fournit pas les informations dans ce délai, le fournisseur suspend la fourniture de ses services à ce professionnel jusqu'à ce que celui-ci ait communiqué toutes les informations en question.

3. Lorsque le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels dispose de suffisamment d'indices ou a des raisons de penser qu'un élément d'information visé au paragraphe 1 obtenu du professionnel concerné est inexact, incomplet ou obsolète, ce fournisseur demande au professionnel de remédier à cette situation, dans les meilleurs délais ou dans le délai prévu par le droit de l'Union et le droit national.

Lorsque le professionnel ne corrige pas ou ne complète pas cette information, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels suspend rapidement la fourniture de son service audit professionnel en ce qui concerne l'offre de produits ou de services aux consommateurs situés dans l'Union, jusqu'à ce que la demande soit entièrement satisfaite.

4. Sans préjudice de l'article 4 du règlement (UE) 2019/1150, si le fournisseur d'une plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels refuse d'autoriser un professionnel à utiliser son service en vertu du paragraphe 1 ou suspend la fourniture de son service en vertu du paragraphe 3 du présent article, le professionnel concerné a le droit d'introduire une réclamation conformément aux articles 20 et 21 du présent règlement.

5. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels stockent les informations obtenues au titre des paragraphes 1 et 2 de façon sécurisée pour une durée de six mois après la fin de leur relation contractuelle avec le professionnel concerné. Ils suppriment par la suite ces informations.

6. Sans préjudice du paragraphe 2 du présent article, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels ne divulgue les informations à des tiers que lorsqu'il y est tenu conformément au droit applicable, y compris les injonctions visées à l'article 10 et toute injonction émise par les autorités compétentes des États membres ou la Commission aux fins de l'exécution des missions qui leur incombent au titre du présent règlement.

7. Le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels met les informations énumérées au paragraphe 1, points a), d) et e), à la disposition des destinataires du service, de manière claire, aisément accessible et compréhensible. Ces informations sont disponibles au moins sur l'interface en ligne de la plateforme en ligne où les informations sur le produit ou le service sont présentées.

Article 31
Conformité dès la conception

1. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels veillent à ce que leur interface en ligne soit conçue et organisée d'une manière permettant aux professionnels de respecter leurs obligations en matière d'informations précontractuelles, de conformité et d'informations sur la sécurité des produits qui leur incombent en vertu du droit applicable de l'Union.

En particulier, le fournisseur concerné veille à ce que son interface en ligne permette aux professionnels de fournir des informations concernant le nom, l'adresse, le numéro de téléphone et l'adresse de courrier électronique de l'opérateur économique, tel qu'il est défini à l'article 3, point 13), du règlement (UE) 2019/1020 et dans d'autres dispositions du droit de l'Union.

2. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels conçoivent et organisent leur

interface en ligne de manière à permettre aux professionnels de fournir au moins ce qui suit:

a) les informations nécessaires à l'identification claire et sans ambiguïté des produits ou services promus ou proposés aux consommateurs situés dans l'Union par l'intermédiaire des services des fournisseurs;
b) tout signe permettant d'identifier le professionnel, tel que la marque, un symbole ou un logo; et

c) le cas échéant, les informations concernant l'étiquetage et le marquage conformément aux règles du droit de l'Union applicable en matière de sécurité et de conformité des produits.

3. Les fournisseurs de plateformes en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels déploient tous leurs efforts pour déterminer si ces professionnels ont communiqué les informations visées aux paragraphes 1 et 2 avant de les autoriser à proposer leurs produits ou leurs services sur lesdites plateformes. Après avoir autorisé le professionnel à proposer des produits ou des services sur sa plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels, le fournisseur s'efforce, dans la mesure du raisonnable, de vérifier de manière aléatoire, dans une base de données en ligne ou une interface en ligne officielle, librement accessible et lisible par une machine, si les produits ou services proposés ont été recensés comme étant illégaux.

Article 32
Droit à l'information

1. Lorsque le fournisseur d'une plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels a connaissance, par quelque moyen que ce soit, qu'un professionnel propose un produit ou service illégal à des consommateurs situés dans l'Union par l'intermédiaire de ses services, ledit fournisseur informe, dans la mesure où il dispose de leurs coordonnées, les consommateurs qui ont acheté le produit ou le service illégal en question par l'intermédiaire de ses services, de ce qui suit:
a) le fait que le produit ou service est illégal;
b) l'identité du professionnel; et
c) tout moyen de recours pertinent.

L'obligation prévue au premier alinéa est limitée aux achats de produits ou services illégaux réalisés dans les six mois précédant le moment où le fournisseur a eu connaissance de l'illégalité.

2. Lorsque, dans la situation visée au paragraphe 1, le fournisseur de la plateforme en ligne permettant aux consommateurs de conclure des contrats à distance avec des professionnels ne dispose pas des coordonnées de tous les consommateurs concernés, il met à la disposition du public, de manière facilement accessible, sur son interface en ligne des informations concernant les produits ou services illégaux, l'identité du professionnel et les voies de recours pertinentes.

SECTION 5
Obligations supplémentaires de gestion des risques systémiques imposées aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

Article 33
Très grandes plateformes en ligne et très grands moteurs de recherche en ligne

1. La présente section s'applique aux plateformes en ligne et aux moteurs de recherche en ligne qui ont un nombre mensuel moyen de destinataires actifs du service dans l'Union égal ou supérieur à 45 millions, et qui sont désignés comme des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne en vertu du paragraphe 4.

2. La Commission adopte des actes délégués conformément à l'article 87 pour ajuster le nombre mensuel moyen de destinataires actifs du service dans l'Union visé au paragraphe 1 lorsque la population de l'Union augmente ou diminue d'au moins 5 % par rapport à sa population de 2020 ou par rapport à sa population après un ajustement effectué au moyen d'un acte délégué dans l'année au cours de laquelle le dernier acte délégué en date a été adopté. Dans ce cas de figure, elle ajuste le nombre de manière à ce qu'il corresponde à 10 % de la population de l'Union dans l'année au cours de laquelle elle adopte l'acte délégué, arrondi à la hausse ou à la baisse de sorte que le nombre puisse être exprimé en millions.

cf. Actes délégués

3. La Commission peut adopter des actes délégués, conformément à l'article 87, après avoir consulté le comité, pour compléter les dispositions du présent règlement en établissant la méthodologie pour calculer le nombre mensuel moyen de destinataires actifs du service dans l'Union aux fins du paragraphe 1 du présent article et de l'article 24, paragraphe 2, en veillant à ce que cette méthode tienne compte des évolutions du marché et de la technologie.

cf. Actes délégués

4. La Commission, après avoir consulté l'État membre d'établissement ou pris en compte les informations fournies par le coordinateur pour les services numériques de l'État membre d'établissement conformément à l'article 24, paragraphe 4, adopte une décision désignant comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne aux fins du présent règlement la plateforme en ligne ou le moteur de recherche en ligne dont le nombre mensuel moyen de destinataires actifs du service est égal ou supérieur au nombre visé au paragraphe 1 du présent article. La Commission prend cette décision sur la base des données communiquées par le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne en vertu de l'article 24, paragraphe 2, des informations demandées en vertu de l'article 24, paragraphe 3, ou de toute autre information à la disposition de la Commission.

Le fait pour le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne de ne pas se conformer à l'article 24, paragraphe 2, ou de ne pas donner suite à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission exprimée en vertu de l'article 24, paragraphe 3, n'empêche pas la Commission de désigner ce fournisseur comme un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne conformément au présent paragraphe.

Lorsque la Commission fonde sa décision sur d'autres informations dont elle dispose en vertu du premier alinéa du présent paragraphe, ou sur des informations complémentaires demandées en vertu de l'article 24, paragraphe 3, elle donne au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné un délai de dix jours ouvrables pour faire part de son point de vue sur ses conclusions préliminaires et sur son intention de désigner la plateforme en ligne ou le moteur de recherche en ligne comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement. La Commission tient dûment compte du point de vue présenté par le fournisseur concerné.

Le fait pour le fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné de ne pas faire part de son point de vue en vertu du troisième alinéa n'empêche pas la Commission de désigner cette plateforme en ligne ou ce moteur de recherche en ligne comme une très grande plateforme en ligne ou un très grand moteur de recherche en ligne, respectivement, sur la base des informations dont elle dispose.

5. La Commission met fin à cette désignation si, pendant une période ininterrompue d'un an, la plateforme en ligne ou le moteur de recherche en ligne n'a pas un nombre mensuel moyen de destinataires actifs supérieur ou égal au nombre visé au paragraphe 1.

6. La Commission notifie, sans retard injustifié, les décisions qu'elle prend en vertu des paragraphes 4 et 5 au fournisseur de la plateforme en ligne ou du moteur de recherche en ligne concerné, au comité et au coordinateur pour les services numériques de l'État membre d'établissement.

La Commission veille à ce que la liste des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne désignés soit publiée au Journal officiel de

l'Union européenne et tient cette liste à jour. Les obligations établies dans la présente section s'appliquent ou cessent de s'appliquer aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne concernés quatre mois après la notification adressée au fournisseur concerné visée au premier alinéa.

Article 34
Évaluation des risques

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne recensent, analysent et évaluent de manière diligente tout risque systémique au sein de l'Union découlant de la conception ou du fonctionnement de leurs services et de leurs systèmes connexes, y compris des systèmes algorithmiques, ou de l'utilisation faite de leurs services.

Ils procèdent aux évaluations des risques au plus tard à la date d'application visée à l'article 33, paragraphe 6, deuxième alinéa, puis au moins une fois par an, et en tout état de cause avant de déployer des fonctionnalités susceptibles d'avoir une incidence critique sur les risques recensés en vertu du présent article. Cette évaluation des risques est spécifique à leurs services et proportionnée aux risques systémiques, de la gravité et de la probabilité desquels elle tient compte, et comprend les risques systémiques suivants:

a) la diffusion de contenus illicites par l'intermédiaire de leurs services;

b) tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, en particulier le droit fondamental à la dignité humaine consacré à l'article 1er de la Charte, au respect de la vie privée et familiale consacré à l'article 7 de la Charte, à la protection des données à caractère personnel consacré à l'article 8 de la Charte, à la liberté d'expression et d'information, y compris la liberté et le pluralisme des médias, consacré à l'article 11 de la Charte, et à la non- discrimination consacré à l'article 21 de la Charte, les droits fondamentaux relatifs aux droits de l'enfant consacrés à l'article 24 de la Charte et le droit fondamental à un niveau élevé de protection des consommateurs consacré à l'article 38 de la Charte;

c) tout effet négatif réel ou prévisible sur le discours civique, les processus électoraux et la sécurité publique;

d) tout effet négatif réel ou prévisible lié aux violences sexistes et à la protection de la santé publique et des mineurs et les conséquences négatives graves sur le bien-être physique et mental des personnes.

2. Lorsqu'ils procèdent à des évaluations des risques, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne examinent notamment si et comment les facteurs suivants influencent les risques systémiques visés au paragraphe 1 et en tiennent compte:

a) la conception de leurs systèmes de recommandation et de tout autre système algorithmique pertinent;

b) leurs systèmes de modération des contenus;

c) les conditions générales applicables et leur mise en application;

d) les systèmes de sélection et de présentation de la publicité;

e) les pratiques du fournisseur en matière de données.

Les évaluations examinent également si et comment les risques visés au paragraphe 1 sont influencés par la manipulation intentionnelle du service desdits fournisseurs, y compris par l'utilisation non authentique ou l'exploitation automatisée du service, ainsi que par l'amplification et la diffusion potentiellement rapide et à grande échelle de contenus illicites et d'informations incompatibles avec leurs conditions générales.

L'évaluation tient compte des aspects régionaux ou linguistiques spécifiques, y compris lorsqu'ils sont propres à un État membre.

3. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne conservent les documents justificatifs des évaluations des risques pendant au moins trois ans après la réalisation de ces évaluations, et les communiquent à la Commission et au coordinateur pour les services numériques de l'État membre d'établissement, à leur demande.

Article 35
Atténuation des risques

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne mettent en place des mesures d'atténuation raisonnables, proportionnées et efficaces, adaptées aux risques systémiques spécifiques recensés conformément à l'article 34, en tenant compte en particulier de l'incidence de ces mesures sur les droits fondamentaux. Ces mesures peuvent inclure, le cas échéant:

a) l'adaptation de la conception, des caractéristiques ou du fonctionnement de leurs services, y compris leurs interfaces en ligne;

b) l'adaptation de leurs conditions générales et de la mise en application de celles-ci;

c) l'adaptation des processus de modération des contenus, y compris la rapidité et la qualité du traitement des notifications relatives à des types spécifiques de contenus illicites et, le cas échéant, le retrait rapide des contenus qui ont fait l'objet d'une notification ou le blocage de l'accès à ces contenus, en particulier en ce qui concerne les discours haineux illégaux ou la cyberviolence, ainsi que l'adaptation des processus décisionnels pertinents et des ressources dédiées à la modération des contenus;

d) le test et l'adaptation de leurs systèmes algorithmiques, y compris leurs systèmes de recommandation;

e) l'adaptation de leurs systèmes de publicité et l'adoption de mesures ciblées destinées à limiter la présentation de publicités, ou à en adapter la présentation, en association avec le service fourni;

f) le renforcement des processus internes, des ressources, des tests, de la documentation ou de la surveillance d'une quelconque de leurs activités, notamment en ce qui concerne la détection des risques systémiques;

g) la mise en place d'une coopération avec les signaleurs de confiance, ou l'ajustement de cette coopération, conformément à l'article 22, ainsi que la mise en œuvre des décisions prises par les organes de règlement extrajudiciaire des litiges en vertu de l'article 21;

h) la mise en place d'une coopération avec d'autres fournisseurs de plateformes en ligne ou de moteurs de recherche en ligne, ou l'ajustement de cette coopération, sur la base des codes de conduite et des protocoles de crise visés aux articles 45 et 48, respectivement;

i) l'adoption de mesures de sensibilisation et l'adaptation de leur interface en ligne, afin de donner plus d'informations aux destinataires du service;

j) l'adoption de mesures ciblées visant à protéger les droits de l'enfant, y compris la vérification de l'âge et des outils de contrôle parental, ou des outils permettant d'aider les mineurs à signaler les abus ou à obtenir un soutien, s'il y a lieu;

k) le recours à un marquage bien visible pour garantir qu'un élément d'information, qu'il s'agisse d'une image, d'un contenu audio ou vidéo généré ou manipulé, qui ressemble nettement à des personnes, à des objets, à des lieux ou à d'autres entités ou événements réels, et apparaît à tort aux yeux d'une personne comme authentique ou digne de foi, est reconnaissable lorsqu'il est présenté sur leurs interfaces en ligne, et, en complément, la mise à disposition d'une fonctionnalité facile d'utilisation permettant aux destinataires du service de signaler ce type d'information.

2. Le comité, en coopération avec la Commission, publie des rapports exhaustifs une fois par an. Ces rapports comprennent les éléments suivants:

a) le recensement et l'évaluation des risques systémiques les plus importants et récurrents signalés par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ou recensés via d'autres sources d'informations, notamment celles fournies conformément aux articles 39, 40 et 42;

b) la définition de bonnes pratiques pour les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne en vue de l'atténuation des risques systémiques recensés.

Ces rapports présentent les risques systémiques ventilés par État membre dans lequel ils sont survenus et pour l'ensemble de l'Union, s'il y a lieu.

3. La Commission, en coopération avec les coordinateurs pour les services numériques, peut publier des lignes directrices sur l'application du paragraphe 1 par rapport à des risques spécifiques, notamment en vue de présenter les bonnes pratiques et de recommander des mesures possibles, en tenant dûment compte des conséquences possibles des mesures sur les droits fondamentaux de toutes les parties concernées consacrés dans la Charte. Dans le cadre de l'élaboration de ces lignes directrices, la Commission organise des consultations publiques.

Article 36
Mécanisme de réaction aux crises

1. En cas de crise, la Commission, sur recommandation du comité, peut adopter une décision exigeant qu'un ou plusieurs fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche entreprennent une ou plusieurs des actions suivantes:

a) évaluer si et, le cas échéant, comment et dans quelle mesure le fonctionnement et l'utilisation de leurs services contribuent de manière significative à une menace grave, telle qu'elle est visée au paragraphe 2, ou sont susceptibles de le faire;

b) déterminer et appliquer des mesures spécifiques, efficaces et proportionnées, telles que celles prévues à l'article 35, paragraphe 1, ou à l'article 48, paragraphe 2, pour prévenir, éliminer ou limiter toute contribution à la menace grave identifiée en vertu du point a) du présent paragraphe;

c) faire rapport à la Commission, à une date donnée ou à intervalles réguliers précisés dans la décision, sur les évaluations visées au point a), le contenu précis, la mise en œuvre et l'impact qualitatif et quantitatif des mesures spécifiques prises en application du point b), ainsi que sur tout autre aspect lié à ces évaluations ou mesures, précisé dans la décision.

Lorsqu'ils déterminent et appliquent des mesures conformément au point b) du présent paragraphe, le ou les fournisseurs de services tiennent dûment compte du caractère sérieux de la menace grave visée au paragraphe 2, de l'urgence des mesures ainsi que des répercussions réelles ou potentielles pour les droits et les intérêts légitimes de toutes les parties concernées, y compris de l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés dans la Charte.

2. Aux fins du présent article, il y a lieu de conclure à une crise lorsque des circonstances extraordinaires entraînent une menace grave pour la sécurité publique ou la santé publique dans l'Union ou dans des parties importantes de l'Union.

3. Lorsqu'elle adopte la décision visée au paragraphe 1, la Commission veille à respecter l'ensemble des exigences suivantes:

a) les actions requises par la décision sont strictement nécessaires, justifiées et proportionnées, compte tenu notamment du caractère sérieux de la menace grave visée au paragraphe 2, de l'urgence des mesures ainsi que des répercussions réelles ou potentielles pour les droits et les intérêts légitimes de toutes les parties concernées, y compris de l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés dans la Charte;

b) la décision définit une période raisonnable durant laquelle les mesures spécifiques visées au paragraphe 1, point b), doivent être prises, compte tenu notamment de l'urgence de ces mesures et du temps nécessaire pour leur élaboration et leur mise en œuvre;
c) les actions requises par la décision sont limitées à une durée n'excédant pas trois mois.

4. Après l'adoption de la décision visée au paragraphe 1, la Commission entreprend sans retard injustifié les actions suivantes:
a) notifier la décision aux fournisseurs qui en sont les destinataires;

b) rendre la décision publique; et

c) informer le comité de la décision, l'inviter à faire part de son point de vue sur celle-ci et le tenir informé de toute évolution ultérieure relative à la décision.

5. Le choix des mesures spécifiques à prendre en vertu du paragraphe 1, point b), et du paragraphe 7, deuxième alinéa, relève de la responsabilité du ou des fournisseurs visés par la décision de la Commission.

6. La Commission peut, de sa propre initiative ou à la demande du fournisseur, engager un dialogue avec ce dernier afin de déterminer si, à la lumière de la situation particulière du fournisseur, les mesures prévues ou appliquées, visées au paragraphe 1, point b), sont efficaces et proportionnées pour atteindre les objectifs poursuivis. En particulier, la Commission veille à ce que les mesures prises par le fournisseur de services au titre du paragraphe 1, point b), respectent les exigences visées au paragraphe 3, points a) et c).

7. La Commission contrôle l'application des mesures spécifiques prises en vertu de la décision visée au paragraphe 1 du présent article en s'appuyant sur les rapports visés au point c) dudit paragraphe et sur toute autre information pertinente, y compris les informations qu'elle peut demander en vertu de l'article 40 ou 67, en tenant compte de l'évolution de la crise. La Commission fait régulièrement rapport au comité sur ce contrôle, au moins une fois par mois.

Lorsque la Commission estime que les mesures spécifiques prévues ou appliquées en vertu du paragraphe 1, point b), ne sont pas efficaces ou proportionnées, elle peut, après consultation du comité, adopter une décision obligeant le fournisseur à réexaminer les mesures spécifiques qui ont été déterminées ou leur application.

8. S'il y a lieu, au regard de l'évolution de la crise, la Commission peut, sur recommandation du comité, modifier la décision visée au paragraphe 1 ou au paragraphe 7, deuxième alinéa, en:

a) révoquant la décision et, s'il y a lieu, en demandant à la très grande plateforme en ligne ou au très grand moteur de recherche en ligne de cesser d'appliquer les mesures déterminées et mises en œuvre en vertu du paragraphe 1, point b), ou du paragraphe 7, deuxième alinéa, en particulier lorsque les motifs justifiant de telles mesures n'existent plus;

b) prolongeant la période visée au paragraphe 3, point c), pour une durée n'excédant pas trois mois;

c) prenant en compte l'expérience acquise dans l'application des mesures, notamment l'éventualité que les mesures ne respectent pas les droits fondamentaux consacrés par la Charte.

9. Les exigences des paragraphes 1 à 6 s'appliquent à la décision et à la modification de celle-ci visées au présent article.

10. La Commission tient le plus grand compte de la recommandation formulée par le comité en vertu du présent article.

11. Tous les ans après l'adoption de décisions conformément au présent article et, en tout état de cause, trois mois après la fin de la crise, la Commission fait rapport au Parlement européen et au Conseil sur l'application des mesures spécifiques prises en vertu desdites décisions.

Article 37
Audit indépendant

1. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne font l'objet d'audits indépendants, à leurs propres frais et au minimum une fois par an, pour évaluer le respect des points suivants:

a) les obligations établies au chapitre III;

b) tout engagement pris en vertu des codes de conduite visés aux articles 45 et 46 et des protocoles de crise visés à l'article 48.

2. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne accordent aux organisations effectuant les audits en vertu du présent article la coopération et l'assistance requises pour leur permettre de réaliser ces audits en temps utile, de manière efficace et efficiente, notamment en leur donnant accès à toutes les données et à tous les locaux pertinents et en répondant aux questions orales ou écrites qui leur sont posées. Ils s'abstiennent d'entraver, d'influencer indûment ou de compromettre la réalisation de l'audit.

Ces audits garantissent un niveau adéquat de confidentialité et de secret professionnel en ce qui concerne les informations obtenues auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne et auprès de tiers dans le cadre des audits, y compris après la clôture de ces audits. Le respect de cette exigence ne porte toutefois pas atteinte à la réalisation des audits et aux autres dispositions du présent règlement, notamment celles concernant la transparence, la surveillance et l'exécution. S'il y a lieu, aux fins des rapports de transparence visés à l'article 42, paragraphe 4, le rapport d'audit et le rapport de mise en œuvre des recommandations d'audit visés aux paragraphes 4 et 6 du présent article sont accompagnés de versions qui ne contiennent pas d'informations qui pourraient raisonnablement être considérées comme confidentielles.

3. Les audits réalisés conformément au paragraphe 1 le sont par des organisations qui:

a) sont indépendantes du fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne concerné et de toute personne morale liée à ce fournisseur et ne sont pas en situation de conflit d'intérêts avec ceux-ci; en particulier:

i) elles n'ont pas fourni de service, autre que d'audit, en rapport avec l'objet de l'audit au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ni à une personne morale liée à ce fournisseur au cours des douze mois précédant le début de l'audit, et elles se sont engagées à ne leur fournir aucun service de ce type au cours des douze mois suivant la clôture de l'audit;

ii) elles n'ont pas fourni de services d'audit en vertu du présent article au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ni à une personne morale liée à ce fournisseur pendant une période supérieure à dix années consécutives;

iii) elles ne réalisent pas l'audit en échange d'honoraires qui dépendent des résultats de cet audit;

b) possèdent une expertise avérée dans le domaine de la gestion des risques, des compétences techniques et des capacités;

c) démontrent une objectivité et une éthique professionnelle avérées, fondées notamment sur l'adhésion à des codes de pratique ou à des normes appropriées.

4. Les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne veillent à ce que les organisations qui réalisent les audits établissent un rapport d'audit à la suite de chaque audit. Ce rapport motivé est établi par écrit et comporte au moins les éléments suivants:

a) le nom, l'adresse et le point de contact du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne faisant l'objet de l'audit et la période couverte;

b) le nom et l'adresse de la ou des organisations réalisant l'audit;

c) une déclaration d'intérêt;

d) une description des éléments spécifiques faisant l'objet de l'audit, et la méthodologie appliquée;

e) une description et une synthèse des principales conclusions tirées de l'audit;

f) une liste des tiers consultés dans le cadre de l'audit;

g) un avis d'audit sur le respect ou non par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne faisant l'objet de l'audit des obligations et des engagements visés au paragraphe 1, soit "positif", soit "positif et assorti de commentaires", soit "négatif";

h) lorsque l'avis d'audit n'est pas "positif", des recommandations opérationnelles sur les mesures spécifiques à prendre pour la mise en conformité ainsi que le calendrier recommandé à cet effet.

5. Lorsque l'organisation qui réalise l'audit n'a pas été en mesure de réaliser un audit à l'égard de certains éléments spécifiques ou d'émettre un avis d'audit sur la base de ses investigations, le rapport d'audit inclut une explication sur les circonstances et les raisons pour lesquelles ces éléments n'ont pas pu faire l'objet d'un audit.

6. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne qui reçoivent un rapport d'audit qui n'est pas "positif" tiennent dûment compte des recommandations opérationnelles qui leur sont adressées en vue de prendre les mesures nécessaires à leur mise en œuvre. Dans le mois à compter de la réception de ces recommandations, ils adoptent un rapport de mise en œuvre des recommandations d'audit énonçant ces mesures. S'ils ne mettent pas en œuvre les recommandations opérationnelles, ils en fournissent les motifs dans le rapport de mise en œuvre des recommandations d'audit et exposent les mesures alternatives prises pour résoudre tout cas de manquement recensé.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 87 pour compléter le présent règlement en établissant les règles nécessaires à la réalisation des audits en vertu du présent article, notamment les règles nécessaires relatives aux étapes de la procédure, aux méthodes d'audit et aux modèles de rapport à utiliser pour les audits réalisés en vertu du présent article. Ces actes délégués tiennent compte de toute norme d'audit volontaire visée à l'article 44, paragraphe 1, point e).

cf. Actes délégués

Article 38
Systèmes de recommandation

Outre les exigences prévues à l'article 27, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne qui utilisent des systèmes de recommandation proposent au moins une option pour chacun de leurs systèmes de recommandation qui ne repose pas sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679.

cf. RGPD

Article 39
Transparence renforcée de la publicité en ligne

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne présentant de la publicité sur leurs interfaces en ligne tiennent et mettent à la disposition du public, dans une section spécifique de leur interface en ligne, à l'aide d'un outil de recherche fiable permettant d'effectuer des recherches multicritères et par l'intermédiaire d'interfaces de programme d'application, un registre contenant les informations visées au paragraphe 2, pour toute la période pendant laquelle ils présentent une publicité et jusqu'à un an après la dernière présentation de la publicité sur leurs interfaces en ligne. Ils veillent à ce que ce registre ne contienne aucune donnée à caractère personnel des destinataires du service auxquels la publicité a été ou aurait pu être présentée et s'efforcent, dans la mesure du raisonnable, de s'assurer de l'exactitude et de l'exhaustivité des informations.

2. Ce registre contient au moins toutes les informations suivantes:
a) le contenu de la publicité, y compris le nom du produit, du service ou de la marque, ainsi que l'objet de la publicité;
b) la personne physique ou morale pour le compte de laquelle la publicité est présentée;
c) la personne physique ou morale qui a payé la publicité, si cette personne est différente de celle visée au point b);
d) la période au cours de laquelle la publicité a été présentée;

e) le fait que la publicité était ou non destinée à être présentée spécifiquement à un ou plusieurs groupes particuliers de destinataires du service et, dans l'affirmative, les principaux paramètres utilisés à cette fin, y compris, s'il y a lieu, les principaux paramètres utilisés pour exclure un ou plusieurs de ces groupes particuliers;
f) les communications commerciales publiées sur les très grandes plateformes en ligne et déterminées en vertu de l'article 26, paragraphe 2;
g) le nombre total de destinataires du service atteint et, le cas échéant, les nombres totaux ventilés par État membre pour le ou les groupes de destinataires que la publicité ciblait spécifiquement.

3. En ce qui concerne le paragraphe 2, points a), b) et c), lorsque le fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne retire une publicité spécifique sur la base d'une allégation d'illégalité ou d'incompatibilité avec ses conditions générales ou rend impossible l'accès à cette publicité, le registre ne contient pas les informations visées dans lesdits points. Dans ce cas, le registre contient, pour la publicité spécifique concernée, les informations visées, selon le cas, à l'article 17, paragraphe 3, points a) à e), ou à l'article 9, paragraphe 2, point a) i).

La Commission peut, après consultation du comité, des chercheurs agréés visés à l'article 40 et du public, formuler des lignes directrices sur la structure, l'organisation et les fonctionnalités des registres visés dans le présent article.

Article 40
Accès aux données et contrôle des données

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne donnent au coordinateur pour les services numériques de l'État membre d'établissement ou à la Commission, à leur demande motivée et dans un délai raisonnable spécifié dans cette demande, l'accès aux données nécessaires pour contrôler et évaluer le respect du présent règlement.

2. Les coordinateurs pour les services numériques et la Commission n'utilisent les données auxquelles ils ont eu accès conformément au paragraphe 1 qu'à des fins de contrôle et d'évaluation du respect du présent règlement et tiennent dûment compte des droits et intérêts des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et des destinataires du service concerné, y compris la protection des données à caractère personnel, la protection des informations confidentielles, en particulier les secrets d'affaires, et le maintien de la sécurité de leur service.

3. Aux fins du paragraphe 1, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne expliquent, à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou de la Commission, la conception, la logique, le fonctionnement et la procédure de test de leurs systèmes algorithmiques, y compris leurs systèmes de recommandation.

4. Sur demande motivée du coordinateur pour les services numériques de l'État membre d'établissement, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne fournissent, dans un délai raisonnable spécifié dans la demande, l'accès aux données à des chercheurs agréés qui satisfont aux exigences énoncées au paragraphe 8 du présent article, à la seule fin de procéder à des recherches contribuant à la détection, au recensement et à la compréhension des risques systémiques dans l'Union tels qu'ils sont énoncés à l'article 34, paragraphe 1, ainsi qu'à l'évaluation du caractère adéquat, de l'efficacité et des effets des mesures d'atténuation des risques prises en vertu de l'article 35.

5. Dans les quinze jours suivant la réception d'une demande visée au paragraphe 4, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne peuvent demander au coordinateur pour les services numériques de l'État membre d'établissement de modifier la demande, lorsqu'ils considèrent ne pas être en mesure de fournir l'accès aux données demandées pour une des deux raisons suivantes:
a) ils n'ont pas accès aux données;
b) fournir l'accès aux données entraînera d'importantes vulnérabilités pour la sécurité de leur service ou la protection d'informations confidentielles, en particulier des secrets d'affaires.

6. Les demandes de modification en vertu du paragraphe 5 contiennent des propositions exposant une ou plusieurs solutions alternatives qui permettent de donner accès aux données demandées ou à d'autres données appropriées et suffisantes aux fins de la demande.

Le coordinateur pour les services numériques de l'État membre d'établissement se prononce sur la demande de modification dans les quinze jours et communique au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne sa décision et, le cas échéant, la demande modifiée et le nouveau délai pour donner suite à la demande.

7. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne facilitent et fournissent l'accès aux données conformément aux paragraphes 1 et 4 par l'intermédiaire d'interfaces appropriées spécifiées dans la demande, y compris des bases de données en ligne ou des interfaces de programmation d'application.

8. Sur demande dûment motivée de chercheurs, le coordinateur pour les services numériques de l'État membre d'établissement accorde auxdits chercheurs le statut de chercheurs agréés pour la recherche spécifique visée dans la demande et adresse une demande motivée d'accès aux données au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne conformément au paragraphe 4, lorsque les chercheurs démontrent qu'ils remplissent l'ensemble des conditions suivantes:

a) ils sont affiliés à un organisme de recherche tel qu'il est défini à l'article 2, point 1), de la directive (UE) 2019/790;

b) ils sont indépendants de tous intérêts commerciaux;

c) leur demande indique la source de financement des recherches;

d) ils sont à même de respecter les exigences spécifiques en matière de sécurité et de confidentialité des données correspondant à chaque demande ainsi que de protéger les données à caractère personnel, et ils décrivent dans leur demande les mesures techniques et organisationnelles appropriées qu'ils ont mis en place à cet effet;

e) dans leur demande, ils démontrent que leur accès aux données et les périodes d'accès demandées sont nécessaires et proportionnés aux fins poursuivies par leur recherche et que les résultats escomptés de cette recherche contribueront aux fins énoncées au paragraphe 4;

f) les activités de recherche prévues sont menées aux fins énoncées au paragraphe 4;

g) ils se sont engagés à mettre gratuitement à la disposition du public les résultats de leurs recherches dans un délai raisonnable après l'achèvement de celles-ci, sous réserve des droits et des intérêts des destinataires du service concerné, conformément au règlement (UE) 2016/679.

cf. RGPD

Dès réception de la demande visée au présent paragraphe, le coordinateur pour les services numériques de l'État membre d'établissement informe la Commission et le comité.

9. Les chercheurs peuvent également soumettre leur demande au coordinateur pour les services numériques de l'État membre de l'organisme de recherche auquel ils sont affiliés. Dès réception de la demande visée au présent paragraphe, le coordinateur pour les services numériques procède à une évaluation initiale visant à déterminer si les différents chercheurs remplissent toutes les conditions énoncées au paragraphe 8. Le coordinateur pour les services numériques concerné envoie la demande, accompagnée des documents justificatifs présentés par les chercheurs ainsi que de l'évaluation initiale, au coordinateur pour les services numériques de l'État membre d'établissement. Le coordinateur pour les services numériques de l'État membre d'établissement adopte dans les meilleurs délais, une décision quant à l'octroi à un chercheur du statut de chercheur agréé.

Tout en tenant dûment compte de l'évaluation initiale fournie, la décision finale d'octroyer à un chercheur le statut de chercheur agréé relève de la compétence du coordinateur pour les services numériques de l'État membre d'établissement, conformément au paragraphe 8.

10. Le coordinateur pour les services numériques ayant octroyé le statut de chercheur agréé et adressé la demande motivée d'accès aux données aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne en faveur d'un chercheur agréé, adopte une décision mettant fin à cet accès s'il constate, à la suite d'une enquête menée soit de sa propre initiative, soit sur la base d'informations reçues de tiers, que le chercheur agréé ne remplit plus les conditions établies au paragraphe 8, et informe le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné de sa décision. Avant de mettre fin à l'accès, le coordinateur pour les services numériques donne au chercheur agréé la possibilité de réagir aux conclusions de l'enquête et à son intention de mettre fin à l'accès.

11. Les coordinateurs pour les services numériques de l'État membre d'établissement communiquent au comité les noms et les coordonnées des personnes physiques ou des entités auxquelles ils ont accordé le statut de chercheur agréé conformément au paragraphe 8, ainsi que l'objet de la recherche pour laquelle la demande a été soumise, ou l'informent qu'ils ont mis fin à l'accès aux données conformément au paragraphe 10 si c'est le cas.

12. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne donnent accès, sans retard injustifié, aux données, y compris, lorsque cela est techniquement possible, aux données en temps réel, à condition que ces données soient publiquement accessibles sur leur interface en ligne aux chercheurs, y compris ceux qui sont affiliés à des organismes et des associations à but non lucratif, qui remplissent les conditions énoncées au paragraphe 8, points b), c), d) et e), et qui utilisent les données uniquement à des fins de recherches contribuant à la détection, à la détermination et à la compréhension des risques systémiques dans l'Union en vertu de l'article 34, paragraphe 1.

13. Après consultation du comité, la Commission adopte des actes délégués qui complètent le présent règlement en établissant les conditions techniques dans lesquelles les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne partagent des données en vertu des paragraphes 1 et 4 et les fins auxquelles ces données peuvent être utilisées. Ces actes délégués établissent les conditions spécifiques dans lesquelles un tel partage de données avec des chercheurs peut avoir lieu en conformité avec le règlement (UE) 2016/679, ainsi que les indicateurs objectifs pertinents, les procédures et, si nécessaire, les mécanismes consultatifs indépendants à l'appui du partage de données, en tenant compte des droits et des intérêts des fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne et des destinataires du service concernés, y compris la protection des informations confidentielles, notamment les secrets d'affaires, et en préservant la sécurité de leur service.

cf. Actes délégués

cf. RGPD

Article 41
Fonction de contrôle de la conformité

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne créent une fonction de contrôle de la conformité, qui est indépendante de leurs fonctions opérationnelles et composée d'un ou de plusieurs responsables de la conformité, y compris le responsable de la fonction de contrôle de la conformité. La fonction de contrôle de la conformité dispose d'une autorité, d'une taille et de ressources suffisantes, ainsi que de l'accès à l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne nécessaire pour contrôler le respect du présent règlement par ce fournisseur.

2. L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne veille à ce que les responsables de la conformité disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe 3.

L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne veille à ce que le responsable de la fonction de

contrôle de la conformité soit un cadre supérieur indépendant chargé spécifiquement de la fonction de contrôle de la conformité.

Le responsable de la fonction de contrôle de la conformité fait directement rapport à l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne et peut faire part de ses préoccupations auprès de cet organe et l'avertir lorsque les risques visés à l'article 34 ou le non-respect du présent règlement affectent ou sont susceptibles d'affecter le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, sans préjudice des responsabilités de l'organe de direction dans ses fonctions de surveillance et de gestion.

Le responsable de la fonction de contrôle de la conformité n'est pas démis de ses fonctions sans l'accord préalable de l'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne.

3. Les responsables de la conformité sont investis des tâches suivantes:

a) coopérer avec le coordinateur pour les services numériques de l'État membre d'établissement et la Commission aux fins du présent règlement;

b) veiller à ce que tous les risques visés à l'article 34 soient recensés et dûment notifiés et à ce que des mesures d'atténuation des risques raisonnables, proportionnées et efficaces soient prises conformément à l'article 35;

c) organiser et superviser les activités du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en lien avec l'audit indépendant en vertu de l'article 37;

d) informer et conseiller la direction et les employés du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne au sujet des obligations pertinentes au titre du présent règlement;

e) contrôler le respect, par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, de ses obligations au titre du présent règlement;

f) le cas échéant, contrôler le respect, par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, des engagements qu'il a pris au titre des codes de conduite en vertu des articles 45 et 46 ou des protocoles de crise en vertu de l'article 48.

4. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne communiquent le nom et les coordonnées du responsable de la fonction de contrôle de la conformité au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission.

5. L'organe de direction du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne détermine et supervise la mise en œuvre des dispositifs de gouvernance du fournisseur qui garantissent l'indépendance de la fonction de contrôle de la conformité, y compris la répartition des responsabilités au sein de l'organisation du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, la prévention des conflits d'intérêts et la bonne gestion des risques systémiques recensés conformément à l'article 34, et est tenu de rendre compte de cette mise en œuvre.

6. L'organe de direction approuve et réexamine périodiquement, au moins une fois par an, les stratégies et les politiques relatives à la prise en compte, à la gestion, au suivi et à l'atténuation des risques recensés conformément à l'article 34 auxquels la très grande plateforme en ligne ou le très grand moteur de recherche en ligne est ou pourrait être exposé.

7. L'organe de direction consacre suffisamment de temps à l'examen des mesures liées à la gestion des risques. Il participe activement aux décisions relatives à la gestion des risques et veille à ce que des ressources adéquates soient allouées à la gestion des risques recensés conformément à l'article 34.

Article 42
Obligations en matière de rapports de transparence

1. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne publient les rapports visés à l'article 15 au plus tard deux mois à compter de la date d'application visée à l'article 33, paragraphe 6, deuxième alinéa, puis au moins tous les six mois.

2. Outre les informations visées à l'article 15 et à l'article 24, paragraphe 1, les rapports visés au paragraphe 1 du présent article, publiés par les fournisseurs de très grandes plateformes en ligne, précisent:

a) les ressources humaines que le fournisseur de très grandes plateformes en ligne consacre à la modération des contenus en ce qui concerne le service proposé dans l'Union, ventilées par langue officielle concernée des États membres, y compris pour le respect des obligations énoncées aux articles 16 et 22 et de celles énoncées à l'article 20;

b) les qualifications et les connaissances linguistiques des personnes accomplissant les activités visées au point a) ainsi que la formation et l'accompagnement qui leur sont apportés;

c) les indicateurs de précision et les informations y afférentes visés à l'article 15, paragraphe 1, point e), ventilés par langue officielle des États membres.

Les rapports sont publiés dans au moins une des langues officielles des États membres.

3. En plus des informations visées à l'article 24, paragraphe 2, les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne incluent, dans les rapports visés au paragraphe 1 du présent article, des informations sur le nombre mensuel moyen de destinataires du service dans chaque État membre.

4. Les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne transmettent au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, sans retard injustifié dès leur achèvement, et mettent à la disposition du public au plus tard trois mois après la réception de chaque rapport d'audit conformément à l'article 37, paragraphe 4:
a) un rapport exposant les résultats de l'évaluation des risques au titre de l'article 34;
b) les mesures spécifiques d'atténuation mises en place en vertu de l'article 35, paragraphe 1;
c) le rapport d'audit prévu à l'article 37, paragraphe 4;
d) le rapport de mise en œuvre des recommandations d'audit prévu à l'article 37, paragraphe 6;
e) s'il y a lieu, les informations relatives aux consultations menées par le fournisseur pour les besoins des évaluations des risques et de la conception des mesures d'atténuation des risques.

5. Lorsqu'un fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne considère que la publication d'informations conformément au paragraphe 4 pourrait mener à la divulgation d'informations confidentielles de ce fournisseur ou des destinataires du service, entraîner d'importantes vulnérabilités pour la sécurité de son service, porter atteinte à la sécurité publique ou nuire aux destinataires, il peut retirer ces informations des rapports accessibles au public. Dans ce cas, le fournisseur transmet les rapports complets au coordinateur pour les services numériques de l'État membre d'établissement et à la Commission, accompagnés d'un exposé des motifs pour lesquels ces informations ont été retirées des rapports accessibles au public.

Article 43
Redevance de surveillance

1. La Commission perçoit auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne une redevance de surveillance annuelle au moment de leur désignation en vertu de l'article 33.

2. Le montant total de la redevance de surveillance annuelle couvre les frais estimés que doit engager la Commission pour mener à bien les missions de surveillance que lui confie le présent règlement, en particulier les frais afférents aux désignations prévues à l'article 33, à la création, à la maintenance et au fonctionnement de la base de données visée à l'article 24, paragraphe 5, et au système de partage d'informations visé à l'article 85, aux saisines visées à l'article 59, à l'appui apporté au comité conformément à l'article 62 et aux missions de surveillance visées à l'article 56 et au chapitre IV, section 4.

3. Une redevance de surveillance est perçue chaque année auprès des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne pour chaque service pour lequel ils ont été désignés en vertu de l'article 33.

La Commission adopte des actes d'exécution fixant le montant de la redevance de surveillance annuelle pour chaque fournisseur de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne. Lorsqu'elle adopte ces actes d'exécution, la Commission applique la méthode établie dans l'acte délégué visé au paragraphe 4 du présent article et respecte les principes énoncés au paragraphe 5 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure de consultation visée à l'article 88.

4. La Commission adoptes des actes délégués conformément à l'article 87 fixant, dans le détail, la méthode et les procédures à employer pour:
a) la détermination des frais estimés visés au paragraphe 2;
b) la détermination des redevances de surveillance annuelles individuelles visées au paragraphe 5, points b) et c);
c) la détermination du plafond global défini au paragraphe 5, point c); et
d) les modalités nécessaires pour effectuer les paiements.

Lorsqu'elle adopte ces actes délégués, la Commission respecte les principes énoncés au paragraphe 5 du présent article.

cf. Actes délégués

5. L'acte d'exécution visé au paragraphe 3 et l'acte délégué visé au paragraphe 4 respectent les principes suivants:
a) l'estimation du montant total de la redevance de surveillance annuelle tient compte des frais engagés lors de l'exercice précédent;
b) la redevance de surveillance annuelle est proportionnelle au nombre mensuel moyen de destinataires actifs dans l'Union de chaque très grande plateforme en ligne ou de chaque très grand moteur de recherche en ligne désigné en vertu de l'article 33;
c) le montant total de la redevance de surveillance annuelle perçue auprès d'un fournisseur donné de très grandes plateformes en ligne ou de très grands moteurs de recherche ne dépasse en aucun cas 0,05 % de son résultat net mondial annuel de l'exercice précédent.

6. Les redevances de surveillance annuelles individuelles perçues conformément au paragraphe 1 du présent article constituent des recettes affectées externes conformément à l'article 21, paragraphe 5, du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil[41].

7. La Commission présente chaque année au Parlement européen et au Conseil un rapport sur le montant total des frais engagés pour l'accomplissement des missions qui lui incombent au titre du présent règlement et sur le montant total des redevances de surveillance annuelles individuelles perçues lors de l'exercice précédent.

41. Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) n° 1296/2013, (UE) n° 1301/2013, (UE) n° 1303/2013, (UE) n° 1304/2013, (UE) n° 1309/2013, (UE) n° 1316/2013, (UE) n° 223/2014, (UE) n° 283/2014 et la décision n° 541/2014/UE, et abrogeant le règlement (UE, Euratom) n° 966/2012 (JO L 193 du 30.7.2018, p. 1).

SECTION 6
Autres dispositions concernant les obligations de diligence

Article 44
Normes

1. La Commission consulte le comité et soutient et encourage le développement ainsi que la mise en œuvre de normes volontaires établies par les organismes de normalisation européens et internationaux pertinents, au minimum pour les aspects suivants:
a) la soumission électronique des notifications au titre de l'article 16;
b) les modèles et les normes de conception et de procédure à employer pour communiquer avec les destinataires du service de manière conviviale sur les restrictions résultant des conditions générales et les modifications qui leur sont apportées;
c) la soumission électronique des notifications par les signaleurs de confiance au titre de l'article 22, y compris par l'intermédiaire d'interfaces de programme d'application;
d) les interfaces spécifiques, y compris les interfaces de programme d'application, visant à faciliter le respect des obligations établies aux articles 39 et 40;
e) l'audit des très grandes plateformes en ligne et des très grands moteurs de recherche en ligne au titre de l'article 37;
f) l'interopérabilité des registres de publicités visés à l'article 39, paragraphe 2;
g) la transmission de données entre les intermédiaires de publicité aux fins des obligations de transparence en vertu de l'article 26, paragraphe 1, points b), c) et d);
h) les mesures techniques permettant de satisfaire aux obligations relatives à la publicité contenues dans le présent règlement, y compris les obligations relatives aux marquages bien visibles à employer pour les publicités et les communications commerciales visées à l'article 26;
i) les interfaces de choix et la présentation des informations sur les principaux paramètres des différents types de systèmes de recommandation, conformément aux articles 27 et 38;
j) les normes applicables aux mesures ciblées destinées à protéger les mineurs en ligne.

2. La Commission soutient la mise à jour des normes à la lumière des évolutions technologiques et du comportement des destinataires des services en question. Les informations pertinentes concernant la mise à jour des normes sont mises à la disposition du public et facilement accessibles.

Article 45
Codes de conduite

1. La Commission et le comité encouragent et facilitent l'élaboration de codes de conduite volontaires au niveau de l'Union pour contribuer à la bonne application du présent règlement, en tenant compte notamment des difficultés spécifiques à surmonter pour faire face à différents types de contenus illicites et de risques systémiques, conformément au droit de l'Union notamment en matière de concurrence et de protection des données à caractère personnel.

2. Lorsqu'un risque systémique important au sens de l'article 34, paragraphe 1, apparaît et concerne plusieurs très grandes plateformes en ligne ou très grands moteurs de recherche en ligne, la Commission peut inviter les fournisseurs des très grandes plateformes en ligne concernées ou les fournisseurs des très grands moteurs de recherche en ligne concernés, et d'autres fournisseurs de très grandes plateformes en ligne, de très grands moteurs de recherche en ligne, de plateformes en ligne et d'autres services intermédiaires, selon qu'il convient, ainsi que les autorités compétentes concernées, des organisations de la société civile et d'autres parties prenantes concernées, à participer à l'élaboration de codes de conduite, y compris en formulant des engagements portant sur l'adoption de mesures spécifiques d'atténuation des risques, ainsi que d'un cadre pour la présentation de rapports réguliers concernant les mesures adoptées et leurs résultats.

3. En donnant effet aux paragraphes 1 et 2, la Commission et le comité, ainsi que d'autres organes s'il y a lieu, s'efforcent de garantir que les codes de conduite établissent clairement leurs objectifs spécifiques, contiennent des indicateurs clés de performance pour mesurer la réalisation de ces objectifs et tiennent dûment compte des

besoins et des intérêts de toutes les parties intéressées, et en particulier des citoyens, au niveau de l'Union. La Commission et le comité s'efforcent également de garantir que les participants communiquent régulièrement à la Commission et à leurs coordinateurs pour les services numériques de l'État membre d'établissement respectifs les mesures qu'ils adoptent et leurs résultats, mesurés par rapport aux indicateurs clés de performance que les codes de conduite contiennent. Les indicateurs de performance clés et les engagements en matière de présentation de rapports tiennent compte des différences de taille et de capacité entre les différents participants.

4. La Commission et le comité évaluent si les codes de conduite satisfont aux objectifs spécifiés aux paragraphes 1 et 3, et contrôlent et évaluent régulièrement la réalisation de leurs objectifs, en tenant compte des indicateurs clés de performance qu'ils pourraient contenir. Ils publient leurs conclusions.

La Commission et le comité encouragent et facilitent également le réexamen régulier et l'adaptation des codes de conduite.

En cas de non-respect systématique des codes de conduite, la Commission et le comité peuvent inviter les signataires desdits codes à prendre les mesures qui s'imposent.

Article 46
Codes de conduite pour la publicité en ligne

1. La Commission encourage et facilite l'élaboration de codes de conduite volontaires au niveau de l'Union par les fournisseurs de plateformes en ligne et d'autres fournisseurs de services pertinents, tels que les fournisseurs de services intermédiaires de publicité en ligne, d'autres acteurs participant à la chaîne de valeur de la publicité programmatique, ou les organisations représentant les destinataires du service et les organisations de la société civile ou les autorités compétentes, en vue de contribuer à une transparence accrue pour les acteurs de la chaîne de valeur de la publicité en ligne, au-delà des exigences des articles 26 et 39.

2. La Commission s'efforce de garantir que les codes de conduite favorisent la transmission efficace des informations, dans le plein respect des droits et intérêts de toutes les parties concernées, ainsi qu'un environnement compétitif, transparent et équitable pour la publicité en ligne, conformément au droit de l'Union et au droit national, notamment en matière de concurrence et de protection de la vie privée et des données à caractère personnel. La Commission s'efforce de garantir que les codes de conduite portent au minimum sur:

a) la transmission des informations détenues par les fournisseurs de services intermédiaires de publicité en ligne aux destinataires du service en ce qui concerne les exigences établies à l'article 26, paragraphe 1, points b), c) et d);

b) la transmission des informations détenues par les fournisseurs de services intermédiaires de publicité en ligne aux registres en vertu de l'article 39;
c) des informations utiles sur la monétisation des données.

3. La Commission encourage l'élaboration des codes de conduite pour le 18 février 2025 et leur application pour le 18 août 2025.

4. La Commission encourage tous les acteurs de la chaîne de valeur de la publicité en ligne visés au paragraphe 1 à adhérer aux engagements formulés dans les codes de conduite et à les respecter.

Article 47
Codes de conduite relatifs à l'accessibilité

1. La Commission encourage et facilite l'élaboration de codes de conduite au niveau de l'Union, avec la participation des fournisseurs de plateformes en ligne et d'autres fournisseurs de services pertinents, les organisations représentant les destinataires du service et les organisations de la société civile ou les autorités compétentes afin de promouvoir la participation pleine et effective des personnes handicapées, sur un pied d'égalité, en améliorant leur accès aux services en ligne qui, du fait de leur conception

initiale ou de leur adaptation ultérieure, répondent aux besoins spécifiques des personnes handicapées.

2. La Commission s'efforce de garantir que les codes de conduite poursuivent l'objectif d'assurer l'accessibilité de ces services, conformément au droit de l'Union et au droit national, afin de garantir une utilisation prévisible optimale par les personnes handicapées de ces services. La Commission s'efforce de garantir que les codes de conduite visent à atteindre au moins les objectifs suivants:

a) concevoir et adapter les services pour qu'ils soient accessibles aux personnes handicapées en les rendant perceptibles, utilisables, compréhensibles et robustes;

b) expliquer comment les services répondent aux exigences d'accessibilité applicables et mettre ces informations à la disposition du public d'une manière accessible aux personnes handicapées;

c) mettre les informations, les formulaires et les mesures fournis en vertu du présent règlement à disposition de manière à ce qu'ils soient faciles à trouver, faciles à comprendre et accessibles aux personnes handicapées.

3. La Commission encourage l'élaboration des codes de conduite au plus tard le 18 février 2025 et leur application au plus tard le 18 août 2025.

Article 48
Protocoles de crise

1. Le comité peut recommander à la Commission de lancer l'élaboration, conformément aux paragraphes 2, 3 et 4, de protocoles de crise volontaires pour faire face aux situations de crise. Ces situations sont strictement limitées à des circonstances extraordinaires affectant la sécurité publique ou la santé publique.

2. La Commission encourage et facilite la participation des fournisseurs de très grandes plateformes en ligne, de très grands moteurs de recherche en ligne et, le cas échéant, les fournisseurs d'autres plateformes en ligne ou d'autres moteurs de recherche en ligne, à l'élaboration, aux essais et à l'application de ces protocoles de crise. La Commission s'efforce de garantir que ces protocoles de crise comprennent une ou plusieurs des mesures suivantes:

a) afficher de manière bien visible les informations relatives à la situation de crise fournies par les autorités des États membres ou au niveau de l'Union ou, en fonction du contexte de la crise, par d'autres organes fiables concernés;

b) veiller à ce que le fournisseur de services intermédiaires désigne un point de contact spécifique pour la gestion des crises; le cas échéant, il peut s'agir du point de contact électronique visé à l'article 11 ou, dans le cas de fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, du responsable de la conformité visé à l'article 41;

c) le cas échéant, adapter les ressources dédiées au respect des obligations établies aux articles 16, 20, 22, 23 et 35 aux besoins découlant de la situation de crise.

3. La Commission associe, selon qu'il convient, les autorités des États membres et peut également associer les organes et organismes de l'Union à l'élaboration, aux essais et à la supervision de l'application des protocoles de crise. La Commission peut également, si nécessaire et selon qu'il convient, associer des organisations de la société civile ou d'autres organisations pertinentes à l'élaboration des protocoles de crise.

4. La Commission s'efforce de garantir que les protocoles de crise établissent clairement l'ensemble des éléments suivants:

a) les paramètres spécifiques utilisés pour déterminer ce qui constitue la circonstance extraordinaire spécifique à laquelle le protocole de crise entend répondre, ainsi que les objectifs qu'il poursuit;

b) le rôle de chacun des participants et les mesures qu'ils doivent mettre en place à titre préparatoire et en cas d'activation du protocole de crise;

c) une procédure claire pour déterminer le moment auquel le protocole de crise doit être activé;

d) une procédure claire pour déterminer la période au cours de laquelle les mesures à prendre en cas d'activation du protocole de crise doivent être prises, qui est strictement limitée à ce qui est nécessaire pour faire face aux circonstances extraordinaires spécifiques concernées;

e) les mesures de sauvegarde contre les effets négatifs éventuels sur l'exercice des droits fondamentaux consacrés dans la Charte, en particulier la liberté d'expression et d'information et le droit à la non-discrimination;

f) une procédure pour communiquer publiquement sur les mesures adoptées, leur durée et leurs résultats lorsque la situation de crise a pris fin.

5. Si la Commission considère qu'un protocole de crise ne répond pas de manière efficace à une situation de crise, ou ne sauvegarde pas l'exercice des droits fondamentaux comme prévu au paragraphe 4, point e), elle demande aux participants de réviser le protocole de crise, notamment en prenant des mesures complémentaires.

CHAPITRE IV
MISE EN ŒUVRE, COOPÉRATION, SANCTIONS ET EXÉCUTION

SECTION 1
Autorités compétentes et coordinateurs nationaux pour les services numériques

Article 49
Autorités compétentes et coordinateurs pour les services numériques

1. Les États membres désignent une ou plusieurs autorités compétentes comme responsables de la surveillance des fournisseurs de services intermédiaires et de l'exécution du présent règlement (ci-après dénommées les "autorités compétentes").

2. Les États membres désignent une des autorités compétentes comme leur coordinateur pour les services numériques. Le coordinateur pour les services numériques est responsable de toutes les questions en lien avec la surveillance et l'exécution du présent règlement dans cet État membre, sauf si l'État membre concerné a assigné certaines missions ou certains secteurs spécifiques à d'autres autorités compétentes. Le coordinateur pour les services numériques a, en tout état de cause, la responsabilité d'assurer la coordination au niveau national vis-à-vis de ces questions et de contribuer à une surveillance et une exécution efficaces et cohérentes du présent règlement dans toute l'Union.

À cette fin, les coordinateurs pour les services numériques coopèrent entre eux, ainsi qu'avec les autres autorités compétentes nationales, le comité et la Commission, sans préjudice de la possibilité dont disposent les États membres de prévoir des mécanismes de coopération et des échanges de vues réguliers entre les coordinateurs pour les services numériques et d'autres autorités nationales, lorsque cela présente de l'intérêt pour l'exécution de leurs missions respectives.

Lorsqu'un État membre désigne une ou plusieurs autorités compétentes en plus du coordinateur pour les services numériques, il veille à ce que les missions respectives de ces autorités et du coordinateur pour les services numériques soient clairement définies et à ce qu'ils coopèrent de manière étroite et efficace dans l'exécution de leurs missions.

3. Les États membres désignent les coordinateurs pour les services numériques au plus tard le 17 février 2024.

Les États membres rendent publics et communiquent à la Commission et au comité le nom de leur autorité compétente désignée en tant que coordinateur pour les services numériques, ainsi que des informations sur la manière dont il peut être contacté. L'État membre concerné communique à la Commission et au comité le nom des autres autorités compétentes visées au paragraphe 2 ainsi que leurs missions respectives.

4. Les dispositions applicables aux coordinateurs pour les services numériques énoncées aux articles 50, 51 et 56 s'appliquent également aux autres autorités compétentes désignées par les États membres en vertu du paragraphe 1 du présent article.

Article 50
Exigences applicables aux coordinateurs pour les services numériques

1. Les États membres veillent à ce que les coordinateurs pour les services numériques accomplissent leurs missions au titre du présent règlement de manière impartiale, transparente et en temps utile. Les États membres veillent à ce que leurs coordinateurs pour les services numériques disposent de toutes les ressources nécessaires à l'accomplissement de leurs missions, y compris des ressources techniques, financières et humaines suffisantes pour surveiller correctement tous les fournisseurs de services intermédiaires relevant de leur compétence. Chaque État membre veille à ce que son coordinateur pour les services numériques dispose d'une autonomie suffisante dans la gestion de son budget dans les limites globales du budget, afin de ne pas porter atteinte à l'indépendance du coordinateur pour les services numériques.

2. Lorsqu'ils accomplissent leurs missions et exercent leurs pouvoirs conformément au présent règlement, les coordinateurs pour les services numériques agissent en toute indépendance. Ils restent libres de toute influence extérieure, directe ou indirecte, et ne sollicitent ni n'acceptent aucune instruction d'aucune autre autorité publique ou partie privée.

3. Le paragraphe 2 du présent article est sans préjudice des missions incombant aux coordinateurs pour les services numériques dans le cadre du système de surveillance et d'exécution prévu dans le présent règlement et de la coopération avec les autres autorités compétentes conformément à l'article 49, paragraphe 2. Le paragraphe 2 du présent article n'empêche pas l'exercice d'un contrôle juridictionnel et est également sans préjudice d'exigences proportionnées en matière de responsabilisation en ce qui concerne les activités générales des coordinateurs pour les services numériques, par exemple en ce qui concerne les dépenses financières ou les rapports à communiquer aux parlements nationaux, à condition que ces exigences ne portent pas atteinte à la réalisation des objectifs du présent règlement.

Article 51
Pouvoirs des coordinateurs pour les services numériques

1. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont investis des pouvoirs d'enquête suivants à l'égard de la conduite des fournisseurs de services intermédiaires relevant de la compétence de leur État membre:

a) le pouvoir d'exiger de ces fournisseurs, ainsi que de toute autre personne agissant pour les besoins de son activité commerciale, industrielle, artisanale ou libérale et raisonnablement susceptible d'être au courant d'informations relatives à une infraction présumée au présent règlement, y compris les organisations qui réalisent les audits visés à l'article 37 et à l'article 75, paragraphe 2, qu'ils fournissent ces informations dans les meilleurs délais;

b) le pouvoir de procéder à des inspections dans tout local utilisé par ces fournisseurs ou ces personnes pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale, ou de demander à une autorité judiciaire de leur État membre d'ordonner une telle inspection, ou de demander à d'autres autorités publiques de procéder à une telle inspection, afin d'examiner, de saisir, de prendre ou d'obtenir des copies d'informations relatives à une infraction présumée sous quelque forme et sur quelque support de stockage que ce soit;

c) le pouvoir de demander à tout membre du personnel ou représentant de ces fournisseurs ou de ces personnes de fournir des explications sur toute information relative

à une infraction présumée et d'enregistrer leurs réponses avec leur consentement à l'aide de tout moyen technique.

2. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont investis des pouvoirs d'exécution suivants à l'égard des fournisseurs de services intermédiaires relevant de la compétence de leur État membre:

a) le pouvoir d'accepter les engagements proposés par ces fournisseurs pour se conformer au présent règlement et de rendre ces engagements contraignants;

b) le pouvoir d'ordonner la cessation des infractions et, le cas échéant, d'imposer des mesures correctives proportionnées à l'infraction et nécessaires pour faire cesser effectivement l'infraction, ou de demander à une autorité judiciaire de leur État membre d'y procéder;

c) le pouvoir d'imposer des amendes, ou de demander à une autorité judiciaire de leur État membre d'y procéder, conformément à l'article 52 pour non-respect du présent règlement, y compris de toute injonction d'enquête émise en vertu du paragraphe 1 du présent article;

d) le pouvoir d'imposer une astreinte, ou de demander à une autorité judiciaire de leur État membre d'y procéder, conformément à l'article 52 pour qu'il soit mis fin à une infraction conformément à une injonction émise en vertu du point b) du présent alinéa ou pour non-respect de toute injonction d'enquête émise en vertu du paragraphe 1 du présent article;

e) le pouvoir d'adopter des mesures provisoires ou de demander à l'autorité judiciaire nationale compétente de leur État membre d'y procéder afin d'éviter le risque de préjudice grave.

En ce qui concerne le premier alinéa, points c) et d), les coordinateurs pour les services numériques disposent également des pouvoirs d'exécution prévus dans ces points à l'égard des autres personnes visées au paragraphe 1 pour non-respect de toute injonction qui leur est adressée en vertu dudit paragraphe. Ils n'exercent ces pouvoirs d'exécution qu'après avoir fourni à ces autres personnes, en temps utile, toutes les informations pertinentes en lien avec ces injonctions, y compris le délai applicable, les amendes ou astreintes susceptibles d'être imposées en cas de non-respect et les possibilités de recours.

3. Lorsque cela est nécessaire à l'accomplissement de leurs missions au titre du présent règlement, les coordinateurs pour les services numériques sont également investis, à l'égard des fournisseurs de services intermédiaires relevant de la compétence de leur État membre, lorsque tous les autres pouvoirs prévus par le présent article pour parvenir à la cessation d'une infraction ont été épuisés, qu'il n'a pas été remédié à l'infraction ou que l'infraction se poursuit et qu'elle entraîne un préjudice grave ne pouvant pas être évité par l'exercice d'autres pouvoirs prévus par le droit de l'Union ou le droit national, du pouvoir de prendre les mesures suivantes:

a) exiger de l'organe de direction de ces fournisseurs, dans les meilleurs délais, qu'il examine la situation, adopte et soumette un plan d'action établissant les mesures nécessaires pour mettre fin à l'infraction, veille à ce que le fournisseur prenne ces mesures et fasse rapport sur les mesures prises;

b) lorsque le coordinateur pour les services numériques considère qu'un fournisseur de services intermédiaires n'a pas suffisamment respecté les exigences visées au point a), qu'il n'a pas été remédié à l'infraction ou que l'infraction se poursuit et qu'elle entraîne un préjudice grave, et que cette infraction constitue une infraction pénale impliquant une menace pour la vie ou la sécurité des personnes, demander à l'autorité judiciaire compétente de son État membre d'ordonner une restriction temporaire de l'accès des destinataires au service concerné par l'infraction ou, uniquement lorsque cela n'est pas techniquement réalisable, à l'interface en ligne du fournisseur de services intermédiaires sur laquelle se produit l'infraction.

Sauf lorsqu'il agit à la demande de la Commission au titre de l'article 82, préalablement à l'envoi de la demande visée au premier alinéa, point b), du présent paragraphe,

le coordinateur pour les services numériques invite les parties intéressées à soumettre des observations écrites dans un délai de minimum deux semaines, en décrivant les mesures qu'il entend demander et en identifiant le ou les destinataires prévus. Le fournisseur de services intermédiaires, le ou les destinataires prévus et tout autre tiers démontrant un intérêt légitime ont le droit de participer à la procédure devant l'autorité judiciaire compétente. Toute mesure ordonnée est proportionnée à la nature, à la gravité, à la répétition et à la durée de l'infraction, et ne restreint pas indûment l'accès des destinataires du service concerné aux informations légales.

La restriction d'accès s'applique pour une durée de quatre semaines, sous réserve de la possibilité dont dispose l'autorité judiciaire compétente, dans son injonction, de permettre au coordinateur pour les services numériques de prolonger ce délai à raison de nouvelles périodes de même durée, le nombre maximal de prolongations étant fixé par cette autorité judiciaire. Le coordinateur pour les services numériques ne prolonge le délai que s'il considère, compte tenu des droits et des intérêts de toutes les parties affectées par cette limitation et de l'ensemble des circonstances pertinentes, y compris de toute information que le fournisseur de services intermédiaires, le ou les destinataires et tout autre tiers ayant démontré un intérêt légitime pourraient lui fournir, que les deux conditions suivantes sont remplies:

a) le fournisseur de services intermédiaires n'a pas pris les mesures nécessaires pour mettre fin à l'infraction;

b) la restriction temporaire ne restreint pas indûment l'accès des destinataires du service aux informations légales, compte tenu du nombre de destinataires affectés et de l'existence éventuelle de toute alternative appropriée et facilement accessible.

Lorsque le coordinateur pour les services numériques considère que les conditions énoncées au troisième alinéa, points a) et b), sont remplies, mais qu'il ne peut pas prolonger davantage la période visée au troisième alinéa, il soumet une nouvelle demande à l'autorité judiciaire compétente, conformément au premier alinéa, point b).

4. Les pouvoirs énumérés aux paragraphes 1, 2 et 3 sont sans préjudice de la section 3.

5. Les mesures prises par les coordinateurs pour les services numériques dans l'exercice de leurs pouvoirs énumérés aux paragraphes 1, 2 et 3 sont efficaces, proportionnées et dissuasives, compte tenu notamment de la nature, de la gravité, de la répétition et de la durée de l'infraction ou de l'infraction présumée à laquelle ces mesures se rapportent, ainsi que de la capacité économique, technique et opérationnelle du fournisseur de services intermédiaires concerné, le cas échéant.

6. Les États membres fixent des conditions et des procédures spécifiques pour l'exercice des pouvoirs visés aux paragraphes 1, 2 et 3 et veillent à ce que tout exercice de ces pouvoirs soit soumis à des mesures de sauvegarde appropriées établies dans le droit national applicable en conformité avec la Charte et les principes généraux du droit de l'Union. Plus particulièrement, ces mesures ne sont prises qu'en conformité avec le droit au respect de la vie privée et les droits de la défense, y compris les droits d'être entendu et d'avoir accès au dossier, et le droit à un recours juridictionnel effectif pour toutes les parties affectées.

Article 52
Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux infractions au présent règlement par les fournisseurs de services intermédiaires relevant de leur compétence et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions conformément à l'article 51.

2. Les sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Les États membres veillent à ce que le montant maximal des amendes qui peuvent être imposées pour non-respect d'une obligation établie dans le présent règlement

représente 6 % du chiffre d'affaires mondial annuel du fournisseur de services intermédiaires concerné réalisé au cours de l'exercice précédent. Les États membres veillent à ce que le montant maximal de l'amende qui peut être imposée pour la fourniture d'informations inexactes, incomplètes ou trompeuses, l'absence de réponse ou la non-rectification d'informations inexactes, incomplètes ou trompeuses et le manquement à l'obligation de se soumettre à une inspection représente 1 % des revenus ou du chiffre d'affaires mondial annuels du fournisseur de services intermédiaires concerné ou de la personne concernée de l'exercice précédent.

4. Les États membres veillent à ce que le montant maximal d'une astreinte représente 5 % des revenus ou du chiffre d'affaires mondial journaliers moyens du fournisseur de services intermédiaires concerné de l'exercice précédent, par jour, calculé à compter de la date spécifiée dans la décision concernée.

Article 53
Droit d'introduire une plainte

Les destinataires du service, ainsi que tout organisme, organisation ou association ayant reçu mandat pour exercer les droits conférés par le présent règlement pour leur compte, ont le droit d'introduire une plainte à l'encontre de fournisseurs de services intermédiaires en invoquant une infraction au présent règlement auprès du coordinateur pour les services numériques de l'État membre dans lequel le destinataire du service est situé ou est établi. Le coordinateur pour les services numériques évalue la plainte et, le cas échéant, la transmet au coordinateur pour les services numériques de l'État membre d'établissement, accompagnée d'un avis lorsqu'il le juge approprié. Lorsque la plainte relève de la responsabilité d'une autre autorité compétente au sein de son État membre, le coordinateur pour les services numériques qui reçoit la plainte la transmet à cette autorité. Au cours de cette procédure, les deux parties ont le droit d'être entendues et de recevoir des informations appropriées sur l'état de la plainte, conformément au droit national.

Article 54
Indemnisation

Les destinataires du service ont le droit de demander réparation aux fournisseurs de services intermédiaires, conformément au droit de l'Union et au droit national, pour les dommages ou pertes subis en raison d'une violation par lesdits fournisseurs des obligations qui leur incombent au titre du présent règlement.

Article 55
Rapports d'activité

1. Les coordinateurs pour les services numériques établissent un rapport annuel relatif à leurs activités au titre du présent règlement, y compris le nombre de plaintes reçues en vertu de l'article 53 ainsi qu'un aperçu des suites qui leur ont été données. Les coordinateurs pour les services numériques mettent les rapports annuels à la disposition du public dans un format lisible par une machine, sous réserve des règles applicables en matière de confidentialité des informations en vertu de l'article 84, et les communiquent à la Commission et au comité.

2. Le rapport annuel comporte également les informations suivantes:
a) le nombre et l'objet des injonctions d'agir contre des contenus illicites et des injonctions de fournir des informations, émises conformément aux articles 9 et 10 par toute autorité judiciaire ou administrative nationale de l'État membre du coordinateur pour les services numériques concerné;
b) les suites données à ces injonctions, telles qu'elles ont été communiquées au coordinateur pour les services numériques conformément aux articles 9 et 10.

3. Lorsqu'un État membre a désigné plusieurs autorités compétentes conformément à l'article 49, il veille à ce que le coordinateur pour les services numériques élabore un rapport unique couvrant les activités de toutes les autorités compétentes et à ce que le coordinateur pour les services numériques reçoive toutes les informations pertinentes et tout le soutien nécessaire à cet effet de la part des autres autorités compétentes concernées.

SECTION 2
Compétences, enquête coordonnée et mécanismes de contrôle de la cohérence

Article 56
Compétences

1. L'État membre dans lequel se situe l'établissement principal du fournisseur de services intermédiaires dispose de pouvoirs exclusifs pour surveiller et faire respecter le présent règlement, à l'exception des pouvoirs prévus aux paragraphes 2, 3 et 4.

2. La Commission dispose de pouvoirs exclusifs pour surveiller et faire respecter le chapitre III, section 5.

3. La Commission dispose de pouvoirs pour surveiller et faire respecter le présent règlement, autres que ceux fixés au chapitre III, section 5, à l'encontre des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne.

4. Lorsque la Commission n'a pas engagé de procédure pour la même infraction, l'État membre dans lequel se situe l'établissement principal du fournisseur de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne dispose, à l'encontre desdits fournisseurs, de pouvoirs pour surveiller et faire respecter les obligations fixées dans le présent règlement, autres que ceux fixés au chapitre III, section 5.

5. Les États membres et la Commission surveillent et assurent le respect des dispositions du présent règlement en étroite coopération.

6. Lorsqu'un fournisseur de services intermédiaires ne dispose pas d'un établissement dans l'Union, l'État membre dans lequel son représentant légal réside ou est établi ou la Commission, selon le cas, dispose, conformément aux paragraphes 1 et 4 du présent article, de pouvoirs pour surveiller et faire respecter les obligations pertinentes fixées dans le présent règlement.

7. Lorsqu'un fournisseur de services intermédiaires ne désigne pas de représentant légal conformément à l'article 13, tous les États membres et, pour ce qui concerne les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne, la Commission disposent de pouvoirs de surveillance et d'exécution conformément au présent article.

Lorsqu'un coordinateur des services numériques a l'intention d'exercer ses pouvoirs en vertu du présent paragraphe, il notifie son intention à tous les autres coordinateurs pour les services numériques ainsi qu'à la Commission et veille à ce que les garanties applicables prévues par la Charte soient respectées, notamment pour éviter que le même comportement ne soit sanctionné plus d'une fois pour une infraction aux obligations fixées par le présent règlement. Lorsque la Commission a l'intention d'exercer ses pouvoirs en vertu du présent paragraphe, elle notifie son intention à tous les autres coordinateurs pour les services numériques. À la suite de la notification visée au présent paragraphe, les autres États membres n'engagent pas de procédure pour la même infraction que celle dont il est question dans la notification.

Article 57
Assistance mutuelle

1. Les coordinateurs pour les services numériques et la Commission coopèrent étroitement et se prêtent mutuellement assistance afin d'appliquer le présent règlement de manière cohérente et efficace. L'assistance mutuelle comprend, en particulier, l'échange d'informations conformément au présent article et l'obligation qui incombe au coordinateur pour les services numériques de l'État membre d'établissement d'informer tous les coordinateurs pour les services numériques des États membres de destination, le comité et la Commission de l'ouverture d'une enquête et de son intention de prendre une décision définitive, y compris son évaluation, à l'égard d'un fournisseur de services intermédiaires spécifique.

2. Aux fins d'une enquête, le coordinateur pour les services numériques de l'État membre d'établissement peut demander à d'autres coordinateurs pour les services numériques de fournir les informations spécifiques en leur possession concernant un fournisseur spécifique de services intermédiaires ou d'exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, en ce qui concerne des informations spécifiques se trouvant dans leur État membre. Le cas échéant, le coordinateur pour les services numériques qui reçoit la demande peut associer d'autres autorités compétentes ou d'autres autorités publiques de l'État membre en question.

3. Le coordinateur pour les services numériques qui reçoit la demande conformément au paragraphe 2 y fait droit et informe le coordinateur pour les services numériques de l'État membre d'établissement des mesures prises, dans les meilleurs délais et au plus tard deux mois après la réception de la demande, sauf si:
a) la portée ou l'objet de la demande ne sont pas suffisamment précis, justifiés ou proportionnés au regard des objectifs de l'enquête; ou
b) ni le coordinateur pour les services numériques qui reçoit la demande ni aucune autre autorité compétente ou autorité publique de cet État membre n'est en possession des informations demandées ou ne peut accéder à celles-ci; ou
c) il n'est pas possible de faire droit à la demande sans violer le droit de l'Union ou le droit national.

Le coordinateur pour les services numériques qui reçoit la demande motive son refus en soumettant une réponse motivée, dans le délai fixé au premier alinéa.

Article 58
Coopération transfrontière entre les coordinateurs pour les services numériques

1. Sauf dans le cas où la Commission a ouvert une enquête pour la même infraction alléguée, lorsqu'un coordinateur pour les services numériques d'un État membre de destination a des raisons de soupçonner que le fournisseur d'un service intermédiaire a enfreint le présent règlement d'une manière qui porte atteinte aux destinataires du service dans l'État membre dudit coordinateur pour les services numériques, il peut demander au coordinateur pour les services numériques de l'État membre d'établissement d'examiner la situation et de prendre les mesures d'enquête et d'exécution nécessaires pour assurer le respect du présent règlement.

2. Sauf dans le cas où la Commission a ouvert une enquête pour la même infraction alléguée, et à la demande d'au moins trois coordinateurs pour les services numériques d'États membres de destination, ayant des raisons de soupçonner qu'un fournisseur de services intermédiaires spécifique a enfreint le présent règlement d'une manière qui porte atteinte aux destinataires du service dans leur État membre, le comité peut demander au coordinateur pour les services numériques de l'État membre d'établissement d'examiner la situation et de prendre les mesures d'enquête et d'exécution nécessaires pour assurer le respect du présent règlement.

3. Toute demande formulée au titre du paragraphe 1 ou 2 est dûment motivée et indique au minimum:

a) le point de contact du fournisseur de services intermédiaires concerné, tel qu'il est prévu à l'article 11;

b) une description des faits pertinents, les dispositions concernées du présent règlement et les raisons pour lesquelles le coordinateur pour les services numériques à l'origine de la demande, ou le comité, soupçonne que le fournisseur a enfreint le présent règlement, y compris la description des effets négatifs de l'infraction alléguée;

c) toute autre information que le coordinateur pour les services numériques à l'origine de la demande, ou le comité, considère comme pertinente, y compris, le cas échéant, des informations recueillies de sa propre initiative ou des suggestions de mesures d'enquête ou d'exécution spécifiques à prendre, y compris des mesures provisoires.

4. Le coordinateur pour les services numériques de l'État membre d'établissement tient le plus grand compte de la demande formulée au titre du paragraphe 1 ou 2 du présent article. Lorsqu'il considère qu'il ne dispose pas de suffisamment d'informa-

tions pour agir sur la base de la demande et qu'il a des raisons de considérer que le coordinateur pour les services numériques à l'origine de la demande, ou le comité, pourrait fournir des informations complémentaires, le coordinateur pour les services numériques de l'État membre d'établissement peut soit demander ces informations conformément à l'article 57, soit lancer, en application de l'article 60, paragraphe 1, une enquête conjointe associant au moins le coordinateur pour les services numériques à l'origine de la demande. Le délai fixé au paragraphe 5 du présent article est suspendu jusqu'à l'obtention de ces informations complémentaires ou jusqu'à ce que l'invitation à participer à l'enquête conjointe ait été déclinée.

5. Dans les meilleurs délais et en tout état de cause dans un délai maximal de deux mois suivant la réception de la demande formulée au titre du paragraphe 1 ou 2, le coordinateur pour les services numériques de l'État membre d'établissement communique au coordinateur pour les services numériques à l'origine de la demande, et au comité, l'évaluation de l'infraction présumée, ainsi qu'une explication de toute mesure d'enquête ou d'exécution prise ou envisagée dans ce cadre afin d'assurer le respect du présent règlement.

Article 59
Saisine de la Commission

1. En l'absence de communication dans le délai fixé à l'article 58, paragraphe 5, en cas de désaccord de la part du comité avec l'évaluation ou les mesures prises ou envisagées au titre de l'article 58, paragraphe 5, ou dans les cas visés à l'article 60, paragraphe 3, le comité peut saisir la Commission de la question, en fournissant toutes les informations pertinentes. Ces informations comprennent au moins la demande ou la recommandation envoyée au coordinateur pour les services numériques de l'État membre d'établissement, l'évaluation réalisée par ce coordinateur pour les services numériques, les raisons du désaccord ainsi que toute information complémentaire justifiant la saisine.

2. La Commission examine la question dans un délai de deux mois suivant la transmission de la question en vertu du paragraphe 1, après avoir consulté le coordinateur pour les services numériques de l'État membre d'établissement.

3. Lorsque, en vertu du paragraphe 2 du présent article, la Commission considère que l'évaluation ou les mesures d'enquête ou d'exécution prises ou envisagées au titre de l'article 58, paragraphe 5, sont insuffisantes pour garantir l'exécution effective du présent règlement ou sont, d'une autre façon, incompatibles avec le présent règlement, elle fait part de son point de vue au coordinateur pour les services numériques de l'État membre d'établissement ainsi qu'au comité, et demande au coordinateur pour les services numériques de l'État membre d'établissement de réexaminer la question.

Le coordinateur pour les services numériques de l'État membre d'établissement prend les mesures d'enquête ou d'exécution nécessaires en vue d'assurer le respect du présent règlement, en tenant le plus grand compte du point de vue et de la demande de réexamen de la Commission. Le coordinateur pour les services numériques de l'État membre d'établissement informe la Commission et le coordinateur pour les services numériques à l'origine de la demande ou le comité qui est intervenu au titre de l'article 58, paragraphe 1 ou 2, des mesures prises dans les deux mois à compter de cette demande de réexamen.

Article 60
Enquêtes conjointes

1. Le coordinateur pour les services numériques de l'État membre d'établissement peut lancer et diriger des enquêtes conjointes avec la participation d'un ou de plusieurs coordinateurs pour les services numériques concernés:

a) de sa propre initiative, en ce qui concerne une infraction alléguée au présent règlement commise par un fournisseur de services intermédiaires donné dans plusieurs États membres; ou

b) sur recommandation du comité, à la demande d'au moins trois coordinateurs pour les services numériques alléguant, sur la base d'une suspicion raisonnable, l'existence

d'une infraction commise par un fournisseur de services intermédiaires donné, portant atteinte aux destinataires du service dans leur État membre.

2. Tout coordinateur pour les services numériques qui démontre qu'il a un intérêt légitime à participer à une enquête conjointe conformément au paragraphe 1 peut demander à le faire. L'enquête conjointe est menée à terme dans un délai de trois mois à compter du moment où elle a été lancée, sauf si les participants en conviennent autrement.

Le coordinateur pour les services numériques de l'État membre d'établissement communique à tous les coordinateurs pour les services numériques, à la Commission et au comité sa position préliminaire sur l'infraction alléguée au plus tard un mois après la fin du délai visé au premier alinéa. La position préliminaire tient compte du point de vue de tous les autres coordinateurs pour les services numériques participant à l'enquête conjointe. Le cas échéant, cette position préliminaire expose également les mesures d'exécution envisagées.

3. Le comité peut saisir la Commission conformément à l'article 59, lorsque:

a) le coordinateur pour les services numériques de l'État membre d'établissement n'a pas communiqué sa position préliminaire dans le délai fixé au paragraphe 2;

b) le comité exprime un désaccord important avec la position préliminaire communiquée par le coordinateur pour les services numériques de l'État membre d'établissement; ou

c) le coordinateur pour les services numériques de l'État membre d'établissement n'a pas lancé l'enquête conjointe promptement à la suite de la recommandation du comité visée au paragraphe 1, point b).

4. Lorsqu'ils procèdent à une enquête conjointe, les coordinateurs pour les services numériques participants coopèrent de bonne foi, en tenant compte, le cas échéant, des indications du coordinateur pour les services numériques de l'État membre d'établissement et de la recommandation du comité. Les coordinateurs pour les services numériques des États membres de destination participant à l'enquête conjointe sont habilités, à la demande du coordinateur pour les services numériques de l'État membre d'établissement ou après l'avoir consulté, à exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, à l'égard des fournisseurs de services intermédiaires concernés par l'infraction alléguée, en ce qui concerne les informations et les locaux situés sur leur territoire.

SECTION 3
Comité européen des services numériques

Article 61
Comité européen des services numériques

1. Un groupe consultatif indépendant de coordinateurs pour les services numériques, dénommé "comité européen des services numériques" (ci-après dénommé "comité") est établi pour assurer la surveillance des fournisseurs de services intermédiaires.

2. Le comité conseille les coordinateurs pour les services numériques et la Commission conformément au présent règlement pour atteindre les objectifs suivants:
a) contribuer à l'application cohérente du présent règlement et à la coopération efficace des coordinateurs pour les services numériques et de la Commission en ce qui concerne les matières relevant du présent règlement;
b) coordonner les lignes directrices et les analyses de la Commission et des coordinateurs pour les services numériques et d'autres autorités compétentes sur les questions émergentes dans l'ensemble du marché intérieur en ce qui concerne les matières relevant du présent règlement, et y contribuer;
c) assister les coordinateurs pour les services numériques et la Commission dans la surveillance des très grandes plateformes en ligne.

Article 62
Structure du comité

1. Le comité se compose des coordinateurs pour les services numériques qui sont représentés par de hauts fonctionnaires. Le fait qu'un ou plusieurs États membres ne désignent pas de coordinateur pour les services numériques ne fait pas obstacle à ce que le comité exécute ses tâches au titre du présent règlement. Lorsque le droit national le prévoit, d'autres autorités compétentes investies de responsabilités opérationnelles spécifiques en vue de l'application et de l'exécution du présent règlement peuvent participer au comité aux côtés du coordinateur pour les services numériques. D'autres autorités nationales peuvent être invitées aux réunions, lorsque les questions examinées relèvent de leurs compétences.

2. Le comité est présidé par la Commission. La Commission convoque les réunions et prépare l'ordre du jour conformément aux missions du comité au titre du présent règlement et à son règlement intérieur. Lorsque le comité est saisi d'une demande d'adopter une recommandation en vertu du présent règlement, il met immédiatement cette demande à la disposition des autres coordinateurs pour les services numériques via le système de partage d'informations prévu à l'article 85.

3. Chaque État membre dispose d'une voix. La Commission n'a pas de droit de vote.

Le comité adopte ses décisions à la majorité simple. Lorsqu'il adopte une recommandation destinée à la Commission ainsi que le prévoit l'article 36, paragraphe 1, premier alinéa, le comité vote dans les 48 heures suivant la demande du président du comité.

4. La Commission apporte un appui administratif et analytique aux activités du comité au titre du présent règlement.

5. Le comité peut inviter des experts et des observateurs à participer à ses réunions, et peut coopérer avec d'autres organes, organismes et groupes consultatifs de l'Union, ainsi qu'avec des experts externes, le cas échéant. Le comité rend publics les résultats de cette coopération.

6. Le comité peut consulter les parties intéressées et rend publics les résultats de telles consultations.

7. Le comité adopte son règlement intérieur une fois celui-ci approuvé par la Commission.

Article 63
Missions du comité

1. Lorsque cela est nécessaire pour réaliser les objectifs énoncés à l'article 61, paragraphe 2, le comité:

a) soutient la coordination d'enquêtes conjointes;

b) soutient les autorités compétentes dans l'analyse des rapports et résultats des audits réalisés auprès des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne dont le présent règlement prévoit la transmission;

c) émet des avis, des recommandations ou des conseils destinés aux coordinateurs pour les services numériques conformément au présent règlement, en tenant compte notamment de la liberté des fournisseurs de services intermédiaires de fournir des services;

d) conseille la Commission en ce qui concerne les mesures visées à l'article 66 et adopte des avis concernant les très grandes plateformes en ligne ou les très grands moteurs de recherche en ligne conformément au présent règlement;

e) soutient et encourage l'élaboration et la mise en œuvre de normes européennes, lignes directrices, rapports, modèles et codes de conduite, en collaboration avec les parties prenantes pertinentes, comme le prévoit le présent règlement, y compris en émettant des avis ou des recommandations sur les questions liées à l'article 44, ainsi

que l'identification des questions émergentes, en ce qui concerne les matières relevant du présent règlement.

2. Les coordinateurs pour les services numériques et, selon le cas, d'autres autorités compétentes qui ne suivent pas les avis, demandes ou recommandations adoptés par le comité qui leur ont été adressés motivent ce choix, notamment en donnant une explication concernant les enquêtes, actions et mesures qu'ils ont mises en œuvre dans les rapports qu'ils établissent conformément au présent règlement ou lors de l'adoption des décisions pertinentes, le cas échéant.

SECTION 4
Surveillance, enquêtes, exécution et contrôle concernant les fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne

Article 64
Développement de l'expertise et des capacités

1. La Commission, en coopération avec les coordinateurs pour les services numériques et le comité, développe l'expertise et les capacités de l'Union, y compris, le cas échéant, en détachant du personnel des États membres.

2. En outre, la Commission, en coopération avec les coordinateurs pour les services numériques et le comité, coordonne l'évaluation des questions systémiques et émergentes relatives aux très grandes plateformes en ligne ou aux très grands moteurs de recherche en ligne qui se posent dans l'ensemble de l'Union en ce qui concerne les matières relevant du présent règlement.

3. La Commission peut demander aux coordinateurs pour les services numériques, au comité et à d'autres organes ou organismes de l'Union disposant de l'expertise pertinente de soutenir l'évaluation des questions systémiques et émergentes qui se posent dans l'ensemble de l'Union au titre du présent règlement.

4. Les États membres coopèrent avec la Commission, en particulier, par l'intermédiaire de leurs coordinateurs pour les services numériques respectifs et d'autres autorités compétentes, le cas échéant, y compris en mettant à disposition leur expertise et leurs capacités.

Article 65
Exécution des obligations des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

1. À des fins d'enquête sur le respect, par les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne, des obligations fixées par le présent règlement, la Commission peut exercer les pouvoirs d'enquête prévus dans la présente section avant même d'engager la procédure prévue à l'article 66, paragraphe 2. Elle peut exercer ces pouvoirs de sa propre initiative ou à la suite d'une demande formulée en vertu du paragraphe 2 du présent article.

2. Lorsqu'un coordinateur pour les services numériques a des raisons de soupçonner qu'un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne a enfreint les dispositions du chapitre III, section 5, ou a systématiquement enfreint l'une des dispositions du présent règlement d'une manière qui affecte gravement les destinataires du service dans son État membre, il peut envoyer à la Commission, via le système de partage d'informations prévu à l'article 85, une demande d'examen de la question.

3. Toute demande formulée en vertu du paragraphe 2 est dûment motivée et indique au minimum:

a) le point de contact du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, comme prévu à l'article 11;

b) une description des faits pertinents, les dispositions du présent règlement concernées et les raisons pour lesquelles le coordinateur pour les services numériques à l'ori-

gine de la demande soupçonne que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné a enfreint le présent règlement, avec une description des faits montrant que l'infraction présumée est de nature systémique;

c) toute autre information que le coordinateur pour les services numériques à l'origine de la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 66
Procédures engagées par la Commission et coopération à l'enquête

1. La Commission peut engager une procédure en vue de l'éventuelle adoption de décisions au titre des articles 73 et 74 à l'égard de la conduite en cause du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne que la Commission soupçonne d'avoir enfreint l'une des dispositions du présent règlement.

2. Lorsque la Commission décide d'engager une procédure en vertu du paragraphe 1 du présent article, elle en informe tous les coordinateurs pour les services numériques et le comité via le système de partage d'informations visé à l'article 85, ainsi que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné.

Les coordinateurs pour les services numériques transmettent à la Commission, dans les meilleurs délais après avoir été informés qu'une procédure a été engagée, toutes les informations qu'ils détiennent au sujet de l'infraction en cause.

L'engagement d'une procédure par la Commission en vertu du paragraphe 1 du présent article relève le coordinateur pour les services numériques, ou toute autorité compétente selon le cas, de ses pouvoirs de surveillance et d'exécution prévus dans le présent règlement conformément à l'article 56, paragraphe 4.

3. Dans l'exercice des pouvoirs d'enquête que lui confère le présent règlement, la Commission peut demander l'aide individuelle ou conjointe des coordinateurs pour les services numériques concernés par l'infraction présumée, notamment du coordinateur pour les services numériques de l'État membre d'établissement. Les coordinateurs pour les services numériques qui ont reçu une telle demande, ainsi que toute autre autorité compétente à laquelle le coordinateur pour les services numériques fait appel, coopèrent de bonne foi et en temps utile avec la Commission et sont habilités à exercer leurs pouvoirs d'enquête visés à l'article 51, paragraphe 1, à l'égard de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne en question, pour ce qui est des informations, des personnes et des locaux situés sur le territoire de leur État membre et conformément à la demande.

4. La Commission fournit au coordinateur pour les services numériques de l'État membre d'établissement et au comité toutes les informations pertinentes sur l'exercice des pouvoirs visés aux articles 67 à 72 et ses conclusions préliminaires conformément à l'article 79, paragraphe 1. Le comité fait part à la Commission de son point de vue sur les conclusions préliminaires dans le délai fixé en vertu de l'article 79, paragraphe 2. La Commission tient le plus grand compte du point de vue du comité dans sa décision.

Article 67
Demandes d'informations

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut, par simple demande ou par voie de décision, requérir du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, ainsi que de toute autre personne physique ou morale agissant pour les besoins de leur activité commerciale, industrielle, artisanale ou libérale qui est raisonnablement susceptible d'avoir connaissance d'informations relatives à l'infraction présumée, y compris des organisations qui réalisent les audits visés à l'article 37 et à l'article 75, paragraphe 2, qu'ils fournissent ces informations dans un délai raisonnable.

2. Lorsqu'elle envoie une simple demande d'informations au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou à une autre personne visée au paragraphe 1 du présent article, la Commission indique la base juridique et le but de la demande, précise les informations demandées et fixe le délai dans lequel elles doivent être fournies. Elle mentionne également les amendes prévues à l'article 74 au cas où une information inexacte, incomplète ou trompeuse serait fournie.

3. Lorsque la Commission requiert, par voie de décision, du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée au paragraphe 1 du présent article, qu'ils fournissent des informations, elle indique la base juridique et le but de la demande, précise les informations demandées et fixe le délai dans lequel elles doivent être fournies. Elle mentionne également les amendes prévues à l'article 74 et mentionne ou inflige les astreintes prévues à l'article 76. Elle mentionne également le droit de faire réexaminer la décision par la Cour de justice de l'Union européenne.

4. Les fournisseurs de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concernés ou une autre personne visée au paragraphe 1 ou leurs représentants et, dans le cas de personnes morales, de sociétés ou d'associations n'ayant pas la personnalité juridique, les personnes mandatées pour les représenter selon la loi ou les statuts, sont tenus de fournir les informations demandées au nom du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée au paragraphe 1. Les avocats dûment mandatés peuvent fournir les informations demandées au nom de leurs mandants. Ces derniers voient leur responsabilité pleinement engagée si les informations fournies s'avèrent incomplètes, inexactes ou trompeuses.

5. À la demande de la Commission, les coordinateurs pour les services numériques et autres autorités compétentes fournissent à la Commission toutes les informations nécessaires à l'accomplissement des tâches qui lui sont assignées par la présente section.

6. La Commission, sans retard injustifié après avoir envoyé la simple demande ou la décision visée au paragraphe 1 du présent article, en envoie une copie aux coordinateurs pour les services numériques, par l'intermédiaire du système de partage d'informations visé à l'article 85.

Article 68
Pouvoir de mener des entretiens et de recueillir des déclarations

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut interroger toute personne physique ou morale qui consent à être interrogée aux fins de la collecte d'informations relatives à l'objet d'une enquête, en lien avec l'infraction présumée. La Commission est habilitée à enregistrer ces entretiens par des moyens techniques appropriés.

2. Si l'entretien visé au paragraphe 1 se déroule dans d'autres locaux que ceux de la Commission, celle-ci en informe le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'entretien a lieu. À la demande dudit coordinateur pour les services numériques, ses fonctionnaires peuvent assister les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour mener l'entretien.

Article 69
Pouvoir d'effectuer des inspections

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut effectuer toutes les inspections nécessaires dans les locaux du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne visée à l'article 67, paragraphe 1.

2. Les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour effectuer une inspection sont investis des pouvoirs suivants:

a) pénétrer dans tous les locaux, terrains et moyens de transport du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou de l'autre personne concernée;

b) examiner les livres et autres registres relatifs à la fourniture du service concerné, quel que soit le support sur lequel ils sont stockés;

c) prendre ou obtenir sous quelque forme que ce soit une copie ou un extrait des livres ou autres registres;

d) exiger du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée qu'il donne accès à son organisation, à son fonctionnement, à son système informatique, à ses algorithmes, à son traitement des données et à ses pratiques commerciales, qu'il fournisse des explications à ce sujet et qu'il enregistre ou documente les explications données;

e) sceller tout local utilisé pour les besoins de l'activité commerciale, industrielle, artisanale ou libérale du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée, ainsi que les livres ou autres registres, pendant la période d'inspection et dans la mesure nécessaires à l'inspection;

f) demander à tout représentant ou membre du personnel du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée, des explications sur des faits ou des documents en rapport avec l'objet et le but de l'inspection et enregistrer les réponses;

g) adresser des questions à tout représentant ou membre du personnel en rapport avec l'objet et le but de l'inspection et enregistrer les réponses.

3. Les inspections peuvent être effectuées avec le concours d'auditeurs ou d'experts nommés par la Commission en vertu de l'article 72, paragraphe 2, et du coordinateur pour les services numériques ou des autorités nationales compétentes de l'État membre sur le territoire duquel l'inspection est menée.

4. Lorsque les livres ou autres registres liés à la fourniture du service concerné dont la production est requise sont produits de manière incomplète ou lorsque les réponses aux questions posées en vertu du paragraphe 2 du présent article sont inexactes, incomplètes ou trompeuses, les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission pour effectuer une inspection exercent leurs pouvoirs sur présentation d'une autorisation écrite précisant l'objet et le but de l'inspection ainsi que les sanctions prévues aux articles 74 et 76. En temps utile avant l'inspection, la Commission informe de l'inspection prévue le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée.

5. Au cours des inspections, les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission, les auditeurs et les experts nommés par la Commission, le coordinateur pour les services numériques ou les autres autorités compétentes de l'État membre sur le territoire duquel l'inspection est effectuée peuvent exiger du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, ou de l'autre personne concernée, qu'il fournisse des explications sur son organisation, son fonctionnement, son système informatique, ses algorithmes, son traitement des données et ses pratiques commerciales, et peuvent adresser des questions à son personnel clé.

6. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou l'autre personne physique ou morale concernée est tenu de se soumettre aux inspections que la Commission a ordonnées par voie de décision. La décision indique l'objet et le but de l'inspection, fixe la date à laquelle elle commence et mentionne les sanctions prévues aux articles 74 et 76, ainsi que le droit de faire réexaminer la décision par la Cour de justice de l'Union européenne. La Commission consulte le coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée avant de prendre cette décision.

7. Les agents du coordinateur pour les services numériques de l'État membre sur le territoire duquel l'inspection doit être effectuée et les autres personnes mandatées ou nommées par ledit coordinateur prêtent activement assistance, à la demande dudit coordinateur pour les services numériques ou de la Commission, aux fonctionnaires et aux autres personnes les accompagnant mandatés par la Commission dans le cadre de l'inspection. Ils disposent à cette fin des pouvoirs énumérés au paragraphe 2.

8. Lorsque les fonctionnaires et les autres personnes les accompagnant mandatés par la Commission constatent que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne, ou l'autre personne concernée, s'oppose à une inspection ordonnée en vertu du présent article, l'État membre sur le territoire duquel l'inspection doit être effectuée leur accorde, sur demande de ces fonctionnaires ou des autres personnes les accompagnant et conformément au droit national de l'État membre, l'assistance nécessaire, y compris, le cas échéant conformément audit droit national, sous la forme de mesures coercitives prises par une autorité répressive compétente, pour leur permettre d'effectuer l'inspection.

9. Si l'assistance prévue au paragraphe 8 requiert l'autorisation d'une autorité judiciaire nationale conformément au droit national de l'État membre concerné, cette autorisation est demandée par le coordinateur pour les services numériques de cet État membre à la demande des fonctionnaires et des autres personnes les accompagnant mandatés par la Commission. Cette autorisation peut également être demandée à titre préventif.

10. Lorsqu'une autorisation visée au paragraphe 9 est demandée, l'autorité judiciaire nationale saisie vérifie que la décision de la Commission ordonnant l'inspection est authentique et que les mesures coercitives envisagées ne sont ni arbitraires ni excessives eu égard à l'objet de l'inspection. Lorsqu'elle procède à cette vérification, l'autorité judiciaire nationale peut demander à la Commission, directement ou par l'intermédiaire des coordinateurs pour les services numériques de l'État membre concerné, des explications détaillées notamment sur les motifs permettant à la Commission de suspecter l'existence d'une infraction au présent règlement, ainsi que sur la gravité de l'infraction suspectée et la nature de l'implication du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ou de l'autre personne concernée. Cependant, l'autorité judiciaire nationale ne peut ni remettre en cause la nécessité de l'inspection ni exiger la communication d'informations figurant dans le dossier de la Commission. Le contrôle de la légalité de la décision de la Commission est réservé à la Cour de justice de l'Union européenne.

Article 70
Mesures provisoires

1. Dans le contexte des procédures susceptibles de mener à l'adoption d'une décision constatant un manquement en application de l'article 73, paragraphe 1, en cas d'urgence justifiée par le fait qu'un préjudice grave risque d'être causé aux destinataires du service, la Commission peut, par voie de décision, ordonner des mesures provisoires à l'encontre du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné sur la base d'un constat prima facie d'infraction.

2. Une décision prise en vertu du paragraphe 1 est applicable pour une durée déterminée et est renouvelable dans la mesure où cela est nécessaire et opportun.

Article 71
Engagements

1. Si, au cours d'une procédure au titre de la présente section, le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné propose des engagements afin de garantir le respect des dispositions pertinentes du présent règlement, la Commission peut, par voie de décision, rendre ces engagements contraignants pour le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné et déclarer qu'il n'y a plus lieu d'agir.

2. La Commission peut rouvrir la procédure, sur demande ou de sa propre initiative:
a) si l'un des faits sur lesquels la décision repose subit un changement important;

b) si le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne contrevient à ses engagements; ou
c) si la décision reposait sur des informations incomplètes, inexactes ou trompeuses fournies par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1.

3. Si la Commission estime que les engagements proposés par le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ne permettent pas de garantir le respect effectif des dispositions pertinentes du présent règlement, elle rejette ces engagements dans une décision motivée lors de la clôture de la procédure.

Article 72
Mesures de contrôle

1. Pour l'accomplissement des tâches qui lui sont assignées par la présente section, la Commission peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne concernés. La Commission peut leur ordonner de donner accès à leurs bases de données et algorithmes, ainsi que de fournir des explications à cet égard. Ces mesures peuvent notamment imposer au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne l'obligation de conserver tous les documents jugés nécessaires pour évaluer la mise en œuvre et le respect des obligations prévues par le présent règlement.

2. Les mesures visées au paragraphe 1 peuvent comprendre la nomination d'experts et d'auditeurs externes indépendants, ainsi que d'experts et d'auditeurs des autorités nationales compétentes avec l'accord de l'autorité concernée, pour aider la Commission à contrôler la mise en œuvre et le respect effectifs des dispositions pertinentes du présent règlement et lui apporter une expertise et des connaissances spécifiques.

Article 73
Non-respect

1. La Commission adopte une décision constatant un manquement lorsqu'elle constate que le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ne respecte pas un ou plusieurs des éléments suivants:
a) les dispositions pertinentes du présent règlement;
b) les mesures provisoires ordonnées en vertu de l'article 70;
c) les engagements rendus contraignants en vertu de l'article 71.

2. Avant d'adopter la décision visée au paragraphe 1, la Commission fait part de ses constatations préliminaires au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné. Dans ses constatations préliminaires, la Commission explique les mesures qu'elle envisage de prendre, ou que le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne devrait prendre, selon elle, afin de donner suite de manière effective aux constatations préliminaires.

3. Dans la décision adoptée en vertu du paragraphe 1, la Commission ordonne au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné de prendre les mesures nécessaires pour assurer le respect de ladite décision dans un délai approprié qui y est précisé et de fournir des informations relatives aux mesures que ledit fournisseur entend adopter pour respecter la décision.

4. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné fournit à la Commission la description des mesures qu'il a prises pour garantir le respect de la décision adoptée en vertu du paragraphe 1 lors de leur mise en œuvre.

5. Lorsque la Commission constate que les conditions énoncées au paragraphe 1 ne sont pas réunies, elle clôt l'enquête par voie de décision. La décision est applicable avec effet immédiat.

Article 74
Amendes

1. Dans la décision visée à l'article 73, la Commission peut infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné des amendes jusqu'à concurrence de 6 % du chiffre d'affaires mondial annuel réalisé au cours de l'exercice précédent lorsqu'elle constate que ledit fournisseur, de propos délibéré ou par négligence:
a) enfreint les dispositions pertinentes du présent règlement;
b) ne respecte pas une décision ordonnant des mesures provisoires en application de l'article 70; ou
c) ne respecte pas un engagement rendu contraignant par voie de décision en vertu de l'article 71.

2. La Commission peut adopter une décision visant à infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche concerné, ou à une autre personne physique ou morale visée à l'article 67, paragraphe 1, des amendes jusqu'à concurrence de 1 % des revenus ou du chiffre d'affaires mondial annuels de l'exercice précédent lorsque, de propos délibéré ou par négligence, ils:

a) fournissent des informations inexactes, incomplètes ou trompeuses en réponse à une simple demande ou à une demande par voie de décision, conformément à l'article 67;
b) omettent de répondre à la demande d'informations par voie de décision dans le délai fixé;

c) omettent de rectifier, dans le délai fixé par la Commission, les informations inexactes, incomplètes ou trompeuses fournies par un membre du personnel, ou omettent ou refusent de fournir des informations complètes;
d) refusent de se soumettre à une inspection décidée en vertu de l'article 69;
e) ne respectent pas les mesures adoptées par la Commission en vertu de l'article 72; ou
f) ne respectent pas les conditions d'accès au dossier de la Commission prévues à l'article 79, paragraphe 4.

3. Avant d'adopter la décision au titre du paragraphe 2 du présent article, la Commission fait part de ses constatations préliminaires au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, ou à une autre personne visée à l'article 67, paragraphe 1.

4. Pour déterminer le montant de l'amende, la Commission prend en considération la nature, la gravité, la durée et la répétition de l'infraction ainsi que, pour les amendes infligées au titre du paragraphe 2, le retard causé à la procédure.

Article 75
Surveillance renforcée des voies de recours pour remédier aux violations des obligations prévues au chapitre III, section 5

1. Lorsqu'elle adopte une décision en vertu de l'article 73 concernant la violation par un fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne de l'une des dispositions du chapitre III, section 5, la Commission fait usage du système de surveillance renforcée prévu au présent article. Ce faisant, elle tient le plus grand compte des avis du comité au titre du présent article.

2. Dans la décision visée à l'article 73, la Commission demande au fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné d'élaborer et de communiquer, dans un délai raisonnable précisé dans la décision, aux coordinateurs pour les services numériques, à la Commission et au comité, un plan d'action exposant les mesures nécessaires pour mettre fin à l'infraction ou y remédier. Ces mesures comprennent un engagement à réaliser un audit indépendant conformément à l'article 37, paragraphes 3 et 4, sur la mise en œuvre des autres mesures, et précisent l'identité des auditeurs ainsi que la méthodologie, le calendrier et le suivi de l'audit. Les mesures peuvent également comprendre, le cas échéant, l'engagement de participer à un code de conduite pertinent tel qu'il est prévu à l'article 45.

3. Dans un délai d'un mois suivant la réception du plan d'action, le comité communique son avis sur celui-ci à la Commission. Dans un délai d'un mois suivant la réception de cet avis, la Commission décide si les mesures prévues dans le plan d'action sont suffisantes pour mettre fin à l'infraction ou y remédier et fixe un délai raisonnable pour sa mise en œuvre. L'engagement éventuel d'adhérer aux codes de conduite pertinents est pris en compte dans cette décision. La Commission contrôle ensuite la mise en œuvre du plan d'action. À cette fin, le fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné communique le rapport d'audit à la Commission sans retard injustifié dès qu'il est disponible et tient la Commission informée des mesures prises pour la mise en œuvre du plan d'action. La Commission peut, lorsque cela est nécessaire aux fins d'un tel contrôle, exiger du fournisseur d'une très grande plateforme en ligne ou d'un très grand moteur de recherche en ligne concerné qu'il fournisse des informations supplémentaires dans un délai raisonnable fixé par la Commission.

La Commission tient le comité et les coordinateurs pour les services numériques informés de la mise en œuvre du plan d'action et de son suivi.

4. La Commission peut prendre les mesures nécessaires conformément au présent règlement, et notamment à l'article 76, paragraphe 1, point e), et à l'article 82, paragraphe 1, lorsque:
a) le fournisseur concerné de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne ne fournit pas de plan d'action, le rapport d'audit, les mises à jour nécessaires ou toute information supplémentaire requise, dans le délai applicable;
b) la Commission rejette le plan d'action proposé, car elle estime que les mesures qui y sont énoncées sont insuffisantes pour mettre fin à l'infraction ou y remédier; ou
c) la Commission considère, sur la base du rapport d'audit, des mises à jour ou des informations supplémentaires fournies ou de toute autre information pertinente dont elle dispose, que la mise en œuvre du plan d'action est insuffisante pour mettre fin à l'infraction ou y remédier.

Article 76
Astreintes

1. La Commission peut adopter une décision visant à infliger au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche concerné ou à une autre personne visée à l'article 67, paragraphe 1, selon le cas, des astreintes jusqu'à concurrence de 5 % des revenus ou du chiffre d'affaires mondial journaliers moyens de l'exercice précédent par jour, calculées à compter de la date qu'elle fixe dans sa décision, pour les contraindre:
a) à fournir des informations exactes et complètes en réponse à une demande d'informations par voie de décision en application de l'article 67;
b) à se soumettre à une inspection ordonnée par voie de décision prise en vertu de l'article 69;

c) à respecter une décision ordonnant des mesures provisoires prise en vertu de l'article 70, paragraphe 1;
d) à respecter des engagements rendus juridiquement contraignants par voie de décision prise en vertu de l'article 71, paragraphe 1;
e) à respecter une décision prise en application de l'article 73, paragraphe 1, y compris, le cas échéant, les exigences qu'elle contient concernant le plan d'action visé à l'article 75.

2. Lorsque le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1, ont satisfait à l'obligation pour l'exécution de laquelle l'astreinte a été infligée, la Commission peut fixer le montant définitif de l'astreinte à un chiffre inférieur à celui qui résulte de la décision initiale.

Article 77
Prescription en matière d'imposition de sanctions

1. Les pouvoirs conférés à la Commission par les articles 74 et 76 sont soumis à un délai de prescription de cinq ans.

2. Le délai de prescription court à compter du jour où l'infraction a été commise. Toutefois, pour les infractions continues ou répétées, le délai de prescription ne court qu'à compter du jour où l'infraction prend fin.

3. Le délai de prescription en matière d'imposition d'amendes ou d'astreintes est interrompu par tout acte de la Commission ou du coordinateur pour les services numériques aux fins de l'enquête ou de la procédure relative à l'infraction. Constituent notamment des actes interrompant la prescription:
a) les demandes d'informations de la Commission ou d'un coordinateur pour les services numériques;
b) l'inspection;
c) l'ouverture d'une procédure par la Commission en vertu de l'article 66, paragraphe 1.

4. Un nouveau délai de prescription commence à courir à partir de chaque interruption. Toutefois, la prescription en matière d'imposition d'amendes ou d'astreintes est acquise au plus tard le jour où un délai égal au double du délai de prescription arrive à expiration sans que la Commission ait prononcé une amende ou astreinte. Ce délai est prolongé de la période pendant laquelle le délai de prescription a été suspendu conformément au paragraphe 5.

5. La prescription en matière d'imposition d'amendes ou d'astreintes est suspendue aussi longtemps que la décision de la Commission fait l'objet d'une procédure pendante devant la Cour de justice de l'Union européenne.

Article 78
Prescription en matière d'exécution des sanctions

1. Le pouvoir de la Commission d'exécuter les décisions prises en application des articles 74 et 76 est soumis à un délai de prescription de cinq ans.

2. Le délai de prescription court à compter du jour où la décision est devenue définitive.

3. Le délai de prescription en matière d'exécution des sanctions est interrompu:
a) par la notification d'une décision modifiant le montant initial de l'amende ou de l'astreinte ou rejetant une demande tendant à obtenir une telle modification;
b) par tout acte de la Commission ou d'un État membre agissant à la demande de la Commission, visant au recouvrement forcé de l'amende ou de l'astreinte.

4. Un nouveau délai de prescription commence à courir à partir de chaque interruption.

5. Le délai de prescription en matière d'exécution forcée des sanctions est suspendu:
a) aussi longtemps qu'un délai de paiement est accordé;
b) aussi longtemps que l'exécution forcée du paiement est suspendue en vertu d'une décision de la Cour de justice de l'Union européenne ou d'une décision d'une juridiction nationale.

Article 79
Droit d'être entendu et droit d'accès au dossier

1. Avant d'adopter une décision au titre de l'article 73, paragraphe 1, de l'article 74 ou de l'article 76, la Commission donne au fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou à une autre personne visée à l'article 67, paragraphe 1, l'occasion de faire connaître son point de vue sur:
a) les constatations préliminaires de la Commission, y compris sur tout grief retenu par la Commission; et
b) les mesures que la Commission peut avoir l'intention de prendre au vu des constatations préliminaires visées au point a).

2. Le fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou une autre personne visée à l'article 67, paragraphe 1, peut présenter ses observations sur les constatations préliminaires de la Commission dans un délai raisonnable fixé par la Commission dans ses constatations préliminaires et qui ne peut être inférieur à quatorze jours.

3. La Commission ne fonde ses décisions que sur les griefs au sujet desquels les parties concernées ont pu faire valoir leurs observations.

4. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties ont le droit d'avoir accès au dossier de la Commission conformément aux modalités d'une divulgation négociée, sous réserve de l'intérêt légitime du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné ou d'une autre personne concernée à ce que leurs secrets d'affaires ne soient pas divulgués. La Commission est habilitée à adopter des décisions fixant ces modalités de divulgation en cas de désaccord entre les parties. Le droit d'accès au dossier de la Commission ne s'étend pas aux informations confidentielles et aux documents internes de la Commission, du comité, des coordinateurs pour les services numériques, d'autres autorités compétentes ou d'autres autorités publiques des États membres. En particulier, le droit d'accès ne s'étend pas à la correspondance entre la Commission et ces autorités. Aucune disposition du présent paragraphe n'empêche la Commission de divulguer et d'utiliser des informations nécessaires pour apporter la preuve d'une infraction.

5. Les informations recueillies par application des articles 67, 68 et 69 ne sont utilisées qu'aux fins du présent règlement.

Article 80
Publication des décisions

1. La Commission publie les décisions qu'elle adopte au titre de l'article 70, paragraphe 1, de l'article 71, paragraphe 1, et des articles 73 à 76. Cette publication mentionne le nom des parties intéressées et l'essentiel de la décision, y compris les sanctions imposées.

2. La publication tient compte des droits et intérêts légitimes du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné, de toute autre personne visée à l'article 67, paragraphe 1, et de tout tiers à ce que leurs informations confidentielles ne soient pas divulguées.

Article 81
Contrôle de la Cour de justice de l'Union européenne

Conformément à l'article 261 du traité sur le fonctionnement de l'Union européenne, la Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission inflige des amendes ou des astreintes. Elle peut supprimer, réduire ou majorer l'amende ou l'astreinte infligée.

Article 82
Demandes de restrictions d'accès et coopération avec les juridictions nationales

1. Lorsque tous les pouvoirs au titre de la présente section pour parvenir à la cessation d'une infraction au présent règlement ont été épuisés, que l'infraction persiste et entraîne un préjudice grave ne pouvant pas être évité via l'exercice d'autres pouvoirs prévus par le droit de l'Union ou le droit national, la Commission peut demander au coordinateur pour les services numériques de l'État membre d'établissement du fournisseur de la très grande plateforme en ligne ou du très grand moteur de recherche en ligne concerné d'agir conformément à l'article 51, paragraphe 3.

Avant d'adresser une telle demande au coordinateur pour les services numériques, la Commission invite les parties intéressées à soumettre des observations écrites dans un délai qui ne peut être inférieur à quatorze jours ouvrables, en décrivant les mesures qu'elle entend demander et en identifiant le ou les destinataires prévus.

2. Lorsque l'application cohérente du présent règlement le justifie, la Commission, agissant d'office, peut soumettre des observations écrites à l'autorité judiciaire compétente visée à l'article 51, paragraphe 3. Avec l'autorisation de l'autorité judiciaire en question, elle peut aussi présenter des observations orales.

Aux seules fins de lui permettre de préparer ses observations, la Commission peut solliciter l'autorité judiciaire afin qu'elle lui transmette ou lui fasse transmettre tout document nécessaire à l'appréciation de l'affaire.

3. Lorsqu'une juridiction nationale statue sur une question qui fait déjà l'objet d'une décision adoptée par la Commission au titre du présent règlement, cette juridiction nationale ne prend aucune décision allant à l'encontre de la décision de la Commission. Les juridictions nationales évitent également de prendre des décisions qui iraient à l'encontre d'une décision envisagée par la Commission dans une procédure qu'elle a intentée au titre du présent règlement. À cette fin, la juridiction nationale peut évaluer s'il est nécessaire de suspendre sa procédure. Cette disposition est sans préjudice de l'article 267 du traité sur le fonctionnement de l'Union européenne.

Article 83
Actes d'exécution relatifs à l'intervention de la Commission

En ce qui concerne l'intervention de la Commission au titre de la présente section, la Commission peut adopter des actes d'exécution établissant les modalités pratiques pour:
a) les procédures au titre des articles 69 et 72;
b) les auditions prévues à l'article 79;
c) la divulgation négociée d'informations prévue à l'article 79.

Avant d'adopter une disposition en vertu du premier alinéa du présent article, la Commission en publie le projet et invite toutes les parties intéressées à lui soumettre leurs observations dans un délai qu'elle fixe et qui ne peut être inférieur à un mois. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

SECTION 5
Dispositions communes relatives à l'exécution

Article 84
Secret professionnel

Sans préjudice de l'échange et de l'utilisation des informations visées dans le présent chapitre, la Commission, le comité, les autorités compétentes des États membres et leurs fonctionnaires, agents et les autres personnes travaillant sous leur supervision respectifs, ainsi que toute autre personne physique ou morale impliquée, dont les auditeurs et experts nommés en vertu de l'article 72, paragraphe 2, sont tenus de ne pas divulguer les informations qu'ils ont recueillies ou échangées au titre du présent règlement et qui, par leur nature, sont couvertes par le secret professionnel.

Article 85
Système de partage d'informations

1. La Commission met en place et maintient un système de partage d'informations fiable et sûr facilitant les communications entre les coordinateurs pour les services numériques, la Commission et le comité. D'autres autorités compétentes peuvent se voir accorder l'accès à ce système, lorsque cela s'avère nécessaire pour l'accomplissement des tâches qui leur sont confiées conformément au présent règlement.

2. Les coordinateurs pour les services numériques, la Commission et le comité utilisent le système de partage d'informations pour toutes les communications au titre du présent règlement.

3. La Commission adopte des actes d'exécution établissant les modalités pratiques et opérationnelles du fonctionnement du système de partage d'informations et de son interopérabilité avec d'autres systèmes pertinents. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 88.

Article 86
Représentation

1. Sans préjudice de la directive (UE) 2020/1828 ou de tout autre type de représentation au titre du droit national, les destinataires de services intermédiaires ont à tout le

moins le droit de mandater un organisme, une organisation ou une association pour exercer les droits conférés par le présent règlement pour leur compte, pour autant que cet organisme, cette organisation ou cette association remplisse toutes les conditions suivantes:
a) il opère sans but lucratif;
b) il a été régulièrement constitué, conformément au droit d'un État membre;
c) ses objectifs statutaires comprennent un intérêt légitime à assurer le respect du présent règlement.

2. Les fournisseurs de plateformes en ligne prennent les mesures techniques et organisationnelles nécessaires pour veiller à ce que les plaintes déposées par les organismes, organisations ou associations visés au paragraphe 1 du présent article au nom des destinataires du service à l'aide des mécanismes prévus à l'article 20, paragraphe 1, soient traitées et donnent lieu à des décisions de manière prioritaire et sans retard injustifié.

SECTION 6
Actes délégués et actes d'exécution

cf. Actes délégués

Article 87
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. La délégation de pouvoir visée aux articles 24, 33, 37, 40 et 43 est conférée à la Commission pour une période de cinq ans à compter du 16 novembre 2022. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée aux articles 24, 33, 37, 40 et 43 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer".

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

6. Un acte délégué adopté en vertu des articles 24, 33, 37, 40 et 43 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 88
Comité

1. La Commission est assistée par un comité (ci-après dénommé "comité pour les services numériques"). Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 s'applique.

CHAPITRE V
DISPOSITIONS FINALES

Article 89
Modifications de la directive 2000/31/CE

1. Les articles 12 à 15 de la directive 2000/31/CE sont supprimés.

2. Les références aux articles 12 à 15 de la directive 2000/31/CE s'entendent comme étant faites respectivement aux articles 4, 5, 6 et 8 du présent règlement.

Article 90
Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:
"68) Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1)."

Article 91
Réexamen

1. Au plus tard le 18 février 2027, la Commission évalue l'effet potentiel du présent règlement sur le développement et la croissance économique des petites et moyennes entreprises et présente un rapport à cet égard au Parlement européen, au Conseil et au Comité économique et social européen.

Au plus tard le 17 novembre 2025, la Commission évalue les éléments suivants et fait rapport à ce sujet au Parlement européen, au Conseil et au Comité économique et social:

a) l'application de l'article 33, y compris l'éventail des fournisseurs de services intermédiaires couverts par les obligations prévues au chapitre III, section 5, du présent règlement;

b) la manière dont le présent règlement interagit avec d'autres actes juridiques, en particulier les actes visés à l'article 2, paragraphes 3 et 4.

2. Au plus tard le 17 novembre 2027, puis tous les cinq ans, la Commission évalue le présent règlement et fait rapport au Parlement européen, au Conseil et au Comité économique et social européen.

Ce rapport porte en particulier sur:

a) l'application du paragraphe 1, deuxième alinéa, points a) et b);

b) la contribution du présent règlement à l'approfondissement et au fonctionnement efficace du marché intérieur des services intermédiaires, notamment en ce qui concerne la fourniture transfrontalière de services numériques;

c) l'application des articles 13, 16, 20, 21, 45 et 46;

d) la portée des obligations pesant sur les petites entreprises et les microentreprises;

e) l'efficacité des mécanismes de surveillance et d'exécution;

f) l'incidence sur le respect du droit à la liberté d'expression et d'information.

3. Le rapport visé aux paragraphes 1 et 2 est accompagné, le cas échéant, d'une proposition de modification du présent règlement.

4. La Commission évalue également, dans le rapport visé au paragraphe 2 du présent article, les rapports d'activité annuels des coordinateurs pour les services numériques présentés à la Commission et au comité au titre de l'article 55, paragraphe 1, et en rend compte dans ledit rapport.

5. Aux fins du paragraphe 2, les États membres et le comité fournissent à la Commission les informations qu'elle demande.

6. Lorsqu'elle procède aux évaluations visées au paragraphe 2, la Commission tient compte des positions et des conclusions du Parlement européen, du Conseil, et d'autres organismes ou sources pertinents et prête une attention particulière aux petites et moyennes entreprises et à la position de nouveaux concurrents.

7. Au plus tard le 18 février 2027, la Commission, après avoir consulté le comité, procède à une évaluation du fonctionnement du comité et de l'application de l'article 43, et elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du règlement. Sur la base des conclusions et en tenant le plus grand compte de l'avis du comité, le rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure du comité.

Article 92
Application anticipée à l'égard des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne

Le présent règlement s'applique aux fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne désignés en vertu de l'article 33, paragraphe 4, quatre mois après la notification adressée au fournisseur concerné visée à l'article 33, paragraphe 6, lorsque cette date est antérieure au 17 février 2024.

Article 93
Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.
2. Le présent règlement est applicable à partir du 17 février 2024.
Toutefois, l'article 24, paragraphes 2, 3 et 6, l'article 33, paragraphes 3 à 6, l'article 37, paragraphe 7, l'article 40, paragraphe 13, l'article 43 et le chapitre IV, sections 4, 5 et 6, sont applicables à partir du 16 novembre 2022.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 19 octobre 2022.

Par le Parlement européen La présidente
R. METSOLA

Par le Conseil Le président
M. BEK

DGA

DGA

RÈGLEMENT (UE) 2022/868 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 30 mai 2022

portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire[2],

considérant ce qui suit:

(1) Le traité sur le fonctionnement de l'Union européenne prévoit l'établissement d'un marché intérieur ainsi que l'instauration d'un régime garantissant que la concurrence sur le marché intérieur n'est pas faussée. La mise en place de règles et pratiques communes dans les États membres en ce qui concerne l'élaboration d'un cadre de gouvernance des données devrait contribuer à la réalisation de ces objectifs, dans le plein respect des droits fondamentaux. Elle devrait également garantir le renforcement de l'autonomie stratégique ouverte de l'Union tout en facilitant la libre circulation des données à l'échelle internationale.

(2) Au cours de la dernière décennie, les technologies numériques ont transformé l'économie et la société, touchant tous les secteurs d'activité et la vie quotidienne. Les données sont au cœur de cette transformation: l'innovation fondée sur les données apportera des avantages considérables aussi bien aux citoyens de l'Union qu'à l'économie, par exemple en améliorant et en personnalisant la médecine, en offrant une mobilité nouvelle et en contribuant à la communication de la Commission du 11 décembre 2019 sur le pacte vert pour l'Europe. Afin que l'économie fondée sur les données soit inclusive à l'égard de tous les citoyens de l'Union, il faut veiller tout particulièrement à réduire la fracture numérique, à encourager la participation des femmes à l'économie des données et à promouvoir une expertise européenne de pointe dans le secteur des technologies. L'économie des données doit être construite de manière à permettre aux entreprises, en particulier aux micro, petites et moyennes entreprises (PME), telles qu'elles sont définies à l'annexe de la recommandation 2003/361/CE de la Commission[3], et aux jeunes pousses de prospérer, en garantissant la neutralité de l'accès aux données ainsi que la portabilité et l'interopérabilité des données,

1. JO C 286 du 16.7.2021, p. 38.
2. Position du Parlement européen du 6 avril 2022 (non encore parue au Journal officiel) et décision du Conseil du 16 mai 2022.
3. Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

et en évitant les effets de verrouillage. Dans sa communication du 19 février 2020 sur une stratégie européenne pour les données (ci-après dénommée «stratégie européenne pour les données»), la Commission a décrit la vision qu'elle a d'un espace européen unique des données, à savoir un marché intérieur des données dans lequel les données pourraient être utilisées quel que soit leur lieu de stockage physique dans l'Union, conformément au droit applicable, et qui soit susceptible, entre autres, de jouer un rôle déterminant dans le développement rapide des technologies de l'intelligence artificielle.

La Commission a également plaidé en faveur de la libre circulation sécurisée des données avec les pays tiers, sous réserve des exceptions et des restrictions en matière de sécurité publique, d'ordre public et d'autres objectifs légitimes de politique publique de l'Union, conformément aux obligations internationales, y compris en ce qui concerne les droits fondamentaux. Afin que cette vision devienne réalité, la Commission a proposé de mettre en place des espaces européens communs de données spécifiques à certains domaines en vue du partage de données et de la mise en commun de données. Ainsi que le propose la stratégie européenne pour les données, ces espaces européens communs de données pourraient couvrir des domaines tels que la santé, la mobilité, l'industrie manufacturière, les services financiers, l'énergie ou l'agriculture, ou une combinaison de ces domaines, par exemple l'énergie et le climat, ainsi que des domaines thématiques tels que le pacte vert pour l'Europe, l'administration publique ou les compétences. Les espaces européens communs de données devraient rendre les données traçables, accessibles, interopérables et réutilisables (ci-après dénommé «principes FAIR pour les données»), tout en garantissant un niveau élevé de cybersécurité. Lorsqu'il existe des conditions de concurrence équitables dans l'économie des données, les entreprises se font concurrence sur la qualité des services, et non sur la quantité de données qu'elles contrôlent. Aux fins de la conception, de la création et du maintien de conditions de concurrence équitables dans l'économie des données, une gouvernance solide est nécessaire, à laquelle les parties prenantes concernées d'un espace européen commun de données doivent participer et dans laquelle elles doivent être représentées.

(3) Il est nécessaire d'améliorer les conditions du partage des données dans le marché intérieur, en créant un cadre harmonisé pour les échanges de données et en définissant un certain nombre d'exigences de base pour la gouvernance des données, en veillant tout particulièrement à faciliter la coopération entre les États membres. Le présent règlement devrait viser à développer davantage le marché intérieur numérique sans frontières ainsi qu'une société et une économie des données centrées sur l'humain, dignes de confiance et sûres. Le droit sectoriel de l'Union peut élaborer, adapter et proposer des éléments nouveaux et complémentaires, en fonction des spécificités du secteur, telles que les dispositions du droit de l'Union envisagées en ce qui concerne l'espace européen des données relatives à la santé et en ce qui concerne l'accès aux données relatives aux véhicules. En outre, certains secteurs de l'économie sont déjà réglementés par le droit sectoriel de l'Union, qui comprend des règles relatives au partage de données ou à l'accès aux données au niveau transfrontalier ou à l'échelle de l'Union, par exemple la directive 2011/24/UE du Parlement européen et du Conseil[4] dans le cadre de l'espace européen des données relatives à la santé, et les actes législatifs pertinents dans le domaine des transports, tels que les règlements (UE) 2019/1239[5] et (UE) 2020/1056[6] et la directive 2010/40/UE[7] du Parlement européen et du Conseil dans le cadre de l'espace européen des données relatives à la mobilité.

Le présent règlement devrait par conséquent être sans préjudice des règlements (CE) no 223/2009[8], (UE) 2018/858[9] et (UE) 2018/1807[10] ainsi que des directives 2000/31/CE[11], 2001/29/CE[12], 2004/48/CE[13], 2007/2/CE[14], 2010/40/UE, (UE) 2015/849[15],

4. Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
5. Règlement (UE) 2019/1239 du Parlement européen et du Conseil du 20 juin 2019 établissant un système de guichet unique maritime européen et abrogeant la directive 2010/65/UE (JO L 198 du 25.7.2019, p. 64).
6. Règlement (UE) 2020/1056 du Parlement européen et du Conseil du 15 juillet 2020 concernant les informations électroniques relatives au transport de marchandises (JO L 249 du 31.7.2020, p. 33).
7. Directive 2010/40/UE du parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).

(UE) 2016/943[16], (UE) 2017/1132[17], (UE) 2019/790[18] et (UE) 2019/1024[19] du Parlement européen et du Conseil et de toute autre disposition du droit sectoriel de l'Union qui régit l'accès aux données et la réutilisation des données. Le présent règlement devrait s'entendre sans préjudice du droit de l'Union et du droit national concernant l'accès aux données et l'utilisation des données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, ainsi qu'aux fins de la coopération internationale dans ce cadre.

Le présent règlement devrait s'entendre sans préjudice des compétences des États membres en ce qui concerne leurs activités relatives à la sécurité publique, à la défense et à la sécurité nationale. La réutilisation des données protégées à de telles fins et détenues par des organismes du secteur public, y compris les données issues des procédures de passation de marchés relevant du champ d'application de la directive 2009/81/CE du Parlement européen et du Conseil[20], ne devrait pas être couverte par le présent règlement. Il convient d'instaurer un régime horizontal pour la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public et pour la fourniture de services d'intermédiation de données et de services fondée sur l'altruisme en matière de données dans l'Union. Les caractéristiques spécifiques des différents secteurs peuvent rendre nécessaire la conception de systèmes sectoriels fondés sur les données, tout en s'appuyant sur les exigences posées par le présent règlement. Les prestataires de services d'intermédiation de données qui satisfont aux exigences fixées dans le présent règlement devraient pouvoir utiliser le label «prestataire de services d'intermédiation de données reconnu dans l'Union». Les personnes morales qui cherchent à promouvoir des objectifs d'intérêt général en mettant à disposition des données pertinentes sur le fondement de l'altruisme en matière de données à la bonne échelle et qui satisfont aux exigences fixées dans le présent règlement devraient pouvoir s'enregistrer en tant que «organisation altruiste en matière de données reconnue dans l'Union» et utiliser ce label. Lorsque le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public, à de tels prestataires de services d'intermédiation de données ou à de telles personnes morales (organisations altruistes en matière de données reconnues) de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, y compris au moyen d'un régime d'autorisation ou de certification, les dispositions du droit sectoriel de l'Union ou du droit sectoriel national devraient également s'appliquer.

(4) Le présent règlement devrait s'entendre sans préjudice des règlements (UE) 2016/679[21] et (UE) 2018/1725[22] du Parlement européen et du Conseil et des directives 2002/58/CE[23] et (UE) 2016/680[24] du Parlement européen et du Conseil et des dispositions correspondantes du droit national, y compris lorsque les données à caractère per-

8. Règlement (CE) no 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) no 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) no 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).
9. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).
10. Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (JO L 303 du 28.11.2018, p. 59).
11. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») (JO L 178 du 17.7.2000, p. 1).
12. Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO L 167 du 22.6.2001, p. 10).
13. Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle (JO L 157 du 30.4.2004, p. 45).
14. Directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE) (JO L 108 du 25.4.2007, p. 1).
15. Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) no 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (JO L 141 du 5.6.2015, p. 73).

sonnel et non personnel d'un ensemble de données sont inextricablement liées. En particulier, le présent règlement ne devrait pas être lu comme créant une nouvelle base juridique pour le traitement des données à caractère personnel dans le cadre de l'une des activités réglementées, ni comme modifiant les exigences en matière d'information prévues par le règlement (UE) 2016/679. La mise en œuvre du présent règlement ne devrait pas empêcher les transferts transfrontaliers de données conformément au chapitre V du règlement (UE) 2016/679. En cas de conflit entre le présent règlement et le droit de l'Union en matière de protection des données à caractère personnel ou le droit national adopté conformément audit droit de l'Union, le droit de l'Union ou le droit national applicable relatif à la protection des données à caractère personnel devrait prévaloir. Il devrait être possible de considérer les autorités chargées de la protection des données comme des autorités compétentes au titre du présent règlement. Lorsque d'autres autorités agissent comme autorités compétentes au titre du présent règlement, elles devraient agir sans préjudice des pouvoirs de surveillance et des compétences conférés aux autorités chargées de la protection des données au titre du règlement (UE) 2016/679.

Lien avec le RGPD : le DGA ne crée pas de nouvelle base juridique et ne modifie pas les exigences en matière d'information.
En cas de conflit entre le DGA et le droit de la protection des données personnelles, c'est ce dernier qui prévaut.

(5) Une action au niveau de l'Union est nécessaire pour accroître la confiance dans le partage des données en établissant des mécanismes appropriés permettant aux personnes concernées et aux détenteurs de données d'exercer un contrôle sur les données les concernant, et pour lever les autres obstacles au bon fonctionnement d'une économie fondée sur les données qui soit compétitive. Cette action devrait être sans préjudice des obligations et des engagements prévus dans les accords commerciaux internationaux conclus par l'Union. Un cadre de gouvernance à l'échelle de l'Union devrait avoir pour objectif d'instaurer la confiance entre les personnes physiques et les entreprises en ce qui concerne l'accès aux données, leur contrôle, leur partage, leur utilisation et leur réutilisation, en particulier en concevant des mécanismes appropriés permettant aux personnes concernées de connaître et d'exercer utilement leurs droits, ainsi qu'en ce qui concerne la réutilisation de certains types de données détenues par des organismes du secteur public, la fourniture de services aux personnes concernées, aux détenteurs de données et aux utilisateurs de données par les prestataires de services d'intermédiation de données, ainsi qu'en ce qui concerne la collecte et le traitement des données mises à disposition à des fins altruistes par des personnes physiques et morales. En particulier, une plus grande transparence en ce qui concerne la finalité de l'utilisation des données et les conditions dans lesquelles les données sont stockées par les entreprises peut contribuer à renforcer la confiance.

La CNIL et ses homologues ont vocation à être compétentes pour l'application du DGA.

(6) L'idée selon laquelle les données produites ou collectées par des organismes du secteur public ou d'autres entités aux frais des budgets publics devraient profiter à la société est depuis longtemps présente dans la politique de l'Union. La directive (UE) 2019/1024 et le droit sectoriel de l'Union garantissent que les organismes du secteur

16. Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).
17. Directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017 relative à certains aspects du droit des sociétés (JO L 169 du 30.6.2017, p. 46).
18. Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).
19. Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (JO L 172 du 26.6.2019, p. 56).
20. Directive 2009/81/CE du Parlement européen et du Conseil du 13 juillet 2009 relative à la coordination des procédures de passation de certains marchés de travaux, de fournitures et de services par des pouvoirs adjudicateurs ou entités adjudicatrices dans les domaines de la défense et de la sécurité, et modifiant les directives 2004/17/CE et 2004/18/CE (JO L 216 du 20.8.2009, p. 76).
21. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).
22. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).
23. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

public rendent facilement accessibles un volume accru des données qu'ils produisent, à des fins d'utilisation et de réutilisation. Toutefois, il arrive souvent que certaines catégories de données, telles que les données commerciales confidentielles, les données couvertes par le secret statistique et les données protégées par des droits de propriété intellectuelle détenus par des tiers, y compris les secrets d'affaires et les données à caractère personnel, figurant dans des bases de données publiques ne soient pas rendues accessibles, même pour des activités de recherche ou d'innovation relevant de l'intérêt public, bien que cette disponibilité soit possible en vertu du droit de l'Union en vigueur, notamment le règlement (UE) 2016/679 et les directives 2002/58/CE et (UE) 2016/680. En raison du caractère sensible de ces données, certaines exigences procédurales de nature technique et juridique doivent être satisfaites avant leur mise à disposition, en particulier afin de garantir le respect des droits que d'autres personnes détiennent sur ces données ou de limiter les répercussions négatives sur les droits fondamentaux, le principe de non-discrimination et la protection des données. Satisfaire à ces exigences nécessite généralement beaucoup de temps et des connaissances pointues. Cela a conduit à une utilisation insuffisante de ces données. Si certains États membres mettent en place des structures, des processus ou des législations pour faciliter ce type de réutilisation, ce n'est pas le cas dans l'ensemble de l'Union. Afin de faciliter l'utilisation des données par les entités privées et publiques dans le cadre de la recherche et de l'innovation en Europe, il est nécessaire de fixer des conditions claires pour l'accès à ces données et leur utilisation dans l'ensemble de l'Union.

cf. RGPD.

(7) Il existe des techniques permettant d'effectuer des analyses dans les bases de données contenant des données à caractère personnel, notamment l'anonymisation, la confidentialité différentielle, la généralisation, la suppression et la randomisation, l'utilisation de données synthétiques ou des méthodes similaires, et d'autres méthodes de préservation de la vie privée à la pointe de la technologie, qui pourraient contribuer à un traitement des données plus respectueux de la vie privée. Les États membres devraient aider les organismes du secteur public à exploiter au mieux ces techniques et à mettre ainsi à disposition un maximum de données à partager. L'application de ces techniques, ainsi que d'analyses d'impact globales en matière de protection des données et d'autres garanties, peut contribuer à une plus grande sécurité dans l'utilisation et la réutilisation des données à caractère personnel et devrait garantir la réutilisation sûre des données commerciales confidentielles à des fins de recherche, d'innovation et de statistiques. Dans de nombreux cas, l'application de ces techniques, analyses d'impact et autres garanties suppose que les données ne peuvent être utilisées et réutilisées que dans un environnement de traitement sécurisé qui est fourni ou contrôlé par l'organisme du secteur public. Il existe, au niveau de l'Union, une certaine expérience de tels environnements de traitement sécurisés, qui sont utilisés pour la recherche sur les microdonnées statistiques sur le fondement du règlement (UE) no 557/2013 de la Commission[25]. D'une manière générale, dans la mesure où des données à caractère personnel sont concernées, le traitement de telles données devrait se fonder sur une ou plusieurs des bases légales relatives au traitement prévues aux articles 6 et 9 du règlement (UE) 2016/679.

cf. RGPD : bases légales.

(8) Conformément au règlement (UE) 2016/679, il n'y a pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. La réidentification des personnes concernées à partir d'ensembles de données anonymisées devrait être interdite. Cette interdiction ne devrait pas porter atteinte à la possibilité de mener des recherches sur des techniques d'anonymisation, en particulier en vue de garantir la sécurité des informations, de renforcer les techniques d'anonymisation existantes et de contribuer à la fiabilité générale de l'anonymisation, en conformité avec le règlement (UE) 2016/679.

cf. RGPD : cas des données anonymes.

cf. RGPD : anonymisation.

24. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

25. Règlement (UE) no 557/2013 de la Commission du 17 juin 2013 mettant en œuvre le règlement (CE) no 223/2009 du Parlement européen et du Conseil relatif aux statistiques européennes en ce qui concerne l'accès aux données confidentielles à des fins scientifiques et abrogeant le règlement (CE) no 831/2002 de la Commission (JO L 164 du 18.6.2013, p. 16).

(9) Afin de faciliter la protection des données à caractère personnel et des données confidentielles et d'accélérer le processus de mise à disposition de ces données en vue de leur réutilisation au titre du présent règlement, les États membres devraient encourager les organismes du secteur public à créer et à mettre à disposition des données conformément au principe d'«ouverture dès la conception et par défaut» visé à l'article 5, paragraphe 2, de la directive (UE) 2019/1024, ainsi qu'à promouvoir la création et l'acquisition de données selon des formats et des structures qui facilitent l'anonymisation à cet égard.

(10) Les catégories de données détenues par des organismes du secteur public qui devraient faire l'objet d'une réutilisation en vertu du présent règlement ne relèvent pas du champ d'application de la directive (UE) 2019/1024, qui exclut les données qui ne sont pas accessibles pour des raisons de confidentialité commerciale ou de secret statistique et les données contenues dans des œuvres ou autres objets pour lesquels des tiers détiennent les droits de propriété intellectuelle. Les données commerciales confidentielles comprennent les données protégées par le secret d'affaires, le savoir-faire protégé et toute autre information dont la divulgation abusive aurait une incidence sur la position sur le marché ou la santé financière de l'entreprise. Le présent règlement devrait s'appliquer aux données à caractère personnel qui ne relèvent pas du champ d'application de la directive (UE) 2019/1024 dans la mesure où les règles d'accès excluent ou limitent l'accès à ces données pour des motifs de protection des données, de protection de la vie privée et d'intégrité de la personne physique, en particulier au regard des règles relatives à la protection des données. La réutilisation de données susceptibles de contenir des secrets d'affaires devrait se faire sans préjudice de la directive (UE) 2016/943, qui fixe le cadre pour l'obtention, l'utilisation ou la divulgation licites des secrets d'affaires.

(11) Le présent règlement ne devrait pas créer une obligation d'autoriser la réutilisation des données détenues par les organismes du secteur public. En particulier, chaque État membre devrait par conséquent pouvoir décider si les données sont rendues accessibles à des fins de réutilisation, y compris en ce qui concerne les finalités et la portée de cet accès. Le présent règlement devrait compléter les obligations plus spécifiques que le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public pour autoriser la réutilisation de données, et il devrait être sans préjudice de ces obligations. L'accès du public aux documents officiels peut être considéré comme étant dans l'intérêt public. Compte tenu du rôle joué par l'accès du public aux documents officiels et par la transparence dans une société démocratique, le présent règlement devrait également être sans préjudice du droit de l'Union ou du droit national relatif à l'octroi de l'accès aux documents officiels et à leur divulgation. L'accès aux documents officiels peut notamment être octroyé conformément au droit national sans imposer de conditions spécifiques ou en imposant des conditions spécifiques qui ne sont pas prévues par le présent règlement.

(12) Le régime de réutilisation prévu par le présent règlement devrait s'appliquer aux données dont la fourniture est une activité qui relève des missions de service public dévolues aux organismes du secteur public concernés en vertu de la loi ou d'autres règles contraignantes en vigueur dans les États membres. En l'absence de telles règles, les missions de service public devraient être définies conformément aux pratiques administratives courantes dans les États membres, sous réserve que l'objet de ces missions soit transparent et soumis à réexamen. Les missions de service public pourraient être définies à titre général ou au cas par cas pour les différents organismes du secteur public. Étant donné que les entreprises publiques ne sont pas couvertes par la définition d'organisme du secteur public, les données que détiennent les entreprises publiques ne devraient pas être couvertes par le présent règlement. Les données détenues par des établissements culturels, tels que les bibliothèques, les archives et les musées ainsi que les orchestres, les opéras, les ballets et les théâtres, et par des établissements d'enseignement ne devraient pas être couvertes par le présent règlement puisque les œuvres et autres documents que détiennent ces établissements sont principalement couverts par des droits de propriété intellectuelle détenus par des tiers. Les organismes exerçant une activité de recherche et les organisations finançant une activité de recherche pourraient aussi être organisés comme des organismes du secteur public ou des organismes de droit public.

Le présent règlement devrait s'appliquer à ces organismes hybrides uniquement en leur qualité d'organismes exerçant une activité de recherche. Si un organisme exerçant une activité de recherche détient des données dans le cadre d'une association public-

privé spécifique avec des organismes du secteur privé ou d'autres organismes du secteur public, des organismes de droit public ou des organismes hybrides exerçant une activité de recherche, c'est-à-dire organisés soit en tant qu'organismes du secteur public soit en tant qu'entreprises publiques, dans le but principal d'effectuer des recherches, ces données ne devraient pas non plus être couvertes par le présent règlement. Le cas échéant, les États membres devraient pouvoir appliquer le présent règlement aux entreprises publiques ou aux entreprises privées qui exercent des fonctions du secteur public ou fournissent des services d'intérêt général. L'échange de données, effectué exclusivement dans le cadre de leurs missions de service public, entre des organismes du secteur public dans l'Union ou entre des organismes du secteur public dans l'Union et des organismes du secteur public dans des pays tiers ou des organisations internationales, ainsi que l'échange de données entre chercheurs à des fins de recherche scientifique non commerciale, ne devraient pas être soumis aux dispositions du présent règlement concernant la réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public.

(13) Les organismes du secteur public devraient respecter le droit de la concurrence lorsqu'ils établissent les principes régissant la réutilisation des données qu'ils détiennent, en évitant la conclusion d'accords qui pourraient avoir pour objet ou pour effet de créer des droits d'exclusivité pour la réutilisation de certaines données. De tels accords ne devraient être possibles que lorsque cela est justifié et nécessaire en vue de la fourniture d'un service ou d'un produit dans l'intérêt général. Tel peut être le cas lorsque l'utilisation exclusive des données est le seul moyen de maximiser les avantages sociétaux des données en question, par exemple lorsqu'il n'existe qu'une seule entité (spécialisée dans le traitement d'un ensemble de données particulier) capable de fournir le service ou le produit permettant à l'organisme du secteur public de fournir un service ou un produit dans l'intérêt général. De tels accords devraient toutefois être conclus conformément au droit de l'Union ou au droit national applicable et pouvoir faire l'objet d'un réexamen régulier sur la base d'une analyse de marché, afin de déterminer si cette exclusivité reste nécessaire. En outre, ces accords devraient respecter les règles applicables en matière d'aides d'État, le cas échéant, et être conclus pour une durée limitée qui ne devrait pas dépasser douze mois. Dans un souci de transparence, ces accords d'exclusivité devraient être publiés en ligne, sous une forme conforme au droit de l'Union applicable en matière de marchés publics. Lorsqu'un droit d'exclusivité pour la réutilisation des données ne respecte pas le présent règlement, il ne devrait pas être valide.

(14) Lorsqu'ils ont été conclus ou étaient déjà en place avant la date d'entrée en vigueur du présent règlement, les accords d'exclusivité interdits et les autres pratiques ou arrangements portant sur la réutilisation des données détenues par des organismes du secteur public qui ne confèrent pas expressément de droits d'exclusivité mais dont on peut raisonnablement s'attendre à ce qu'ils restreignent la disponibilité des données à des fins de réutilisation ne devraient pas être renouvelés à leur terme. Dans le cas d'accords à durée indéterminée ou à long terme, la résiliation devrait intervenir dans un délai de trente mois à compter de la date d'entrée en vigueur du présent règlement.

(15) Il convient que le présent règlement fixe les conditions de réutilisation des données protégées qui s'appliquent aux organismes du secteur public désignés comme compétents en vertu du droit national pour octroyer ou refuser l'accès à des fins de réutilisation, et qui s'entendent sans préjudice des droits ou obligations concernant l'accès à ces données. Ces conditions devraient être non discriminatoires, transparentes, proportionnées et objectivement justifiées, sans restreindre la concurrence, l'accent étant mis sur la promotion de l'accès à ces données par les PME et les jeunes pousses. Les conditions de réutilisation devraient être conçues de manière à promouvoir la recherche scientifique afin que, par exemple, le fait de privilégier la recherche scientifique puisse en principe être considéré comme non discriminatoire. Les organismes du secteur public autorisant la réutilisation devraient disposer des moyens techniques nécessaires pour assurer la protection des droits et intérêts des tiers et être habilités à demander les informations nécessaires au réutilisateur. Les conditions liées à la réutilisation des données devraient être limitées à ce qui est nécessaire pour préserver les droits et intérêts des tiers à l'égard des données, ainsi que l'intégrité des systèmes d'information et de communication des organismes du secteur public. Ces derniers devraient appliquer des conditions qui servent au mieux les intérêts du réutilisateur sans entraîner de charge disproportionnée pour les organismes du secteur public. Les conditions liées à la réutilisation des données devraient être conçues de manière à offrir des garanties efficaces en matière de protection des données à carac-

tère personnel. Avant leur transmission, les données à caractère personnel devraient être anonymisées, afin d'empêcher l'identification des personnes concernées, et les données contenant des informations commerciales confidentielles devraient être modifiées de telle sorte qu'aucune information confidentielle ne soit divulguée. Dans le cas où la fourniture de données anonymisées ou modifiées ne permettrait pas de répondre aux besoins du réutilisateur, sous réserve de satisfaire à toutes les exigences découlant des articles 35 et 36 du règlement (UE) 2016/679 qui imposent d'effectuer une analyse d'impact relative à la protection des données et de consulter l'autorité de contrôle, et lorsqu'il a été constaté que les risques pour les droits et les intérêts des personnes concernées sont minimes, la réutilisation des données dans un environnement de traitement sécurisé, sur place ou à distance, pourrait être autorisée.

cf. RGPD : cas où une AIPD est nécessaire.

Il pourrait s'agir d'un arrangement approprié pour la réutilisation des données pseudonymisées. Les analyses de données dans ces environnements de traitement sécurisés devraient être supervisées par l'organisme du secteur public, afin de protéger les droits et intérêts des tiers. En particulier, des données à caractère personnel ne devraient être transmises à un tiers à des fins de réutilisation que lorsqu'une base juridique au titre du droit sur la protection des données autorise une telle transmission. Les données à caractère non personnel ne devraient être transmises que lorsqu'il n'y a aucune raison de penser que la combinaison d'ensembles de données à caractère non personnel conduirait à l'identification des personnes concernées. Cela devrait également s'appliquer aux données pseudonymisées qui conservent leur statut de données à caractère personnel. En cas de réidentification de personnes concernées, une obligation de notifier une telle violation de données à l'organisme du secteur public devrait s'appliquer en plus d'une obligation de notifier cette violation de données à une autorité de contrôle et à la personne concernée conformément au règlement (UE) 2016/679. Le cas échéant, les organismes du secteur public devraient faciliter la réutilisation des données fondée sur le consentement des personnes concernées ou l'autorisation des détenteurs de données quant à la réutilisation des données les concernant, par des moyens techniques appropriés. À cet égard, l'organisme du secteur public devrait tout mettre en oeuvre pour aider les réutilisateurs potentiels à solliciter un tel consentement ou une telle autorisation, en mettant en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation émanant des réutilisateurs, lorsque cela est réalisable en pratique. Les coordonnées permettant aux utilisateurs de prendre directement contact avec les personnes concernées ou les détenteurs de données ne devraient pas être communiquées. Lorsque l'organisme du secteur public transmet une demande de consentement ou d'autorisation, il devrait veiller à ce que la personne concernée ou le détenteur de données soit clairement informé de la possibilité de refuser de donner son consentement ou son autorisation.

cf. RGPD : notification de violation en cas de réidentification.

(16) Afin de faciliter et d'encourager l'utilisation des données détenues par des organismes du secteur public à des fins de recherche scientifique, ces organismes sont encouragés à élaborer une approche harmonisée et des procédures harmonisées pour rendre ces données facilement accessibles aux fins de la recherche scientifique dans l'intérêt public. Il pourrait s'agir, entre autres, de mettre en place des procédures administratives rationalisées, des formats de données normalisés, des métadonnées informatives sur les choix méthodologiques et les choix en matière de collecte de données, ainsi que des champs de données normalisés qui permettent de chainer aisément des ensembles de données provenant de différentes sources de données du secteur public, lorsque cela est pertinent à des fins d'analyse. L'objectif de ces pratiques devrait être de promouvoir des données financées et produites par les pouvoirs publics à des fins de recherche scientifique, conformément au principe «aussi ouvert que possible, aussi fermé que nécessaire».

(17) Le présent règlement ne devrait pas porter atteinte aux droits de propriété intellectuelle détenus par des tiers. Le présent règlement ne devrait pas non plus porter atteinte à l'existence des droits de propriété intellectuelle des organismes du secteur public ou à la qualité de titulaires de droits de propriété intellectuelle de ces organismes, de même qu'il ne devrait restreindre en aucune manière l'exercice de ces droits. Les obligations imposées conformément au présent règlement ne devraient s'appliquer que dans la mesure où elles sont compatibles avec les accords internationaux sur la protection des droits de propriété intellectuelle, notamment la convention de Berne pour la protection des œuvres littéraires et artistiques (convention de Berne), l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord sur les ADPIC) et le traité de l'Organisation mondiale de la propriété intellectuelle sur le droit d'auteur (WCT), ainsi qu'avec le droit de la propriété intellectuelle

de l'Union ou national. Les organismes du secteur public devraient, toutefois, exercer leurs droits d'auteur d'une manière qui facilite la réutilisation des données.

(18) Les données faisant l'objet de droits de propriété intellectuelle ainsi que les secrets d'affaires ne devraient être transmis à un tiers que si cette transmission est licite en vertu du droit de l'Union ou du droit national ou avec l'accord du titulaire des droits. Lorsque les organismes du secteur public sont titulaires du droit du fabricant d'une base de données prévu à l'article 7, paragraphe 1, de la directive 96/9/CE du Parlement européen et du Conseil[26], ils ne devraient pas exercer ce droit dans le but de prévenir la réutilisation de données ou de restreindre la réutilisation au-delà des limites fixées par le présent règlement.

(19) Les entreprises et les personnes concernées devraient pouvoir avoir la certitude que la réutilisation de certaines catégories de données protégées qui sont détenues par les organismes du secteur public se fera dans le respect de leurs droits et intérêts. Des garanties supplémentaires devraient dès lors être mises en place pour les situations dans lesquelles la réutilisation de telles données du secteur public a lieu sur la base d'un traitement des données en dehors du secteur public, comme l'obligation pour les organismes du secteur public de veiller à ce que les droits et intérêts des personnes physiques et morales soient pleinement protégés, en particulier en ce qui concerne les données à caractère personnel, les données commercialement sensibles et les droits de propriété intellectuelle, dans tous les cas, y compris lorsque ces données sont transférées vers des pays tiers. Les organismes du secteur public ne devraient pas autoriser la réutilisation des informations stockées dans les applications de santé en ligne par des entreprises d'assurance ou tout autre prestataire de services à des fins de discrimination dans la fixation des prix, car cela irait à l'encontre du droit fondamental d'accès aux soins de santé.

(20) En outre, afin de préserver une concurrence loyale et une économie de marché ouverte, il est de la plus haute importance de préserver les données protégées à caractère non personnel, en particulier les secrets d'affaires, mais aussi les données à caractère non personnel représentant des contenus protégés par des droits de propriété intellectuelle, contre tout accès illicite susceptible de conduire à un vol de propriété intellectuelle ou à de l'espionnage industriel. Afin de garantir la protection des droits ou des intérêts des détenteurs de données, il devrait être possible de transférer les données à caractère non personnel qui doivent être protégées contre un accès illicite ou non autorisé conformément au droit de l'Union ou au droit national et qui sont détenues par des organismes du secteur public vers des pays tiers, mais uniquement lorsque des garanties appropriées sont prévues pour l'utilisation des données. Parmi ces garanties appropriées devrait figurer l'obligation pour l'organisme du secteur public de ne transmettre des données protégées à un réutilisateur que si ledit réutilisateur prend des engagements contractuels dans l'intérêt de la protection des données. Un réutilisateur ayant l'intention de transférer les données protégées vers un pays tiers devrait respecter les obligations prévues dans le présent règlement, même après le transfert des données vers le pays tiers. Afin de garantir la bonne exécution de ces obligations, le réutilisateur devrait également admettre, pour le règlement judiciaire des litiges, la compétence de l'État membre de l'organisme du secteur public qui a autorisé la réutilisation.

(21) La mise en place de garanties appropriées devrait également être envisagée lorsque, dans le pays tiers vers lequel des données à caractère non personnel sont transférées, il existe des mesures équivalentes garantissant que les données bénéficient d'un niveau de protection similaire à celui qui est applicable en vertu du droit de l'Union, notamment en ce qui concerne la protection des secrets d'affaires et les droits de propriété intellectuelle. À cette fin, la Commission devrait pouvoir déclarer, par voie d'actes d'exécution, lorsque cela est justifié en raison d'un grand nombre de demandes dans l'ensemble de l'Union concernant la réutilisation de données à caractère non personnel dans des pays tiers déterminés, qu'un pays tiers offre un niveau de protection essentiellement équivalent à celui prévu par le droit de l'Union. La Commission devrait évaluer la nécessité de tels actes d'exécution sur la base des informations fournies par les États membres par l'intermédiaire du comité européen de l'innovation dans le domaine des données. De tels actes d'exécution permettraient de

26. Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données (JO L 77 du 27.3.1996, p. 20).

garantir aux organismes du secteur public que la réutilisation, dans le pays tiers concerné, de données détenues par les organismes du secteur public ne risque pas de compromettre la nature protégée de ces données. Pour évaluer le niveau de protection offert dans le pays tiers concerné, il convient en particulier de prendre en considération le droit général et sectoriel applicable, y compris en matière de sécurité publique, de défense, de sécurité nationale et de droit pénal, en ce qui concerne l'accès aux données à caractère non personnel et à leur protection, tout accès par les organismes du secteur public de ce pays tiers aux données transférées, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes qui sont chargées dans le pays tiers de veiller au respect du régime juridique garantissant l'accès à ces données et de le faire appliquer, les engagements internationaux pris par le pays tiers concerné en ce qui concerne la protection des données, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de la participation à des systèmes multilatéraux ou régionaux.

L'existence de voies de droit effectives pour les détenteurs de données, les organismes du secteur public ou les prestataires de services d'intermédiation de données dans le pays tiers concerné revêt une importance particulière dans le contexte du transfert de données à caractère non personnel vers ce pays tiers. Ces garanties devraient donc inclure l'existence de droits opposables et de voies de droit effectives. Ces actes d'exécution devraient être sans préjudice de toute obligation juridique déjà contractée ou de tout arrangement contractuel déjà pris par un réutilisateur dans l'intérêt de la protection des données à caractère non personnel, en particulier des données industrielles, et du droit des organismes du secteur public d'obliger les réutilisateurs à respecter les conditions de réutilisation, conformément au présent règlement.

(22) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à transférer directement des données à caractère non personnel dans l'Union, ou à donner aux pouvoirs publics l'accès à de telles données, sous le contrôle de personnes physiques et morales relevant de la juridiction des États membres. Les décisions de juridictions de pays tiers ou les décisions d'autorités administratives de pays tiers qui exigent un tel transfert de données à caractère non personnel ou un accès à de telles données devraient être exécutoires lorsqu'elles sont fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. Dans certains cas, il peut arriver que l'obligation, découlant du droit d'un pays tiers, de transférer des données à caractère non personnel ou de donner accès à de telles données soit incompatible avec une obligation concurrente de protéger ces données en vertu du droit de l'Union ou du droit national, en particulier en ce qui concerne la protection des droits fondamentaux des personnes physiques ou des intérêts fondamentaux d'un État membre en matière de sécurité nationale ou de défense, ainsi que la protection des données commercialement sensibles et la protection des droits de propriété intellectuelle, y compris les engagements contractuels pris en matière de confidentialité conformément à ce droit. En l'absence d'accords internationaux régissant ces questions, il convient de n'autoriser le transfert de données à caractère non personnel ou l'accès à de telles données que si, en particulier, il a été vérifié que le système juridique du pays tiers exige que les motifs et la proportionnalité de la décision judiciaire ou administrative soient exposés, que la décision judiciaire ou administrative a un caractère spécifique et que l'objection motivée du destinataire peut faire l'objet d'un réexamen dans le pays tiers par une juridiction compétente habilitée à tenir dûment compte des intérêts juridiques pertinents du fournisseur de ces données.

En outre, les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues devraient veiller, lorsqu'ils signent des accords contractuels avec d'autres parties privées, à ce que les données à caractère non personnel détenues dans l'Union ne soient accessibles dans des pays tiers ou transférées vers des pays tiers que conformément au droit de l'Union ou au droit national de l'État membre concerné.

(23) Pour renforcer la confiance dans l'économie des données de l'Union, il est essentiel de veiller à ce que les garanties permettant aux citoyens, au secteur public et aux entreprises de l'Union d'exercer un contrôle sur leurs données stratégiques et sensibles soient appliquées, et à ce que le droit, les valeurs et les normes de l'Union en matière, entre autres, de sécurité, de protection des données et de protection des consommateurs, soient respectés. Afin d'empêcher un accès illicite à des données à caractère non

personnel, les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues devraient prendre toutes les mesures raisonnables pour empêcher l'accès aux systèmes dans lesquels des données à caractère non personnel sont stockées, y compris le cryptage des données ou des politiques internes. À cette fin, il convient de veiller à ce que les organismes du secteur public, les personnes physiques ou morales auxquelles le droit de réutilisation des données a été accordé, les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues respectent l'ensemble des normes techniques, codes de conduite et certifications pertinents au niveau de l'Union.

(24) Afin de développer la confiance dans les mécanismes de réutilisation, il peut être nécessaire d'assortir de conditions plus strictes certains types de données à caractère non personnel dont le caractère hautement sensible peut être reconnu dans des actes législatifs spécifiques futurs de l'Union, en ce qui concerne le transfert vers des pays tiers, si un tel transfert risque de compromettre des objectifs de politique publique de l'Union, conformément aux engagements internationaux. Par exemple, dans le domaine de la santé, certains ensembles de données détenus par des acteurs du système de santé publique, tels que les hôpitaux publics, pourraient être reconnus comme des données relatives à la santé hautement sensibles. Parmi les autres secteurs concernés figurent les transports, l'énergie, l'environnement et la finance. Afin de garantir l'harmonisation des pratiques dans l'ensemble de l'Union, ces types de données publiques à caractère non personnel hautement sensibles devraient être définis par le droit de l'Union, par exemple dans le cadre de l'espace européen des données relatives à la santé ou d'autres dispositions du droit sectoriel. Ces conditions liées au transfert de telles données vers des pays tiers devraient être fixées dans des actes délégués. Elles devraient être proportionnées, non discriminatoires et nécessaires pour protéger des objectifs légitimes de politique publique de l'Union déterminés, tels que la protection de la santé publique, la sécurité, l'environnement, la moralité publique, la protection des consommateurs, la protection de la vie privée et la protection des données à caractère personnel. Les conditions devraient correspondre aux risques mis en évidence en ce qui concerne la sensibilité de ces données, y compris le risque de réidentification des personnes physiques. Ces conditions pourraient comprendre des conditions applicables au transfert ou des arrangements techniques, tels que l'obligation d'utiliser un environnement de traitement sécurisé, des limitations en ce qui concerne la réutilisation des données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou pouvant y avoir accès dans des pays tiers. Dans des cas exceptionnels, ces conditions pourraient également inclure des restrictions au transfert des données vers des pays tiers afin de protéger l'intérêt public.

Organismes du secteur public.

(25) Les organismes du secteur public devraient avoir la possibilité de percevoir des redevances pour la réutilisation des données, mais aussi d'autoriser la réutilisation de ces données moyennant le paiement d'une redevance réduite ou gratuitement, par exemple pour certaines catégories de réutilisation telles que la réutilisation à des fins non commerciales ou à des fins de recherche scientifique, ou la réutilisation par les PME et les jeunes pousses, la société civile et les établissements d'enseignement, de manière à inciter à cette réutilisation pour stimuler la recherche et l'innovation et soutenir des entreprises qui représentent une source importante d'innovation et ont généralement plus de difficultés à collecter elles-mêmes des données pertinentes, conformément aux règles en matière d'aides d'État. Dans ce contexte spécifique, les finalités liées à la recherche scientifique devraient s'entendre comme incluant tout type d'objectif en rapport avec la recherche, quelle que soit la structure organisationnelle ou financière de l'organisme de recherche concerné, à l'exception de la recherche menée par une entreprise ayant pour but la mise au point, l'amélioration ou l'optimisation de produits ou de services. Ces redevances devraient être transparentes, non discriminatoires et limitées aux coûts nécessaires supportés et ne devraient pas restreindre la concurrence. Il convient de rendre publique une liste des catégories de réutilisateurs pour lesquels des redevances réduites ou nulles s'appliquent, assortie des critères utilisés pour établir cette liste.

Point d'information unique.

(26) Afin d'inciter à la réutilisation de ces catégories de données spécifiques détenues par des organismes du secteur public, les États membres devraient créer un point d'information unique servant d'interface pour les réutilisateurs qui souhaitent réutiliser ces données. Ses attributions devraient s'étendre à plusieurs secteurs et compléter,

si nécessaire, les dispositions prises au niveau sectoriel. Le point d'information unique devrait pouvoir s'appuyer sur des moyens automatisés lorsqu'il transmet des demandes d'information ou des demandes de réutilisation. Un contrôle humain suffisant devrait être assuré pendant le processus de transmission. À cette fin, les modalités pratiques existantes, telles que les portails des données ouvertes, pourraient être utilisées. Le point d'information unique devrait disposer d'une liste de ressources comprenant un aperçu de toutes les ressources en données disponibles, y compris, le cas échéant, les ressources en données qui sont disponibles dans les points d'information sectoriels, régionaux ou locaux, ainsi que les informations pertinentes décrivant les données disponibles. En outre, les États membres devraient désigner, établir ou contribuer à établir des organismes compétents pour soutenir les activités des organismes du secteur public autorisant la réutilisation de certaines catégories de données protégées. L'une des tâches qui leur sont confiées peut être d'octroyer l'accès aux données, lorsque le droit sectoriel de l'Union ou le droit sectoriel national l'exige. Ces organismes compétents devraient fournir une assistance aux organismes du secteur public en recourant à des techniques de pointe, notamment en ce qui concerne la meilleure manière de structurer et de stocker les données en vue de les rendre facilement accessibles, en particulier au moyen d'interfaces de programmation d'applications, et de rendre les données interopérables, transférables et interrogeables, en tenant compte des meilleures pratiques en matière de traitement des données et de toutes les normes réglementaires et techniques existantes ainsi que des environnements sécurisés pour le traitement des données, qui permettent l'analyse des données d'une manière qui préserve le caractère privé des informations.

Les organismes compétents devraient agir conformément aux instructions reçues de l'organisme du secteur public. Une telle structure d'assistance pourrait aider les personnes concernées et les détenteurs de données dans la gestion du consentement ou de l'autorisation de réutilisation, y compris en ce qui concerne le consentement et l'autorisation relatifs à certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les organismes compétents ne devraient pas avoir de fonction de contrôle, celle-ci étant réservée aux autorités de contrôle au titre du règlement (UE) 2016/679. Sans préjudice des pouvoirs de contrôle conférés aux autorités chargées de la protection des données, le traitement des données devrait être réalisé sous la responsabilité de l'organisme du secteur public responsable du registre contenant les données, qui reste un responsable du traitement des données tel qu'il est défini dans le règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel. Les États membres devraient pouvoir se doter d'un ou de plusieurs organismes compétents, qui pourraient agir dans différents secteurs. Les services internes des organismes du secteur public pourraient également faire office d'organismes compétents. Un organisme compétent pourrait être un organisme du secteur public qui aide d'autres organismes du secteur public à autoriser la réutilisation de données, le cas échéant, ou un organisme du secteur public autorisant lui-même la réutilisation. L'assistance apportée à d'autres organismes du secteur public devrait impliquer de les informer, sur demande, des meilleures pratiques concernant la manière de satisfaire aux exigences prévues par le présent règlement, par exemple en ce qui concerne les moyens techniques permettant de mettre à disposition un environnement de traitement sécurisé ou de garantir le respect de la vie privée et la confidentialité lorsqu'un accès est donné pour la réutilisation des données relevant du champ d'application du présent règlement.

cf. RGPD : fonction de contrôle réservée aux autorités de contrôle.

Services d'intermédiation de données.

(27) Les services d'intermédiation de données sont appelés à jouer un rôle essentiel dans l'économie des données, notamment en soutenant et en promouvant les pratiques volontaires de partage de données entre les entreprises, ou en facilitant le partage de données dans le cadre des obligations fixées par le droit de l'Union ou le droit national. Ils pourraient devenir un outil facilitant l'échange de quantités substantielles de données pertinentes. Les prestataires de services d'intermédiation de données, lesquels peuvent comprendre des organismes du secteur public, qui proposent des services mettant en relation les différents acteurs contribuent potentiellement à la mise en commun efficace des données ainsi qu'à la facilitation du partage bilatéral des données. Les services d'intermédiation de données spécialisés qui sont indépendants des personnes concernées, des détenteurs de données et des utilisateurs de données pourraient jouer un rôle de facilitation dans l'émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché, tout en permettant un accès non discriminatoire à l'économie des données pour les entreprises de toutes tailles, notamment les PME et les jeunes pousses disposant de moyens financiers, juridiques ou administratifs limités. Cela revêtira une

importance particulière dans la perspective de la création d'espaces européens communs de données, c'est-à-dire de cadres interopérables spécifiques à chaque finalité ou à chaque secteur ou transsectoriels de normes et de pratiques communes visant à partager ou à traiter conjointement des données aux fins, entre autres, de la mise au point de nouveaux produits et services, de la recherche scientifique ou d'initiatives de la société civile. Les services d'intermédiation de données pourraient inclure le partage bilatéral ou multilatéral de données ou la création de plateformes ou de bases de données permettant l'échange ou l'exploitation conjointe de données, ainsi que la mise en place d'une infrastructure spécifique pour l'interconnexion des personnes concernées et des détenteurs de données avec les utilisateurs de données.

(28) Le présent règlement devrait concerner les services qui visent à établir, par des moyens techniques, juridiques ou autres, des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et des utilisateurs de données, d'autre part, y compris aux fins de l'exercice des droits des personnes concernées à l'égard des données à caractère personnel. Lorsque des entreprises ou autres entités proposent de multiples services liés aux données, seules les activités qui concernent directement la fourniture de services d'intermédiation de données devraient être couvertes par le présent règlement. La fourniture de services de stockage en nuage, d'analyse, de logiciels de partage de données, de navigateurs internet, de modules d'extension de navigateurs ou de services de messagerie électronique ne devrait pas être considérée comme une fourniture de services d'intermédiation de données au sens du présent règlement, à condition que ces services ne fournissent que des outils techniques permettant aux personnes concernées ou aux détenteurs de données de partager des données avec d'autres personnes, mais que la fourniture de tels outils ne vise ni à établir une relation commerciale entre les détenteurs de données et les utilisateurs de données, ni à permettre au prestataire de services d'intermédiation de données d'obtenir des informations sur l'établissement de relations commerciales à des fins de partage de données. Parmi les exemples de services d'intermédiation de données figurent les places de marché de données sur lesquelles les entreprises pourraient mettre des données à la disposition de tiers, les maîtres d'œuvre d'écosystèmes de partage de données ouverts à toutes les parties intéressées, par exemple dans le cadre d'espaces européens communs de données, ainsi que les réserves de données mises en place conjointement par plusieurs personnes morales ou physiques dans le but de concéder à toutes les parties intéressées des licences d'utilisation de ces réserves de données, de façon à ce que tous les participants qui contribuent aux réserves de données reçoivent une contrepartie pour leur contribution.

En seraient exclus les services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale entre les détenteurs de données et les utilisateurs de données. Seraient également exclus les services qui sont à l'usage exclusif d'un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets.

(29) Les services axés sur l'intermédiation de contenus protégés par le droit d'auteur, tels que les fournisseurs de services de partage de contenus en ligne au sens de l'article 2, point 6), de la directive (UE) 2019/790, ne devraient pas être couverts par le présent règlement. Les fournisseurs de système consolidé de publication, définis à l'article 2, paragraphe 1, point 35), du règlement (UE) no 600/2014 du Parlement européen et du Conseil[27] et les prestataires de services d'information sur les comptes définis à l'article 4, point 19), de la directive (UE) 2015/2366 du Parlement européen et du Conseil[28], ne devraient pas être considérés comme des prestataires de services d'intermédiation de données aux fins du présent règlement. Le présent règlement ne devrait pas s'appliquer aux services proposés par des organismes du secteur public afin de

27. Règlement (UE) no 600/2014 du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant le règlement (UE) no 648/2012 (JO L 173 du 12.6.2014, p. 84).

faciliter soit la réutilisation de données protégées détenues par les organismes du secteur public conformément au présent règlement, soit l'utilisation de toute autre donnée, dans la mesure où ces services ne visent pas à établir de relations commerciales. Les organisations altruistes en matière de données qui sont régies par le présent règlement ne devraient pas être considérées comme proposant des services d'intermédiation de données, pour autant que ces services n'établissent pas de relation commerciale entre les utilisateurs potentiels des données, d'une part, et les personnes concernées et les détenteurs de données qui mettent des données à disposition à des fins altruistes, d'autre part. D'autres services qui ne visent pas à établir des relations commerciales, tels que les référentiels visant à permettre la réutilisation des données de la recherche scientifique conformément aux principes du libre accès, ne devraient pas être considérés comme des services d'intermédiation de données au sens du présent règlement.

Services d'intermédiation des données à l'intention des personnes concernées.

(30) Les prestataires de services qui proposent leurs services à des personnes concernées constituent une catégorie spécifique de prestataires de services d'intermédiation de données. Ces prestataires de services d'intermédiation de données cherchent à renforcer la capacité d'action des personnes concernées, et plus particulièrement le contrôle qu'exercent les personnes physiques sur les données les concernant. Ces prestataires devraient aider les personnes physiques à exercer leurs droits au titre du règlement (UE) 2016/679, notamment l'octroi et le retrait de leur consentement au traitement des données, le droit d'accès à leurs propres données, le droit de rectification des données à caractère personnel inexactes, le droit à l'effacement ou droit «à l'oubli», le droit à la limitation du traitement, et le droit à la portabilité des données qui permet aux personnes concernées de transférer leurs données à caractère personnel d'un responsable du traitement des données à un autre. Dans ce contexte, il importe que le modèle commercial de ces prestataires garantisse qu'il n'existe pas d'incitations inadaptées poussant les personnes physiques à recourir à de tels services pour mettre à disposition, en vue d'un traitement, davantage de données les concernant qu'elles ne devraient le faire dans leur intérêt. Les prestataires pourraient notamment conseiller les personnes physiques sur les utilisations potentielles de leurs données et pratiquer des contrôles de diligence raisonnable à l'égard des utilisateurs de données avant de les autoriser à contacter les personnes concernées, afin d'éviter des pratiques frauduleuses. Dans certaines circonstances, il pourrait être souhaitable de compiler des données réelles dans un espace de données à caractère personnel, de telle sorte que le traitement puisse avoir lieu dans cet espace sans que les données à caractère personnel soient transmises à des tiers, afin d'assurer une protection maximale des données à caractère personnel et de la vie privée. Ces espaces de données à caractère personnel pourraient contenir des données à caractère personnel statiques, telles que le nom, l'adresse ou la date de naissance, ainsi que des données dynamiques qu'une personne physique génère, par exemple, lorsqu'elle recourt à un service en ligne ou à un objet connecté à l'internet des objets. Ils pourraient aussi être utilisés pour stocker des données d'identification vérifiées telles que le numéro de passeport ou les informations relatives à la sécurité sociale, ainsi que des justificatifs tels que permis de conduire, diplômes ou coordonnées de compte bancaire.

cf. RGPD : exercice des droits des personnes.

Coopératives de données

(31) Les coopératives de données visent à atteindre un certain nombre d'objectifs, et notamment à renforcer la position des personnes physiques en leur permettant de faire des choix en connaissance de cause avant de donner leur consentement à l'utilisation des données, en influant sur les conditions et modalités appliquées par les organisations d'utilisateurs de données à l'utilisation des données d'une manière qui offre de meilleurs choix aux membres individuels du groupe ou en trouvant, le cas échéant, des solutions aux conflits de positions des membres individuels d'un groupe sur la manière d'utiliser les données lorsque celles-ci portent sur plusieurs personnes concernées au sein de ce groupe. Dans ce contexte, il importe de tenir compte du fait que les droits consacrés par le règlement (UE) 2016/679 sont des droits personnels de la personne concernée et que les personnes concernées ne peuvent y renoncer. Les coopératives de données pourraient également constituer un outil utile pour les entreprises unipersonnelles et les PME, qui sont souvent comparables à des personnes physiques en termes de connaissance du partage des données.

cf. RGPD. Non répudiation des droits des par les personnes concernées.

28. Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

(32) Afin d'accroître la confiance dans ces services d'intermédiation de données, notamment en ce qui concerne l'utilisation des données et le respect des conditions imposées par les personnes concernées et les détenteurs de données, il est nécessaire de créer un cadre réglementaire à l'échelle de l'Union qui fixe des exigences largement harmonisées concernant la prestation fiable de ces services d'intermédiation de données et qui soit mis en œuvre par les autorités compétentes. Ce cadre contribuera à renforcer le contrôle que les personnes concernées et les détenteurs de données ainsi que les utilisateurs de données exercent sur l'accès à leurs données et sur l'utilisation de celles-ci, conformément au droit de l'Union. La Commission pourrait également encourager et faciliter l'élaboration de codes de conduite au niveau de l'Union, en associant les parties prenantes concernées, en particulier en ce qui concerne l'interopérabilité. Tant dans les situations où le partage de données intervient entre entreprises que dans celles où il intervient entre entreprises et consommateurs, les prestataires de services d'intermédiation de données devraient proposer une nouvelle gouvernance des données «à l'européenne», en prévoyant une séparation, dans l'économie des données, entre fourniture, intermédiation et utilisation des données. Les prestataires de services d'intermédiation de données pourraient également mettre à disposition une infrastructure technique spécifique pour l'interconnexion des personnes concernées et des détenteurs de données avec les utilisateurs de données. À cet égard, il est particulièrement important de façonner cette infrastructure de telle sorte que les PME et les jeunes pousses ne rencontrent aucune barrière technique ni d'autres barrières à leur participation à l'économie des données.

Les prestataires de services d'intermédiation de données devraient être autorisés à fournir, aux détenteurs de données ou aux personnes concernées, des outils et services spécifiques supplémentaires visant spécifiquement à faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation. Ces outils et services ne devraient être utilisés qu'à la demande expresse ou que moyennant l'approbation expresse du détenteur de données ou de la personne concernée et les outils de tiers proposés dans ce contexte ne devraient pas utiliser les données à d'autres fins. Parallèlement, les prestataires de services d'intermédiation de données devraient être autorisés à apporter des adaptations aux données échangées afin d'améliorer la facilité d'utilisation des données par l'utilisateur de données, si ce dernier le souhaite, ou d'améliorer l'interopérabilité, par exemple en convertissant les données dans des formats spécifiques.

(33) Il est important de favoriser un environnement compétitif pour le partage des données. La neutralité des prestataires de services d'intermédiation de données à l'égard des données échangées entre les détenteurs de données ou les personnes concernées et les utilisateurs de données est fondamentale pour renforcer la confiance et accroître le contrôle des détenteurs de données, des personnes concernées et des utilisateurs de données à l'égard des services d'intermédiation de données. Il est donc nécessaire que les prestataires de services d'intermédiation de données agissent uniquement en tant qu'intermédiaires dans les transactions, et qu'ils n'utilisent les données échangées à aucune autre fin. Les conditions commerciales, y compris la tarification, pour la fourniture de services d'intermédiation de données ne devraient pas dépendre du fait qu'un détenteur ou un utilisateur potentiel de données utilise d'autres services fournis par le même prestataire de services d'intermédiation de données ou par une entité liée à lui, notamment le stockage, l'analyse, l'intelligence artificielle ou d'autres applications fondées sur les données, ni, le cas échéant, de la mesure dans laquelle le détenteur de données ou l'utilisateur de données utilise ces autres services. Cela nécessitera également une séparation structurelle entre le service d'intermédiation de données et tout autre service fourni, afin d'éviter des conflits d'intérêts. Cela signifie que le service d'intermédiation de données devrait être fourni par une personne morale distincte des autres activités dudit prestataire de services d'intermédiation de données. Toutefois, les prestataires de services d'intermédiation de données devraient pouvoir utiliser les données fournies par le détenteur de données pour améliorer leurs services d'intermédiation de données.

Séparation structurelle entre services d'intermédiation et autres services.

Les prestataires de services d'intermédiation de données ne devraient être en mesure de mettre à la disposition des détenteurs de données, des personnes concernées ou des utilisateurs de données leurs propres outils ou les outils de tiers aux fins de faciliter l'échange de données, tels que des outils de conversion ou d'organisation de données, qu'à la demande expresse ou que moyennant l'approbation expresse de la personne concernée ou du détenteur de données. Les outils de tiers proposés dans ce contexte ne devraient pas utiliser les données à des fins autres que celles liées aux services d'inter-

médiation de données. Les prestataires de services d'intermédiation de données agissant en tant qu'intermédiaires dans l'échange de données entre des personnes physiques qui sont des personnes concernées et des personnes morales qui sont des utilisateurs de données devraient, en outre, assumer un devoir de loyauté à l'égard des personnes physiques, pour garantir qu'ils agissent au mieux des intérêts des personnes concernées. Les questions de responsabilité pour tous les dommages et préjudices matériels et immatériels résultant d'un comportement du prestataire de services d'intermédiation de données pourraient être traitées dans le contrat concerné, sur la base des régimes nationaux en matière de responsabilité.

(34) Les prestataires de services d'intermédiation de données devraient prendre des mesures raisonnables pour assurer l'interopérabilité au sein d'un secteur et entre les différents secteurs afin d'assurer le bon fonctionnement du marché intérieur. Parmi les mesures raisonnables pourrait figurer le respect des normes en vigueur et couramment mises en œuvre dans le secteur dans lequel les prestataires de services d'intermédiation de données exercent leurs activités. Le comité européen de l'innovation dans le domaine des données devrait faciliter l'émergence de normes industrielles supplémentaires, si nécessaire. Les prestataires de services d'intermédiation de données devraient, en temps utile, mettre en œuvre les mesures d'interopérabilité entre les services d'intermédiation de données adoptées par le comité européen de l'innovation dans le domaine des données.

(35) Le présent règlement est sans préjudice de l'obligation qui est faite aux prestataires de services d'intermédiation de données de respecter le règlement (UE) 2016/679 et de la responsabilité qui incombe aux autorités de contrôle de veiller au respect dudit règlement. Lorsque les prestataires de services d'intermédiation de données traitent des données à caractère personnel, le présent règlement ne devrait pas avoir d'incidence sur la protection de ces données. Lorsque les prestataires de services d'intermédiation de données sont des responsables du traitement ou des sous-traitants au sens du règlement (UE) 2016/679, ils sont liés par les règles prévues dans ledit règlement.

cf. RGPD.

(36) Les prestataires de services d'intermédiation de données devraient avoir mis en place des procédures et des mesures pour sanctionner les pratiques frauduleuses ou abusives en lien avec des parties qui cherchent à obtenir un accès par le biais des services d'intermédiation de données qu'ils proposent, y compris des mesures telles que l'exclusion des utilisateurs de données qui enfreignent les conditions de service ou le droit en vigueur.

(37) Les prestataires de services d'intermédiation de données devraient également prendre des mesures pour veiller au respect du droit de la concurrence et avoir mis en place des procédures à cette fin. Cela vaut en particulier dans les situations où le partage de données permet aux entreprises de prendre connaissance des stratégies de marché de leurs concurrents réels ou potentiels. Parmi ces informations sensibles sous l'angle de la concurrence, on trouve généralement des informations sur les données relatives aux clients, les prix futurs, les coûts de production, les quantités, les chiffres d'affaires, les ventes ou les capacités.

Procédure de notification

(38) Une procédure de notification pour les services d'intermédiation de données devrait être mise en place afin de garantir que la gouvernance des données au sein de l'Union est fondée sur un échange de données digne de confiance. Le meilleur moyen de tirer avantage d'un environnement digne de confiance serait d'imposer un certain nombre d'exigences pour la fourniture de services d'intermédiation de données sans pour autant qu'une décision expresse ou un acte administratif ne soient exigés de l'autorité compétente en matière de services d'intermédiation de données pour la fourniture de tels services. La procédure de notification ne devrait pas créer d'obstacles injustifiés pour les PME, les jeunes pousses et les organisations de la société civile et elle devrait respecter le principe de non-discrimination.

(39) Afin de favoriser l'efficacité de la prestation transfrontalière de services, le prestataire de services d'intermédiation de données devrait être invité à envoyer une notification uniquement à l'autorité compétente en matière de services d'intermédiation de données de l'État membre dans lequel est situé son établissement principal ou dans lequel se trouve son représentant légal. Une telle notification ne devrait nécessiter qu'une simple déclaration de l'intention de proposer de tels services, assortie uniquement de la mise à disposition des informations énoncées dans le présent règlement.

Après la notification concernée, le prestataire de services d'intermédiation de données devrait être en mesure de commencer ses activités dans tout État membre sans autre obligation de notification.

(40) La procédure de notification prévue par le présent règlement devrait s'entendre sans préjudice des règles spécifiques complémentaires applicables à la fourniture de services d'intermédiation de données en vertu du droit sectoriel.

(41) L'établissement principal d'un prestataire de services d'intermédiation de données dans l'Union devrait être le lieu de son administration centrale dans l'Union. L'établissement principal d'un prestataire de services d'intermédiation de données dans l'Union devrait être déterminé conformément à des critères objectifs et impliquer l'exercice effectif et réel d'activités de gestion. Les activités d'un prestataire de services d'intermédiation de données devraient respecter le droit national de l'État membre dans lequel il a son établissement principal.

(42) Afin de garantir le respect par les prestataires de services d'intermédiation de données du présent règlement, il convient qu'ils aient leur établissement principal dans l'Union. Lorsqu'un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union propose des services à l'intérieur de l'Union, il devrait désigner un représentant légal. La désignation d'un représentant légal est nécessaire dans de telles situations, étant donné que ces prestataires de services d'intermédiation de données traitent des données à caractère personnel ainsi que des données commerciales confidentielles, ce qui nécessite un contrôle étroit du respect, par ces prestataires de services d'intermédiation de données, du présent règlement. Afin de déterminer si un tel prestataire de services d'intermédiation de données propose des services dans l'Union, il convient de vérifier s'il est clair qu'il envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet ou d'une adresse électronique et d'autres coordonnées du prestataire de services d'intermédiation de données, ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où le prestataire de services d'intermédiation de données est établi, devraient être considérées comme insuffisantes aux fins de vérifier si telle est son intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisées dans un ou plusieurs États membres avec la possibilité de commander des services dans cette langue ou la mention d'utilisateurs qui se trouvent dans l'Union pourraient indiquer clairement que le prestataire de services d'intermédiation de données envisage d'offrir des services dans l'Union.

Un représentant légal désigné devrait agir pour le compte du prestataire de services d'intermédiation de données et les autorités compétentes en matière de services d'intermédiation de données devraient pouvoir contacter le représentant légal, en plus du prestataire de services d'intermédiation de données ou à la place de celui-ci, y compris en cas d'infraction, aux fins de lancer une procédure d'exécution à l'encontre d'un prestataire de services d'intermédiation de données non établi dans l'Union qui ne respecterait pas ses obligations. Le représentant légal devrait être désigné par un mandat écrit du prestataire de services d'intermédiation de données le chargeant d'agir pour son compte afin de remplir les obligations qui incombent à ce dernier au titre du présent règlement.

(43) Afin d'aider les personnes concernées et les détenteurs de données à identifier facilement les prestataires de services d'intermédiation de données reconnus dans l'Union et, partant, de renforcer leur confiance en ces derniers, il convient de créer un logo commun reconnaissable dans toute l'Union, outre le label «prestataire de services d'intermédiation de données reconnu dans l'Union».

Autorités compétentes en matière de services d'intermédiation de données.

(44) Les autorités compétentes en matière de services d'intermédiation de données désignées pour contrôler le respect des exigences du présent règlement par les prestataires de services d'intermédiation de données devraient être choisies sur la base de leurs capacités et de leur expertise en matière de partage de données horizontal ou sectoriel. Elles devraient être indépendantes de tout prestataire de services d'intermédiation de données, transparentes et impartiales dans l'exercice de leurs tâches. Les États membres devraient notifier à la Commission l'identité de ces autorités compétentes en matière de services d'intermédiation de données. Les pouvoirs et compétences des autorités compétentes en matière de services d'intermédiation de données devraient être sans préjudice des pouvoirs des autorités chargées de la protection des données. En particulier, pour toute question nécessitant une évaluation du respect du règlement

(UE) 2016/679, l'autorité compétente en matière services d'intermédiation de données devrait solliciter, s'il y a lieu, un avis ou une décision de l'autorité de contrôle compétente instituée en vertu dudit règlement.

cf. RGPD. Consultation de l'autorité de contrôle par l'autorité compétente en matière de services d'intermédiation de données.

(45) Pour atteindre des objectifs d'intérêt général, nombreuses sont les possibilités offertes par l'utilisation de données mises à disposition volontairement par les personnes concernées sur le fondement de leur consentement éclairé ou, lorsqu'il s'agit de données à caractère non personnel, mises à disposition par des détenteurs de données. Ces objectifs auraient trait notamment aux soins de santé, à la lutte contre le changement climatique, à l'amélioration de la mobilité, à la facilitation du développement, de la production et de la diffusion de statistiques officielles, à l'amélioration de la prestation de services publics ou à l'élaboration des politiques publiques. Le soutien à la recherche scientifique devrait également être considéré comme un objectif d'intérêt général. Le présent règlement devrait viser à contribuer à l'émergence de réserves de données d'une taille suffisante mises à disposition sur le fondement de l'altruisme en matière de données pour permettre l'analyse des données et l'apprentissage automatique, y compris dans l'ensemble de l'Union. Pour atteindre cet objectif, les États membres devraient pouvoir mettre en place des arrangements organisationnels ou techniques, ou les deux, qui faciliteraient l'altruisme en matière de données. Ces arrangements pourraient comprendre la disponibilité d'outils facilement utilisables permettant aux personnes concernées ou aux détenteurs de données de donner leur consentement ou leur autorisation à l'utilisation altruiste de leurs données, l'organisation de campagnes de sensibilisation ou un échange structuré entre les autorités compétentes sur la manière dont les politiques publiques, telles que l'amélioration du trafic, la santé publique et la lutte contre le changement climatique, tirent profit de l'altruisme en matière de données. À cette fin, les États membres devraient pouvoir élaborer des politiques nationales concernant l'altruisme en matière de données. Les personnes concernées ne devraient pouvoir recevoir de compensation que pour les coûts qu'elles supportent lorsqu'elles mettent leurs données à disposition pour des objectifs d'intérêt général.

Organisations altruistes en matière de données.

(46) L'enregistrement d'organisations altruistes en matière de données reconnues et l'utilisation du label «organisation altruiste en matière de données reconnue dans l'Union» devraient aboutir à la mise en place de référentiels de données. L'enregistrement dans un État membre serait valable dans toute l'Union et devrait faciliter l'utilisation transfrontalière des données au sein de l'Union et l'émergence de réserves de données couvrant plusieurs États membres. Les détenteurs de données pourraient autoriser le traitement de leurs données à caractère non personnel pour une série de finalités non définies au moment où l'autorisation est accordée. Le respect, par de telles organisations altruistes en matière de données reconnues, d'un ensemble d'exigences prévues par le présent règlement devrait susciter la confiance dans le fait que les données mises à disposition à des fins altruistes servent un objectif d'intérêt général. Cette confiance devrait résulter notamment de l'existence d'un lieu d'établissement ou d'un représentant légal dans l'Union, ainsi que de l'obligation pour les entités altruistes en matière de données reconnues d'être des organisations à but non lucratif, des exigences de transparence et des garanties spécifiques mises en place pour protéger les droits et les intérêts des personnes concernées et des entreprises.

D'autres garanties devraient inclure la possibilité de traiter les données pertinentes dans un environnement de traitement sécurisé exploité par les organisations altruistes en matière de données reconnues, des mécanismes de surveillance tels que l'existence de conseils d'éthique ou de conseils d'administration, y compris des représentants de la société civile afin de garantir que le responsable du traitement respecte des normes rigoureuses en matière d'éthique scientifique et de protection des droits fondamentaux, des moyens techniques efficaces et clairement communiqués pour retirer ou modifier son consentement à tout moment, sur la base des obligations d'information incombant aux sous-traitants au titre du règlement (UE) 2016/679, ainsi que des moyens permettant aux personnes concernées de rester informées au sujet de l'utilisation des données qu'elles ont mises à disposition. L'enregistrement en tant qu'organisation altruiste en matière de données reconnue ne devrait pas être une condition préalable à l'exercice d'activités altruistes en matière de données. La Commission devrait, par voie d'actes délégués, préparer un recueil de règles en étroite coopération avec les organisations altruistes en matière de données et les parties prenantes. Le respect de ce recueil de règles devrait constituer une exigence pour l'enregistrement en tant qu'organisation altruiste en matière de données reconnue.

cf. RGPD : obligations d'information incombant aux sous-traitants.

(47) Afin d'aider les personnes concernées et les détenteurs de données à identifier facilement les organisations altruistes en matière de données reconnues et, partant, de renforcer leur confiance en ces dernières, il convient de créer un logo commun reconnaissable dans toute l'Union. Le logo commun devrait s'accompagner d'un code QR comportant un lien vers le registre public de l'Union des organisations altruistes en matière de données reconnues.

(48) Le présent règlement devrait être sans préjudice de l'établissement, de l'organisation et du fonctionnement des entités qui souhaitent s'engager dans l'altruisme en matière de données en vertu du droit national et s'inspirer des exigences imposées par le droit national pour exercer des activités légalement dans un État membre en tant qu'organisation à but non lucratif.

(49) Le présent règlement devrait s'entendre sans préjudice de l'établissement, de l'organisation et du fonctionnement d'entités autres que les organismes du secteur public qui s'engagent dans le partage de données et de contenus sur la base de licences ouvertes, contribuant ainsi à la création de ressources communes accessibles à tous. Cela devrait inclure des plateformes de partage de connaissances collaboratives ouvertes, des référentiels scientifiques et universitaires en libre accès, des plateformes de développement de logiciels ouverts et des plateformes d'agrégation de contenu en libre accès.

(50) Les organisations altruistes en matière de données reconnues devraient être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres. Le traitement des données collectées pourrait être effectué par des organisations altruistes en matière de données à des fins qu'elles définissent elles-mêmes ou, le cas échéant, elles pourraient autoriser le traitement par des tiers à ces fins. Lorsque les organisations altruistes en matière de données reconnues sont des responsables du traitement ou des sous-traitants tels qu'ils sont définis dans le règlement (UE) 2016/679, elles devraient respecter ledit règlement. En règle générale, l'altruisme en matière de données reposerait sur le consentement des personnes concernées, au sens de l'article 6, paragraphe 1, point a), et de l'article 9, paragraphe 2, point a), du règlement (UE) 2016/679, qui devrait respecter les exigences régissant un consentement licite énoncées aux articles 7 et 8 dudit règlement. Conformément au règlement (UE) 2016/679, le consentement donné en ce qui concerne certains domaines de recherche scientifique lorsqu'ils respectent des normes éthiques reconnues en matière de recherche scientifique, ou uniquement en ce qui concerne certains domaines de recherche ou certaines parties de projets de recherche, pourrait soutenir les finalités de la recherche scientifique. L'article 5, paragraphe 1, point b), du règlement (UE) 2016/679 précise que le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques ne devrait pas être considéré, conformément à l'article 89, paragraphe 1, dudit règlement, comme incompatible avec les finalités initiales. Pour les données à caractère non personnel, les limitations d'utilisation devraient figurer dans l'autorisation donnée par le détenteur de données.

cf. RGPD : définition de sous-traitant.

cf. RGPD : définition du consentement. L'altruisme en matière de données repose en général sur le consentement.

cf. RGPD : consentement dans le domaine de la recherche scientifique.

(51) Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données désignées pour contrôler le respect des exigences du présent règlement par les organisations altruistes en matière de données reconnues devraient être choisies sur la base de leurs capacités et de leur expertise. Elles devraient être indépendantes de toute organisation altruiste en matière de données, transparentes et impartiales dans l'exercice de leurs tâches. Les États membres devraient notifier à la Commission l'identité desdites autorités compétentes pour l'enregistrement des organisations altruistes en matière de données. Les pouvoirs et les compétences des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données devraient être sans préjudice des pouvoirs des autorités chargées de la protection des données. En particulier, pour toute question nécessitant une évaluation du respect du règlement (UE) 2016/679, l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données devrait solliciter, s'il y a lieu, un avis ou une décision de l'autorité de contrôle compétente instituée en application dudit règlement.

Autorités compétentes pour l'enregistrement des organisations altruistes

cf. RGPD. Consultation de l'autorité de contrôle par l'autorité compétente pour l'altruisme en matière de données.

(52) Afin de promouvoir la confiance et d'apporter davantage de sécurité juridique et de simplicité à la procédure d'octroi et de retrait du consentement, en particulier dans le cadre de la recherche scientifique et de l'utilisation statistique des données mises à disposition sur une base altruiste, il convient d'élaborer et d'utiliser un formulaire

européen de consentement à l'altruisme en matière de données en cas de partage de données altruiste. Un tel formulaire devrait contribuer à accroître la transparence à l'égard des personnes concernées quant au fait que leurs données seront consultées et utilisées conformément à leur consentement et dans le plein respect des règles en matière de protection des données. Il devrait également faciliter l'octroi et le retrait du consentement et être utilisé pour rationaliser l'altruisme en matière de données pratiqué par les entreprises et fournir un mécanisme permettant à ces entreprises de retirer leur autorisation d'utiliser les données. Afin de tenir compte des spécificités de chaque secteur, y compris sur le plan de la protection des données, le formulaire européen de consentement à l'altruisme en matière de données devrait être conçu selon une approche modulaire permettant son adaptation à des secteurs particuliers et pour des finalités différentes.

(53) Afin de mettre en œuvre avec succès le cadre de gouvernance des données, il convient d'instaurer un comité européen de l'innovation dans le domaine des données, sous la forme d'un groupe d'experts. Le comité européen de l'innovation dans le domaine des données devrait être composé de représentants des autorités compétentes pour les services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'Agence de l'Union européenne pour la cybersécurité (ENISA), de la Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière. Le comité européen de l'innovation dans le domaine des données devrait être composé d'un nombre de sous-groupes, y compris d'un sous-groupe chargé de la participation des parties prenantes composé de représentants compétents issus de l'industrie, notamment dans les domaines de la santé, de l'environnement, de l'agriculture, des transports, de l'énergie, de la fabrication industrielle, des médias, des secteurs de la culture et de la création et des statistiques, ainsi que de la recherche, du monde universitaire, de la société civile, des organismes de normalisation, des espaces européens communs de données pertinents et d'autres parties prenantes concernées et de tiers, entre autres d'organismes possédant une expertise spécifique tels que les instituts nationaux de statistique.

Comité européen de l'innovation dans le domaine des données.

CEIDD :
- ACSID
- ACEOAMD
- CEPD/EDPB
- CEPD/EDPS
- ENISA
- ...

(54) Le comité européen de l'innovation dans le domaine des données devrait aider la Commission à coordonner les pratiques et les politiques nationales sur les thèmes couverts par le présent règlement et à soutenir l'utilisation transsectorielle des données, en respectant les principes du cadre d'interopérabilité européen et en ayant recours à des normes et spécifications européennes et internationales, notamment à la plateforme européenne multipartite sur la normalisation des TIC, aux vocabulaires de base et aux blocs constitutifs du MIE, et devrait tenir compte des travaux de normalisation menés dans des secteurs ou domaines spécifiques. Les travaux de normalisation technique pourraient inclure la définition de priorités pour l'élaboration de normes et la création et l'actualisation d'un ensemble de normes techniques et juridiques régissant la transmission de données entre deux environnements de traitement afin d'organiser des espaces de données, notamment en clarifiant et en distinguant les normes et pratiques qui sont intersectorielles et celles qui sont sectorielles. Le comité européen de l'innovation dans le domaine des données devrait coopérer avec des organismes, des réseaux ou des groupes d'experts sectoriels, ou toute autre organisation intersectorielle intervenant dans la réutilisation des données. En ce qui concerne l'altruisme en matière de données, le comité européen de l'innovation dans le domaine des données devrait aider la Commission à élaborer le formulaire européen de consentement à l'altruisme en matière de données, après consultation du comité européen de la protection des données. En proposant des lignes directrices sur les espaces européens communs des données, le comité européen de l'innovation dans le domaine des données devrait soutenir le développement d'une économie européenne des données qui fonctionne sur la base de ces espaces de données, comme le prévoit la stratégie européenne pour les données.

(55) Les États membres devraient fixer des règles en matière de sanctions applicables aux infractions au présent règlement et devraient prendre toutes les mesures nécessaires afin de garantir leur mise en œuvre. Ces sanctions devraient être effectives, proportionnées et dissuasives. D'importantes disparités entre les règles en matière de sanctions pourraient entraîner une distorsion de la concurrence sur le marché unique numérique. L'harmonisation de ces règles pourrait être utile à cet égard.

Sanctions

(56) Afin de garantir une application efficace du présent règlement et de veiller à ce que les prestataires de services d'intermédiation de données et les entités qui souhaitent s'enregistrer en tant qu'organisations altruistes en matière de données reconnues puissent accéder aux procédures de notification et d'enregistrement et les mener à bien intégralement en ligne et par-delà les frontières, ces procédures devraient être proposées par l'intermédiaire du portail numérique unique établi en vertu du règlement (UE) 2018/1724 du Parlement européen et du Conseil[29]. Il convient d'ajouter ces procédures à la liste des procédures figurant à l'annexe II du règlement (UE) 2018/1724.

(57) Il convient, dès lors, de modifier le règlement (UE) 2018/1724 en conséquence.

(58) Afin de garantir l'efficacité du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne afin de compléter le présent règlement en fixant les conditions particulières applicables aux transferts vers des pays tiers de certaines catégories de données à caractère non personnel considérées comme hautement sensibles dans des actes législatifs de l'Union déterminés et en établissant, pour les organisations altruistes en matière de données reconnues, un recueil de règles que ces organisations doivent respecter, qui fixe les exigences liées aux informations, aux aspects techniques et à la sécurité ainsi que les feuilles de route en matière de communication et les normes d'interopérabilité. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer»[30]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(59) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission pour aider les organismes du secteur public et les réutilisateurs à respecter les conditions de réutilisation énoncées dans le présent règlement en élaborant des clauses contractuelles types pour le transfert par des réutilisateurs de données à caractère non personnel vers un pays tiers, pour déclarer que le cadre juridique et le dispositif de surveillance et d'exécution d'un pays tiers sont équivalents à la protection garantie au titre du droit de l'Union, pour concevoir le logo commun destiné aux prestataires de services d'intermédiation de données et le logo commun destiné aux organisations altruistes en matière de données reconnues et pour créer et élaborer le formulaire européen de consentement à l'altruisme en matière de données. Ces compétences devraient être exercées conformément au règlement (UE) no 182/2011 du Parlement européen et du Conseil[31].

(60) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles relatives à la concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne. Cela concerne en particulier les règles relatives à l'échange d'informations sensibles sous l'angle de la concurrence entre concurrents réels ou potentiels au moyen de services d'intermédiation de données.

29. Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) no 1024/2012 (JO L 295 du 21.11.2018, p. 1).
30. JO L 123 du 12.5.2016, p. 1.
31. Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(61) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et ont rendu leur avis le 10 mars 2021.

(62) Le présent règlement a pour principes directeurs le respect des droits fondamentaux et des principes reconnus en particulier par la Charte des droits fondamentaux de l'Union européenne, notamment le respect de la vie privée, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété et l'intégration des personnes handicapées. En ce qui concerne ce dernier élément, les organismes de service public et les services relevant du présent règlement devraient, s'il y a lieu, respecter les directives (UE) 2016/2102[32] et (UE) 2019/882 [33] du Parlement européen et du Conseil. En outre, il convient de tenir compte de la conception universelle dans le contexte des technologies de l'information et de la communication, qui consiste en un effort délibéré et systématique d'appliquer de manière proactive les principes, méthodes et outils de promotion de la conception universelle dans les technologies informatiques, y compris les technologies basées sur l'internet, ce qui évite que des adaptations a posteriori ou une conception spéciale ne soient nécessaires.

(63) Étant donné que les objectifs du présent règlement, à savoir la réutilisation, au sein de l'Union, de certaines catégories de données détenues par des organismes du secteur public, ainsi que l'établissement d'un cadre de notification et de surveillance pour la fourniture de services d'intermédiation de données, d'un cadre pour l'enregistrement volontaire des entités qui mettent des données à disposition à des fins altruistes et d'un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données, ne peuvent pas être atteints de manière suffisante par les États membres mais peuvent, en raison de leurs dimensions et de leurs effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
Dispositions générales

Article premier
Objet et champ d'application

1. Le présent règlement établit:

a) les conditions de réutilisation, au sein de l'Union, de certaines catégories de données détenues par des organismes du secteur public;

b) un cadre de notification et de surveillance pour la fourniture de services d'intermédiation de données;

c) un cadre pour l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes; et

d) un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données.

2. Le présent règlement ne crée, pour les organismes du secteur public, aucune obligation d'autoriser la réutilisation des données et ne libère pas les organismes du secteur public des obligations de confidentialité qui leur incombent au titre du droit de l'Union ou du droit national.

Le présent règlement est sans préjudice:

32. Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).
33. Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

a) des dispositions particulières du droit de l'Union ou du droit national concernant l'accès à certaines catégories de données ou la réutilisation de celles-ci, notamment en ce qui concerne l'octroi de l'accès à des documents officiels et leur divulgation; et

b) de l'obligation incombant aux organismes du secteur public au titre du droit de l'Union ou du droit national d'autoriser la réutilisation des données ou des exigences liées au traitement des données à caractère non personnel.

Lorsque le droit sectoriel de l'Union ou le droit sectoriel national impose aux organismes du secteur public, aux prestataires de services d'intermédiation de données ou aux organisations altruistes en matière de données reconnues de respecter des exigences techniques, administratives ou organisationnelles particulières supplémentaires, notamment au moyen d'un régime d'autorisation ou de certification, ces dispositions dudit droit sectoriel de l'Union ou dudit droit sectoriel national s'appliquent également. Des exigences particulières supplémentaires de ce type sont non discriminatoires, proportionnées et objectivement justifiées.

3. Le droit de l'Union et le droit national en matière de protection des données à caractère personnel s'appliquent à toutes les données à caractère personnel traitées en lien avec le présent règlement. En particulier, le présent règlement est sans préjudice des règlements (UE) 2016/679 et (UE) 2018/1725 et des directives 2002/58/CE et (UE) 2016/680, y compris en ce qui concerne les pouvoirs et compétences des autorités de contrôle. En cas de conflit entre le présent règlement et les dispositions du droit de l'Union en matière de protection des données à caractère personnel ou du droit national adopté conformément audit droit de l'Union, les dispositions pertinentes du droit de l'Union ou du droit national en matière de protection des données à caractère personnel prévalent. Le présent règlement ne crée pas de base juridique pour le traitement des données à caractère personnel et ne modifie pas les droits et obligations énoncés dans le règlement (UE) 2016/679 ou (UE) 2018/1725 ou dans la directive 2002/58/CE ou (UE) 2016/680.

cf. RGPD.

cf. RGPD. Le DGA ne crée pas de base juridique et ne modifie pas les droits et obligations issus du RGPD.

4. Le présent règlement est sans préjudice de l'application du droit de la concurrence.

5. Le présent règlement est sans préjudice des compétences des États membres en ce qui concerne leurs activités relatives à la sécurité publique, à la défense et à la sécurité nationale.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

1) «données»: toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;

2) «réutilisation»: l'utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les données ont été produites, à l'exception de l'échange de données entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public;

3) «données à caractère personnel»: les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD. Définition de données à caractère personnel.

4) «données à caractère non personnel»: les données autres que les données à caractère personnel;

5) «consentement»: le consentement au sens de l'article 4, point 11), du règlement (UE) 2016/679;

cf. RGPD. Définition de consentement.

6) «autorisation»: le fait d'accorder aux utilisateurs de données le droit au traitement de données à caractère non personnel;

7) «personne concernée»: la personne concernée visée à l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD. Définition de personne concernée.

8) «détenteur de données»: une personne morale, y compris des organismes du secteur public et des organisations internationales, ou une personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui, conformément au droit de l'Union ou au droit national applicable, a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel;

9) «utilisateur de données»: une personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui a le droit, y compris au titre du règlement (UE) 2016/679 lorsqu'il s'agit de données à caractère personnel, d'utiliser ces données à des fins commerciales ou non commerciales;

cf. RGPD. droit d'utiliser les données à caractère personnel.

10) «partage de données»: la fourniture de données à un utilisateur de données par une personne concernée ou un détenteur de données, en vue de l'utilisation conjointe ou individuelle desdites données, sur la base d'accords volontaires ou du droit de l'Union ou du droit national, directement ou via un intermédiaire, par exemple dans le cadre de licences ouvertes ou commerciales, moyennant le paiement d'une redevance ou gratuitement;

11) «service d'intermédiation de données»: un service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel, à l'exclusion au minimum de ce qui suit:

a) des services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale directe entre les détenteurs de données et les utilisateurs de données;

b) des services axés sur l'intermédiation de contenus protégés par le droit d'auteur;

c) des services qui sont utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets;

d) des services pour le partage de données proposés par des organismes du secteur public qui ne cherchent pas à établir des relations commerciales;

12) «traitement»: le traitement au sens de l'article 4, point 2), du règlement (UE) 2016/679 en ce qui concerne les données à caractère personnel ou de l'article 3, point 2), du règlement (UE) 2018/1807 en ce qui concerne les données à caractère non personnel;

cf. RGPD. Définition de traitement.

13) «accès»: l'utilisation de données conformément à des exigences techniques, juridiques ou organisationnelles particulières, sans que cela implique nécessairement la transmission ou le téléchargement de données;

accès : y compris sans transmission ou téléchargement.

14) «établissement principal»: en ce qui concerne une personne morale, le lieu de son administration centrale dans l'Union;

15) «services de coopératives de données»: les services d'intermédiation de données proposés par une structure organisationnelle constituée de personnes concernées, d'entreprises unipersonnelles ou de PME qui sont membres de cette structure dont les objectifs principaux consistent à aider ses membres à exercer leurs droits à l'égard de certaines données, y compris quant au fait d'opérer des choix en connaissance de cause avant qu'ils ne consentent au traitement de données, à mener des échanges de vues sur les finalités et les conditions du traitement de données qui représenteraient le mieux les intérêts de ses membres en ce qui concerne leurs données, et à négocier les conditions et modalités du traitement des données au nom de ses membres avant que

ceux-ci ne donnent l'autorisation de traiter des données à caractère non personnel ou ne donnent leur consentement au traitement de données à caractère personnel;

16) «altruisme en matière de données»: le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national, le cas échéant, par exemple les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, la facilitation du développement, de la production et de la diffusion de statistiques officielles, l'amélioration de la prestation de services publics, l'élaboration des politiques publiques ou la recherche scientifique dans l'intérêt général;

17) «organisme du secteur public»: l'État, les autorités régionales ou locales, les organismes de droit public ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes de droit public;

18) «organismes de droit public»: les organismes présentant les caractéristiques suivantes:

à noter : la définition d'organisme de droit public est récursive (cf. c).

a) ils ont été créés pour satisfaire spécifiquement des besoins d'intérêt général et n'ont pas de caractère industriel ou commercial;

b) ils sont dotés de la personnalité juridique;

c) ils sont financés majoritairement par l'État, les autorités régionales ou locales ou d'autres organismes de droit public, leur gestion est soumise à un contrôle de ces autorités ou organismes, ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou locales ou d'autres organismes de droit public;

cf. note précédente : « financés [...] ou par d'autres organismes de droit public »

19) «entreprise publique»: toute entreprise sur laquelle les organismes du secteur public peuvent exercer directement ou indirectement une influence dominante du fait de la propriété de l'entreprise, de la participation financière qu'ils y détiennent ou des règles qui la régissent; aux fins de la présente définition, une influence dominante des organismes du secteur public sur l'entreprise est présumée dans tous les cas suivants lorsque ces organismes, directement ou indirectement:

a) détiennent la majorité du capital souscrit de l'entreprise;

b) disposent de la majorité des voix attachées aux parts émises par l'entreprise;

c) peuvent désigner plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance de l'entreprise;

20) «environnement de traitement sécurisé»: l'environnement physique ou virtuel et les moyens organisationnels pour garantir le respect du droit de l'Union, tel que le règlement (UE) 2016/679, en particulier en ce qui concerne les droits des personnes concernées, les droits de propriété intellectuelle, la confidentialité commerciale et le secret statistique, l'intégrité et l'accessibilité, ainsi que le respect du droit national applicable, et pour permettre à l'entité fournissant l'environnement de traitement sécurisé de déterminer et de surveiller toutes les opérations de traitement de données, notamment l'affichage, le stockage, le téléchargement et l'exportation de données et le calcul de données dérivées au moyen d'algorithmes de calcul;

cf. RGPD.

21) «représentant légal»: une personne physique ou morale établie dans l'Union, expressément désignée pour agir pour le compte d'un prestataire de services d'intermédiation de données ou d'une entité qui collecte pour des objectifs d'intérêt général des données mises à disposition par des personnes physiques ou morales sur le fondement de l'altruisme en matière de données non établi(e) dans l'Union, qui peut être contactée par les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en plus du prestataire de services d'intermédiation de données ou de l'entité, ou à leur place, en ce qui concerne les obligations prévues dans le pré-

sent règlement, y compris en ce qui concerne le lancement d'une procédure d'exécution à l'encontre d'un prestataire de services d'intermédiation de données ou d'une entité non établi(e) dans l'Union qui ne respecte pas ses obligations.

CHAPITRE II
Réutilisation de certaines catégories de données protégées détenues par des organismes du secteur public

Article 3
Catégories de données

Données concernées.

1. Le présent chapitre s'applique aux données détenues par des organismes du secteur public, qui sont protégées pour des motifs:

a) de confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise;

b) de secret statistique;

c) de protection des droits de propriété intellectuelle de tiers; ou

d) de protection des données à caractère personnel, dans la mesure où de telles données ne relèvent pas du champ d'application de la directive (UE) 2019/1024.

Le DGA s'applique en particulier aux données à caractère personnel détenues par des organismes du secteur public.

Données exclues.

2. Le présent chapitre ne s'applique pas:

a) aux données détenues par des entreprises publiques;

b) aux données détenues par des radiodiffuseurs de service public et leurs filiales et par d'autres organismes ou leurs filiales pour l'accomplissement d'une mission de radiodiffusion de service public;

c) aux données détenues par des établissements culturels et des établissements d'enseignement;

d) aux données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale; ou

e) aux données dont la fourniture est une activité qui ne relève pas de la mission de service public dévolue aux organismes du secteur public concernés telle qu'elle est définie par la loi ou par d'autres règles contraignantes en vigueur dans l'État membre concerné ou, en l'absence de telles règles, telle qu'elle est définie conformément aux pratiques administratives courantes dans cet État membre, sous réserve que l'objet des missions de service public soit transparent et soumis à réexamen.

3. Le présent chapitre est sans préjudice:

a) du droit de l'Union, du droit national et des accords internationaux auxquels l'Union ou les États membres sont parties en ce qui concerne la protection des catégories de données visées au paragraphe 1; et

b) du droit de l'Union et du droit national en matière d'accès aux documents.

Article 4
Interdiction des accords d'exclusivité

1. Sont interdits les accords ou autres pratiques relatifs à la réutilisation de données détenues par des organismes du secteur public contenant des catégories de données visées à l'article 3, paragraphe 1, qui octroient des droits d'exclusivité ou qui ont pour objet ou pour effet d'octroyer de tels droits d'exclusivité ou de restreindre la disponibilité des données à des fins de réutilisation par des entités autres que les parties à ces accords ou autres pratiques.

2. Par dérogation au paragraphe 1, un droit d'exclusivité pour la réutilisation des données visées audit paragraphe peut être accordé dans la mesure nécessaire à la fourni-

ture d'un service ou d'un produit d'intérêt général qui, sans cela, ne pourrait pas être obtenu.

3. Un droit d'exclusivité tel qu'il est visé au paragraphe 2 est accordé par le biais d'un acte administratif ou d'un arrangement contractuel conformément au droit de l'Union ou au droit national applicable, dans le respect des principes de transparence, d'égalité de traitement et de non-discrimination.

4. La durée du droit d'exclusivité pour la réutilisation des données ne dépasse pas douze mois. Lorsqu'un contrat est conclu, la durée du contrat est la même que la durée du droit d'exclusivité.

5. L'octroi d'un droit d'exclusivité en vertu des paragraphes 2, 3 et 4, notamment les raisons justifiant la nécessité d'accorder un tel droit, est transparent et est rendu public en ligne, sous une forme qui respecte les dispositions pertinentes du droit de l'Union en matière de marchés publics.

6. Les accords ou autres pratiques tombant sous le coup de l'interdiction visée au paragraphe 1 qui ne remplissent pas les conditions prévues aux paragraphes 2 et 3, et qui ont été respectivement conclus ou convenues avant le 23 juin 2022 prennent fin au terme du contrat applicable et, en tout état de cause, au plus tard le 24 décembre 2024.

Article 5
Conditions applicables à la réutilisation

Conditions de réutilisation

1. Les organismes du secteur public qui sont compétents en vertu du droit national pour octroyer ou refuser l'accès aux fins de la réutilisation d'une ou de plusieurs des catégories de données visées à l'article 3, paragraphe 1, rendent publiques les conditions d'autorisation de cette réutilisation et la procédure de demande de réutilisation par l'intermédiaire du point d'information unique visé à l'article 8. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, ils peuvent être assistés par les organismes compétents visés à l'article 7, paragraphe 1.

Les États membres veillent à ce que les organismes du secteur public soient dotés des ressources nécessaires pour se conformer au présent article.

2. Les conditions applicables à la réutilisation sont non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation, ainsi que la nature des données pour lesquelles la réutilisation est autorisée. Ces conditions ne sont pas utilisées pour restreindre la concurrence.

3. Les organismes du secteur public veillent à ce que, conformément au droit de l'Union et au droit national, le caractère protégé des données soit préservé. Ils peuvent prévoir les exigences suivantes:

a) l'accès aux données à des fins de réutilisation n'est octroyé que lorsque l'organisme du secteur public ou l'organisme compétent, à la suite d'une demande de réutilisation, a fait en sorte que les données:

i) aient été anonymisées dans le cas des données à caractère personnel; et

ii) aient été modifiées, agrégées ou traitées selon toute autre méthode de contrôle de la divulgation dans le cas des informations commerciales confidentielles, y compris des secrets d'affaires et des contenus protégés par des droits de propriété intellectuelle;

b) l'accès aux données et leur réutilisation se font à distance dans un environnement de traitement sécurisé qui est fourni ou contrôlé par l'organisme du secteur public;

c) l'accès aux données et leur réutilisation se font dans les locaux où se trouve l'environnement de traitement sécurisé, dans le respect de normes de sécurité élevées, à condition que l'accès à distance ne puisse être autorisé sans qu'il soit porté atteinte aux droits et aux intérêts des tiers.

4. Lorsque la réutilisation est autorisée conformément au paragraphe 3, points b) et c), les organismes du secteur public imposent des conditions qui préservent l'intégrité du fonctionnement des systèmes techniques de l'environnement de traitement sécurisé utilisé. L'organisme du secteur public se réserve le droit de vérifier le processus, les moyens et tout résultat du traitement de données effectué par le réutilisateur afin de préserver l'intégrité de la protection des données et se réserve le droit d'interdire l'utilisation des résultats qui contiennent des informations portant atteinte aux droits et aux intérêts de tiers. La décision d'interdire l'utilisation des résultats est transparente et compréhensible par le réutilisateur.

5. Sauf si le droit national prévoit des garanties spécifiques concernant les obligations de confidentialité applicables en cas de réutilisation des données visées à l'article 3, paragraphe 1, l'organisme du secteur public subordonne la réutilisation des données fournies conformément au paragraphe 3 du présent article au respect par le réutilisateur d'une obligation de confidentialité interdisant la divulgation de toute information compromettant les droits et intérêts de tiers que le réutilisateur peut avoir acquis malgré les garanties mises en place. Il est interdit aux réutilisateurs de rétablir l'identité de toute personne concernée à laquelle se rapportent les données et ils prennent des mesures techniques et opérationnelles pour empêcher toute réidentification et notifier à l'organisme du secteur public toute violation de données ayant pour effet de réidentifier les personnes concernées. En cas de réutilisation non autorisée de données à caractère non personnel, le réutilisateur informe sans retard, au besoin avec l'aide de l'organisme du secteur public, les personnes morales dont les droits et intérêts peuvent être affectés.

6. Lorsqu'il est impossible d'autoriser la réutilisation des données en respectant les obligations prévues aux paragraphes 3 et 4 du présent article et qu'il n'existe pas de base juridique pour la transmission des données au titre du règlement (UE) 2016/679, l'organisme du secteur public met tout en œuvre, conformément au droit de l'Union et au droit national, pour aider les réutilisateurs potentiels à demander le consentement des personnes concernées ou l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation, lorsque cela est faisable sans charge disproportionnée pour l'organisme du secteur public. Lorsqu'il fournit cette aide, l'organisme du secteur public peut être assisté par les organismes compétents visés à l'article 7, paragraphe 1.

cf. RGPD. Base juridique pour la transmission des données.

7. La réutilisation des données n'est autorisée que dans le respect des droits de propriété intellectuelle. Les organismes du secteur public n'exercent pas le droit du fabricant d'une base de données prévu à l'article 7, paragraphe 1, de la directive 96/9/CE en vue d'empêcher la réutilisation de données ou de limiter celle-ci au-delà des limites fixées par le présent règlement.

8. Lorsque les données demandées sont considérées comme confidentielles, conformément au droit de l'Union ou au droit national en matière de confidentialité commerciale ou de secret statistique, les organismes du secteur public veillent à ce que les données confidentielles ne soient pas divulguées du fait de l'autorisation à des fins de réutilisation, à moins que cette réutilisation ne soit autorisée conformément au paragraphe 6.

9. Lorsqu'un réutilisateur a l'intention de transférer à un pays tiers des données à caractère non personnel protégées pour les motifs énoncés à l'article 3, paragraphe 1, il informe l'organisme du secteur public de son intention de transférer ces données ainsi que de la finalité de ce transfert au moment de demander la réutilisation desdites données. En cas de réutilisation conformément au paragraphe 6 du présent article, le réutilisateur informe, au besoin avec l'aide de l'organisme du secteur public, la personne morale dont les droits et intérêts peuvent être affectés de cette intention, de la finalité et des garanties appropriées. L'organisme du secteur public n'autorise pas la réutilisation à moins que la personne morale n'autorise le transfert.

10. Les organismes du secteur public ne transmettent des données confidentielles à caractère non personnel ou des données protégées par des droits de propriété intellectuelle à un réutilisateur qui a l'intention de transférer lesdites données vers un pays tiers autre qu'un pays désigné conformément au paragraphe 12 que si le réutilisateur s'engage contractuellement à:

a) respecter les obligations imposées conformément aux paragraphes 7 et 8, même après le transfert des données vers le pays tiers; et

b) admettre la compétence des juridictions de l'État membre de l'organisme du secteur public qui transmet les données en ce qui concerne tout litige lié au respect des paragraphes 7 et 8.

11. Les organismes du secteur public, s'il y a lieu et dans la mesure de leurs capacités, fournissent des conseils et une assistance aux réutilisateurs pour ce qui est de respecter les obligations visées au paragraphe 10 du présent article.

Afin d'aider les organismes du secteur public et les réutilisateurs, la Commission peut adopter des actes d'exécution établissant des clauses contractuelles types pour le respect des obligations visées au paragraphe 10 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 33, paragraphe 3.

12. Lorsque cela est justifié en raison du nombre important de demandes dans l'ensemble de l'Union concernant la réutilisation de données à caractère non personnel dans des pays tiers déterminés, la Commission peut adopter des actes d'exécution déclarant que le cadre juridique et le dispositif de surveillance et d'exécution d'un pays tiers:

a) assurent la protection de la propriété intellectuelle et des secrets d'affaires d'une manière qui est essentiellement équivalente à la protection assurée par le droit de l'Union;

b) sont effectivement appliqués et leur application est contrôlée; et

c) prévoient un recours juridictionnel effectif.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 33, paragraphe 3.

13. Des actes législatifs spécifiques de l'Union peuvent considérer que certaines catégories de données à caractère non personnel détenues par des organismes du secteur public sont hautement sensibles aux fins du présent article, lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union, tels que la sécurité et la santé publique, ou peut entraîner un risque de réidentification de données anonymisées à caractère non personnel. Lorsqu'un tel acte est adopté, la Commission adopte des actes délégués conformément à l'article 32 afin de compléter le présent règlement en fixant des conditions particulières applicables aux transferts de telles données vers des pays tiers.

Ces conditions particulières sont fondées sur la nature des catégories de données à caractère non personnel identifiées dans l'acte législatif spécifique de l'Union et sur les motifs conduisant à considérer ces catégories comme hautement sensibles, en tenant compte des risques de réidentification de données anonymisées à caractère non personnel. Elles sont non discriminatoires et limitées à ce qui est nécessaire pour atteindre les objectifs de politique publique de l'Union définis dans ledit acte, conformément aux obligations internationales de l'Union.

Lorsque les actes législatifs spécifiques de l'Union visés au premier alinéa l'exigent, de telles conditions particulières peuvent notamment comprendre des conditions applicables au transfert ou des arrangements techniques à cet égard, des limitations en ce qui concerne la réutilisation de données dans des pays tiers ou les catégories de personnes habilitées à transférer ces données vers des pays tiers ou, dans des cas exceptionnels, des restrictions en ce qui concerne les transferts vers des pays tiers.

14. La personne physique ou morale à laquelle le droit de réutiliser des données à caractère non personnel a été accordé ne peut transférer ces données que vers les pays tiers pour lesquels il est satisfait aux exigences énoncées aux paragraphes 10, 12 et 13.

Article 6
Redevances

Redevances

1. Les organismes du secteur public qui autorisent la réutilisation des catégories de données visées à l'article 3, paragraphe 1, peuvent percevoir des redevances pour autoriser la réutilisation de ces données.

2. Les redevances perçues en vertu du paragraphe 1 sont transparentes, non discriminatoires, proportionnées et objectivement justifiées et ne restreignent pas la concurrence.

3. Les organismes du secteur public font en sorte que les redevances puissent aussi être acquittées en ligne au moyen de services de paiement transfrontaliers largement disponibles, sans discrimination fondée sur le lieu d'établissement du prestataire de services de paiement, le lieu d'émission de l'instrument de paiement ou la localisation du compte de paiement dans l'Union.

4. Lorsque les organismes du secteur public perçoivent des redevances, ils prennent des mesures pour inciter à la réutilisation des catégories de données visées à l'article 3, paragraphe 1, à des fins non commerciales, par exemple à des fins de recherche scientifique, ainsi que par les PME et les jeunes pousses conformément aux règles en matière d'aides d'État. À cet égard, les organismes du secteur public peuvent également mettre ces données à disposition moyennant une redevance réduite ou à titre gratuit, notamment pour les PME, les jeunes pousses, les organisations de la société civile et les établissements d'enseignement. À cette fin, les organismes du secteur public peuvent établir une liste des catégories de réutilisateurs pour lesquelles les données à des fins de réutilisation sont mises à disposition moyennant une redevance réduite ou à titre gratuit. Cette liste, ainsi que les critères utilisés pour l'établir, sont rendus publics.

5. Les redevances sont calculées sur la base des coûts liés à la conduite de la procédure de demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1, et limitées aux coûts nécessaires relatifs:

a) à la reproduction, à la fourniture et à la diffusion des données;

b) à l'acquisition des droits;

c) à l'anonymisation ou à d'autres formes de préparation des données à caractère personnel et des données commerciales confidentielles conformément à l'article 5, paragraphe 3;

d) à la maintenance de l'environnement de traitement sécurisé;

e) à l'acquisition du droit d'autoriser la réutilisation conformément au présent chapitre par des tiers extérieurs au secteur public; et

f) à l'assistance fournie aux réutilisateurs pour obtenir le consentement des personnes concernées et l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation.

6. Les critères et la méthode de calcul des redevances sont arrêtés par les États membres et publiés. L'organisme du secteur public publie une description des principales catégories de coûts et des règles utilisées pour la répartition des coûts.

Article 7
Organismes compétents

Organismes compétents

1. En vue d'effectuer les tâches visées au présent article, chaque État membre désigne un ou plusieurs organismes compétents, qui peuvent être compétents pour un secteur particulier, pour aider les organismes du secteur public qui octroient ou refusent l'accès aux fins de la réutilisation des catégories de données visées à l'article 3, paragraphe 1. Les États membres peuvent soit établir un ou plusieurs nouveaux organismes compétents, soit s'appuyer sur des organismes du secteur public ou sur des services internes d'organismes du secteur public existants qui remplissent les conditions fixées par le présent règlement.

2. Les organismes compétents peuvent également être habilités à octroyer l'accès aux fins de la réutilisation des catégories de données visées à l'article 3, paragraphe 1, en application des dispositions du droit de l'Union ou du droit national qui prévoient l'octroi d'un tel accès. Lorsqu'ils octroient ou refusent l'accès à des fins de réutilisation, les articles 4, 5, 6 et 9 s'appliquent à ces organismes compétents.

3. Les organismes compétents disposent des ressources juridiques, financières, techniques et humaines suffisantes pour mener à bien les tâches qui leur sont assignées, y compris des connaissances techniques nécessaires pour être en mesure de respecter le droit de l'Union ou le droit national applicable en ce qui concerne les régimes d'accès pour les catégories de données visées à l'article 3, paragraphe 1.

4. L'assistance prévue au paragraphe 1 consiste notamment, le cas échéant:

a) à fournir une assistance technique en mettant à disposition un environnement de traitement sécurisé pour donner accès à la réutilisation de données;

b) à fournir des orientations et une assistance technique sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles;

c) à fournir un soutien technique pour la pseudonymisation et à garantir le traitement des données d'une manière qui préserve efficacement le caractère privé, la confidentialité, l'intégrité et l'accessibilité des informations contenues dans les données pour lesquelles la réutilisation est autorisée, notamment les techniques d'anonymisation, de généralisation, de suppression et de randomisation des données à caractère personnel ou d'autres méthodes de préservation de la vie privée à la pointe de la technologie, et la suppression des informations commerciales confidentielles, y compris les secrets d'affaires ou les contenus protégés par des droits de propriété intellectuelle;

d) à aider les organismes du secteur public, le cas échéant, à fournir une assistance aux réutilisateurs pour demander le consentement des personnes concernées à la réutilisation ou l'autorisation des détenteurs de données conformément à leurs décisions spécifiques, y compris en ce qui concerne le territoire où le traitement des données est prévu et à aider les organismes du secteur public à mettre en place des mécanismes techniques permettant la transmission des demandes de consentement ou d'autorisation des réutilisateurs, lorsque cela est réalisable en pratique;

e) à fournir aux organismes du secteur public une assistance lorsqu'il s'agit d'évaluer l'adéquation des engagements contractuels pris par un réutilisateur en vertu de l'article 5, paragraphe 10.

5. Chaque État membre notifie à la Commission l'identité des organismes compétents désignés en application du paragraphe 1 au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure concernant l'identité de ces organismes compétents.

Les organismes compétents doivent être désignés avant le 24 septembre 2023.

Article 8
Points d'information unique

Points d'information unique

1. Les États membres veillent à ce que toutes les informations pertinentes concernant l'application des articles 5 et 6 soient disponibles et facilement accessibles par l'intermédiaire d'un point d'information unique. Les États membres établissent un nouvel organisme ou désignent un organisme existant ou une structure existante en tant que point d'information unique. Le point d'information unique peut être lié à des points d'information sectoriels, régionaux ou locaux. Les fonctions du point d'information unique peuvent être automatisées, à condition que l'organisme du secteur public apporte un soutien adéquat.

2. Le point d'information unique est compétent pour recevoir les demandes d'information ou demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1, et les transmettre, par des moyens automatisés lorsque cela est possible et opportun, aux organismes du secteur public compétents, ou aux organismes compétents visés à l'article 7, paragraphe 1, le cas échéant. Le point d'information unique met à disposition par voie électronique une liste de ressources consultable contenant un aperçu de toutes les ressources en données disponibles, y compris, le cas échéant, les ressources en données qui sont disponibles au niveau des points d'information sec-

toriels, régionaux ou locaux, avec des informations pertinentes décrivant les données disponibles, y compris au minimum le format et la taille des données ainsi que les conditions applicables à leur réutilisation.

3. Le point d'information unique peut établir un canal d'information distinct, simplifié et bien documenté pour les PME et les jeunes pousses, afin de répondre à leurs besoins et à leurs capacités en matière de demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1.

4. La Commission établit un point d'accès unique européen mettant à disposition un registre électronique consultable des données disponibles au niveau des points d'information uniques nationaux ainsi que d'autres informations sur la manière de demander des données par l'intermédiaire de ces points d'information uniques nationaux.

Article 9
Procédure relative aux demandes de réutilisation

Procédure de demande de réutilisation

1. Sauf si des délais plus courts ont été fixés conformément au droit national, les organismes du secteur public compétents ou les organismes compétents visés à l'article 7, paragraphe 1, adoptent une décision sur la demande de réutilisation des catégories de données visées à l'article 3, paragraphe 1, dans un délai de deux mois à compter de la date de réception de la demande.

En cas de demandes de réutilisation exceptionnellement détaillées et complexes, ce délai de deux mois peut être prolongé de trente jours au maximum. En pareils cas, les organismes du secteur public compétents ou les organismes compétents visés à l'article 7, paragraphe 1, informent le demandeur dès que possible de la nécessité d'un délai supplémentaire pour conduire la procédure, ainsi que des raisons qui justifient le retard.

2. Toute personne physique ou morale directement affectée par une décision visée au paragraphe 1 dispose d'un droit de recours effectif dans l'État membre dans lequel est situé ledit organisme. Un tel droit de recours est fixé par le droit national et inclut la possibilité d'un réexamen par un organisme impartial doté des compétences appropriées, telle que l'autorité nationale de la concurrence, l'autorité pertinente d'accès aux documents, l'autorité de contrôle établie conformément au règlement (UE) 2016/679 ou une autorité judiciaire nationale, dont les décisions sont contraignantes pour l'organisme du secteur public concerné ou l'organisme compétent concerné.

Droit de recours auprès de l'AdLC, la CADA, la CNIL, ou autorité judiciaire

cf. RGPD. Autorité de contrôle.

CHAPITRE III
Exigences applicables aux services d'intermédiation de données

Article 10
Services d'intermédiation de données

Services d'intermédiation de données

La fourniture des services d'intermédiation de données suivants respecte l'article 12 et est soumise à une procédure de notification:

a) les services d'intermédiation entre les détenteurs de données et les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres nécessaires pour permettre la fourniture desdits services; ces services peuvent comprendre des échanges bilatéraux ou multilatéraux de données ou la création de plateformes ou de bases de données permettant l'échange ou l'utilisation conjointe de données, ainsi que la mise en place d'une autre infrastructure spécifique pour l'interconnexion des détenteurs de données avec les utilisateurs de données;

b) les services d'intermédiation entre, d'une part, les personnes concernées qui cherchent à mettre à disposition leurs données à caractère personnel ou des personnes physiques qui cherchent à mettre à disposition des données à caractère non personnel et, d'autre part, les utilisateurs de données potentiels, y compris la mise à disposition des moyens techniques ou autres nécessaires pour permettre la fourniture desdits services, et notamment pour permettre l'exercice des droits des personnes concernées prévus par le règlement (UE) 2016/679;

cf. RGPD. Exercice des droits des personnes concernées.

c) les services de coopératives de données.

Article 11
Notification par des prestataires de services d'intermédiation de données

Notification par des prestataires de services d'intermédiation

1. Tout prestataire de services d'intermédiation de données qui a l'intention de fournir les services d'intermédiation de données visés à l'article 10 soumet une notification à l'autorité compétente en matière de services d'intermédiation de données.

2. Aux fins du présent règlement, un prestataire de services d'intermédiation de données qui a des établissements dans plusieurs États membres est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal, sans préjudice du droit de l'Union réglementant les actions transfrontalières en dommages et intérêts et les procédures connexes.

3. Un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union mais qui propose les services d'intermédiation de données visés à l'article 10 dans l'Union désigne un représentant légal dans l'un des États membres où il propose lesdits services.

Afin de garantir le respect du présent règlement, le représentant légal est mandaté par le prestataire de services d'intermédiation de données pour être contacté, en plus dudit prestataire ou à sa place, par les autorités compétentes pour les services d'intermédiation de données ou les personnes concernées et les détenteurs de données, sur toutes les questions liées aux services d'intermédiation de données fournis. Le représentant légal coopère avec les autorités compétentes pour les services d'intermédiation de données et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par le prestataire de services d'intermédiation de données pour garantir le respect du présent règlement.

Le prestataire de services d'intermédiation de données est considéré comme relevant de la compétence de l'État membre dans lequel se trouve le représentant légal. La désignation d'un représentant légal par le prestataire de services d'intermédiation de données est sans préjudice d'actions en justice qui pourraient être intentées contre le prestataire de services d'intermédiation de données.

4. Après avoir soumis une notification conformément au paragraphe 1, le prestataire de services d'intermédiation de données peut commencer l'activité sous réserve des conditions énoncées au présent chapitre.

5. La notification visée au paragraphe 1 donne au prestataire de services d'intermédiation de données le droit de fournir des services d'intermédiation de données dans tous les États membres.

6. La notification visée au paragraphe 1 comporte les renseignements suivants:

a) le nom du prestataire de services d'intermédiation de données;

b) le statut juridique, la forme, la structure de propriété et les filiales pertinentes du prestataire de services d'intermédiation de données ainsi que, lorsque le prestataire de services d'intermédiation de données est enregistré dans un registre de commerce ou dans un autre registre public national similaire, son numéro d'enregistrement;

c) l'adresse de l'éventuel établissement principal du prestataire de services d'intermédiation de données dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou l'adresse du représentant légal;

d) un site internet public contenant des informations complètes et à jour sur le prestataire de services d'intermédiation de données et ses activités, y compris au minimum les renseignements visés aux points a), b), c) et f);

e) les personnes de contact et les coordonnées du prestataire de services d'intermédiation de données;

f) une description du service d'intermédiation de données que le prestataire de services d'intermédiation de données a l'intention de fournir, ainsi qu'une indication des catégories énumérées à l'article 10 dont relève ce service d'intermédiation de données;

g) une estimation de la date de lancement de l'activité, si celle-ci est différente de la date de la notification.

7. L'autorité compétente en matière de services d'intermédiation de données veille à ce que la procédure de notification soit non discriminatoire et ne fausse pas la concurrence.

8. À la demande du prestataire de services d'intermédiation de données, l'autorité compétente en matière de services d'intermédiation de données délivre, dans un délai d'une semaine à partir du moment où la notification est dûment et entièrement complétée, une déclaration standardisée confirmant que le prestataire de services d'intermédiation de données a soumis la notification visée au paragraphe 4 et que cette notification contient les informations visées au paragraphe 6.

9. À la demande du prestataire de services d'intermédiation de données, l'autorité compétente en matière de services d'intermédiation de données confirme que le prestataire de services d'intermédiation de données respecte le présent article et l'article 12. Dès réception de cette confirmation, ledit prestataire de services d'intermédiation de données peut utiliser le label «prestataire de services d'intermédiation de données reconnu dans l'Union» dans ses communications écrites et orales, ainsi qu'un logo commun.

Afin de garantir que les prestataires de services d'intermédiation de données reconnus dans l'Union sont facilement identifiables dans toute l'Union, la Commission conçoit le logo commun par la voie d'actes d'exécution. Les prestataires de services d'intermédiation de données reconnus dans l'Union affichent clairement le logo commun sur chaque publication en ligne et hors ligne qui se rapporte à leurs activités d'intermédiation de données.

Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

10. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission, sans retard et par voie électronique, toute nouvelle notification. La Commission tient et met régulièrement à jour un registre public de tous les prestataires de services d'intermédiation de données proposant leurs services dans l'Union. Les informations visées au paragraphe 6, points a), b), c), d), f) et g), sont publiées dans le registre public.

11. L'autorité compétente en matière de services d'intermédiation de données peut percevoir des redevances pour la notification conformément au droit national. Ces redevances sont proportionnées et objectives et sont fondées sur les coûts administratifs liés au contrôle du respect des dispositions et aux autres activités de contrôle du marché menées par les autorités compétentes en matière de services d'intermédiation de données en rapport avec les notifications des prestataires de services d'intermédiation de données. Dans le cas des PME et des jeunes pousses, l'autorité compétente en matière de services d'intermédiation de données peut percevoir une redevance réduite ou renoncer à la redevance.

12. Les prestataires de services d'intermédiation de données notifient à l'autorité compétente en matière de services d'intermédiation de données toute modification des renseignements communiqués en vertu du paragraphe 6 dans un délai de quatorze jours à compter de la date de la modification.

13. Lorsqu'un prestataire de services d'intermédiation de données cesse ses activités, il le notifie dans un délai de quinze jours à l'autorité compétente en matière de services d'intermédiation de données concernée, déterminée conformément aux paragraphes 1, 2 et 3.

14. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission, sans retard et par voie électronique, chaque notification visée aux

paragraphes 12 et 13. La Commission met à jour en conséquence le registre public des prestataires de services d'intermédiation de données dans l'Union.

Article 12
Conditions liées à la fourniture de services d'intermédiation de données

Conditions de fourniture de services d'intermédiation

La fourniture de services d'intermédiation de données visés à l'article 10 est soumise aux conditions suivantes:

a) le prestataire de services d'intermédiation de données ne peut pas utiliser les données pour lesquelles il fournit des services d'intermédiation de données à des fins autres que leur mise à disposition des utilisateurs de données, et il fournit les services d'intermédiation de données par l'intermédiaire d'une personne morale distincte;

b) les modalités commerciales, y compris la tarification, de la fourniture de services d'intermédiation de données à un détenteur de données ou à un utilisateur de données ne doivent pas être subordonnées au fait que le détenteur de données ou l'utilisateur de données utilise ou non d'autres services fournis par le même prestataire de services d'intermédiation de données ou par une entité liée, et dans l'affirmative, à la mesure dans laquelle le détenteur de données ou l'utilisateur de données utilise ces autres services;

c) les données collectées en ce qui concerne toute activité d'une personne physique ou morale aux fins de la fourniture d'un service d'intermédiation de données, notamment la date, l'heure et les données de géolocalisation, la durée de l'activité et les connexions établies avec d'autres personnes physiques ou morales par la personne qui utilise le service d'intermédiation de données ne doivent être utilisées que pour le développement dudit service d'intermédiation de données, ce qui peut impliquer l'utilisation de données pour la détection de fraudes ou pour la cybersécurité, et sont mises à la disposition des détenteurs de données sur demande;

d) le prestataire de services d'intermédiation de données facilite l'échange des données au format dans lequel il les reçoit d'une personne concernée ou d'un détenteur des données, ne convertit les données dans des formats spécifiques que pour améliorer l'interopérabilité intrasectorielle et transsectorielle, ou si l'utilisateur de données le demande, ou lorsque le droit de l'Union le requiert, ou pour assurer l'harmonisation avec des normes internationales ou européennes en matière de données, et donne aux personnes concernées ou aux détenteurs de données une possibilité de non-participation en ce qui concerne ces conversions, à moins que la conversion ne soit requise par le droit de l'Union;

e) les services d'intermédiation de données peuvent prévoir de fournir aux détenteurs de données ou aux personnes concernées des instruments et services spécifiques supplémentaires dans le but particulier de faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation, ces instruments étant uniquement utilisés à la demande expresse ou moyennant l'approbation expresse du détenteur de données ou de la personne concernée et les instruments de tiers proposés dans ce contexte nétant pas utilisés à d'autres fins;

f) le prestataire de services d'intermédiation de données veille à ce que la procédure d'accès à son service soit équitable, transparente et non discriminatoire à l'égard tant des personnes concernées et des détenteurs de données que des utilisateurs de données, y compris en ce qui concerne les prix et les conditions de service;

g) le prestataire de services d'intermédiation de données met en place des procédures pour prévenir les pratiques frauduleuses ou abusives en lien avec des parties cherchant à obtenir un accès via ses services d'intermédiation de données;

h) en cas d'insolvabilité, le prestataire de services d'intermédiation de données assure une continuité raisonnable de la fourniture de ses services d'intermédiation de données et, lorsque ces services d'intermédiation de données assurent le stockage de données, il met en place des mécanismes pour permettre aux détenteurs de données et aux utilisateurs de données d'avoir accès à leurs données, de les transférer ou de les extraire et, lorsque ces services d'intermédiation de données sont fournis entre des personnes

concernées et des utilisateurs de données, pour permettre aux personnes concernées d'exercer leurs droits;

i) le prestataire de services d'intermédiation de données prend les mesures appropriées pour assurer l'interopérabilité avec d'autres services d'intermédiation de données, entre autres au moyen de normes ouvertes communément utilisées dans le secteur dans lequel le prestataire de services d'intermédiation de données exerce ses activités;

j) le prestataire de services d'intermédiation de données met en place des mesures techniques, juridiques et organisationnelles appropriées afin d'empêcher le transfert de données à caractère non personnel ou l'accès à celles-ci dans les cas où ils sont illicites au regard du droit de l'Union ou du droit national de l'État membre concerné;

k) le prestataire de services d'intermédiation de données informe sans retard les détenteurs de données en cas de transfert, d'accès ou d'utilisation non autorisés portant sur les données à caractère non personnel qu'il a partagées;

l) le prestataire de services d'intermédiation de données prend les mesures nécessaires pour garantir un niveau de sécurité approprié pour le stockage, le traitement et la transmission de données à caractère non personnel, et le prestataire de services d'intermédiation de données garantit également le niveau de sécurité le plus élevé pour le stockage et la transmission d'informations sensibles sous l'angle de la concurrence;

m) le prestataire de services d'intermédiation de données proposant des services à des personnes concernées agit au mieux de leurs intérêts lorsqu'il facilite l'exercice de leurs droits, notamment en informant et, le cas échéant, en conseillant les personnes concernées de manière concise, transparente, compréhensible et aisément accessible sur les utilisations prévues des données par les utilisateurs de données et sur les conditions générales applicables à ces utilisations, avant que les personnes concernées ne donnent leur consentement;

n) lorsqu'un prestataire de services d'intermédiation de données fournit des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données, il précise, le cas échéant, la juridiction des pays tiers où l'utilisation des données est prévue et fournit aux personnes concernées des outils permettant à la fois de donner et de retirer leur consentement et aux détenteurs de données des outils permettant à la fois de donner et de retirer l'autorisation de traiter des données;

o) le prestataire de services d'intermédiation de données tient un journal de l'activité d'intermédiation de données.

Article 13
Autorités compétentes en matière de services d'intermédiation de données

Autorités compétentes pour les serices d'intermédiation

1. Chaque État membre désigne une ou plusieurs autorités compétentes pour effectuer les tâches liées à la procédure de notification pour les services d'intermédiation de données et notifie à la Commission l'identité de ces autorités compétentes au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure de l'identité de ces autorités compétentes.

Les autorités compétentes pour les services d'intermédiation doivent être identifiées avant le 24 septembre 2023

2. Les autorités compétentes en matière de services d'intermédiation de données respectent les exigences énoncées à l'article 26.

3. Les pouvoirs des autorités compétentes en matière de services d'intermédiation de données sont sans préjudice des pouvoirs des autorités chargées de la protection des données, des autorités nationales de la concurrence, des autorités chargées de la cybersécurité et des autres autorités sectorielles concernées. Dans le respect de leurs compétences respectives au titre du droit de l'Union et du droit national, ces autorités établissent une coopération solide et échangent les informations qui sont nécessaires à l'accomplissement de leurs tâches en rapport avec les prestataires de services d'intermédiation de données, et visent à assurer la cohérence des décisions prises en application du présent règlement.

Article 14
Contrôle du respect des dispositions

Contrôle du respect des dispositions

1. Les autorités compétentes en matière de services d'intermédiation de données contrôlent et surveillent le respect par les prestataires de services d'intermédiation de données des exigences énoncées dans le présent chapitre. Les autorités compétentes en matière de services d'intermédiation de données peuvent également contrôler et surveiller le respect par les prestataires de services d'intermédiation de données de leurs obligations, sur la base d'une demande présentée par une personne physique ou morale.

2. Les autorités compétentes en matière de services d'intermédiation de données ont le pouvoir de demander aux prestataires de services d'intermédiation de données ou à leurs représentants légaux toutes les informations nécessaires pour vérifier le respect des exigences énoncées dans le présent chapitre. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.

3. Lorsque l'autorité compétente en matière de services d'intermédiation de données constate qu'un prestataire de services d'intermédiation de données ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre, elle notifie ces constatations audit prestataire de services d'intermédiation de données et lui donne la possibilité d'exposer son point de vue dans un délai de trente jours à compter de la réception de la notification.

4. L'autorité compétente en matière de services d'intermédiation de données a le pouvoir d'exiger qu'il soit mis fin à l'infraction visée au paragraphe 3, dans un délai raisonnable, ou immédiatement dans le cas d'une infraction grave, et prend des mesures appropriées et proportionnées visant à garantir le respect des obligations. À cet égard, les autorités compétentes en matière de services d'intermédiation de données ont le pouvoir, le cas échéant:

a) d'imposer, par le biais de procédures administratives, des sanctions financières dissuasives, pouvant comporter des astreintes et des sanctions avec effet rétroactif, d'engager des procédures judiciaires en vue d'infliger des amendes, ou les deux;

b) d'exiger un report du début de la fourniture du service d'intermédiation de données ou une suspension de cette fourniture jusqu'à ce que les modifications des conditions demandées par l'autorité compétente en matière de services d'intermédiation de données aient été réalisées; ou

c) d'exiger la cessation de la fourniture du service d'intermédiation de données dans le cas où il n'a pas été remédié à des infractions graves ou répétées malgré l'envoi d'une notification préalable conformément au paragraphe 3.

L'autorité compétente en matière de services d'intermédiation de données demande à la Commission de radier le prestataire de services d'intermédiation de données du registre des prestataires de services d'intermédiation de données, une fois qu'elle a ordonné la cessation de la fourniture du service d'intermédiation de données conformément au premier alinéa, point c).

Si un prestataire de service d'intermédiation de données remédie aux infractions, ledit prestataire de service d'intermédiation de données adresse une nouvelle notification à l'autorité compétente en matière de services d'intermédiation de données. L'autorité compétente en matière de services d'intermédiation de données notifie à la Commission chaque nouvelle renotification.

5. Lorsqu'un prestataire de services d'intermédiation de données qui n'est pas établi dans l'Union ne désigne pas de représentant légal ou que ce représentant légal, bien que l'autorité compétente en matière de services d'intermédiation de données lui en fasse la demande, ne fournit pas les informations nécessaires prouvant de manière exhaustive le respect du présent règlement, l'autorité compétente en matière de services d'intermédiation de données a le pouvoir de reporter le début de la fourniture du service d'intermédiation de données ou de suspendre cette fourniture jusqu'à ce que le représentant légal soit désigné ou que les informations nécessaires soient fournies.

6. Les autorités compétentes en matière de services d'intermédiation de données notifient sans retard au prestataire de services d'intermédiation de données concerné les mesures imposées au titre des paragraphes 4 et 5, leur motivation, ainsi que les mesures dont l'adoption est nécessaire pour corriger les manquements constatés, et fixent au prestataire de services d'intermédiation de données concerné un délai raisonnable, ne dépassant pas trente jours, pour se conformer à ces mesures.

7. Si un prestataire de services d'intermédiation de données a son établissement principal ou son représentant légal dans un État membre mais fournit des services dans d'autres États membres, l'autorité compétente en matière de services d'intermédiation de données de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes en matière de services d'intermédiation de données de ces autres États membres coopèrent et se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes en matière de services d'intermédiation de données concernées aux fins de l'accomplissement de leurs tâches au titre du présent règlement et sur les demandes motivées de prendre les mesures visées au présent article.

Lorsqu'une autorité compétente en matière de services d'intermédiation de données dans un État membre sollicite l'assistance d'une autorité compétente en matière de services d'intermédiation de données d'un autre État membre, elle présente une demande motivée. Lorsqu'elle reçoit une telle demande, l'autorité compétente en matière de services d'intermédiation de données fournit une réponse sans retard et dans des délais proportionnés à l'urgence de la demande.

Toutes les informations échangées dans le cadre de la demande d'assistance et fournies au titre du présent paragraphe ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 15
Dérogations

Dérogations

Le présent chapitre ne s'applique pas aux organisations altruistes en matière de données reconnues ni aux autres entités sans but lucratif dans la mesure où leurs activités consistent à collecter, pour des objectifs d'intérêt général, des données mises à disposition par des personnes physiques ou morales sur le fondement de l'altruisme en matière de données, à moins que ces organisations et entités ne visent à établir des relations commerciales entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et des utilisateurs de données, d'autre part.

CHAPITRE IV
Altruisme en matière de données

Altruisme en matière de données

Article 16
Dispositions nationales relatives à l'altruisme en matière de données

Les États membres peuvent avoir mis en place des dispositions organisationnelles ou techniques, ou les deux, pour faciliter l'altruisme en matière de données. À cette fin, les États membres peuvent élaborer des politiques nationales dans le domaine de l'altruisme en matière de données. Ces politiques nationales peuvent notamment aider les personnes concernées à mettre à disposition volontairement, à des fins d'altruisme en matière de données, des données à caractère personnel les concernant détenues par des organismes du secteur public, et déterminer les informations nécessaires qui doivent être fournies aux personnes concernées en ce qui concerne la réutilisation de leurs données dans l'intérêt général.

Si un État membre élabore de telles politiques nationales, il le notifie à la Commission.

Article 17
Registres publics d'organisations altruistes en matière de données reconnues

Registre des organisations altruistes

1. Chaque autorité compétente pour l'enregistrement des organisations altruistes en matière de données tient et met à jour régulièrement un registre public national des organisations altruistes en matière de données reconnues.

2. La Commission gère, à des fins d'information, un registre public de l'Union des organisations altruistes en matière de données reconnues. Dès lors qu'une entité est enregistrée dans le registre public national des organisations altruistes en matière de données reconnues conformément à l'article 18, elle peut utiliser le label «organisation altruiste en matière de données reconnue dans l'Union» dans ses communications écrites et orales, ainsi qu'un logo commun.

Afin de garantir que les organisations altruistes en matière de données reconnues soient facilement identifiables dans toute l'Union, la Commission conçoit un logo commun par voie d'actes d'exécution. Les organisations altruistes en matière de données reconnues affichent clairement le logo commun sur chaque publication en ligne et hors ligne qui se rapporte à leurs activités altruistes en matière de données. Le logo commun s'accompagne d'un code QR comportant un lien vers le registre public de l'Union des organisations altruistes en matière de données reconnues.

Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

Article 18
Conditions générales d'enregistrement

Conditions d'enregistrement

Pour être admise à l'enregistrement dans un registre public national des organisations altruistes en matière de données reconnues, une entité doit:

a) mener des activités altruistes en matière de données;

b) être une personne morale constituée en vertu du droit national pour poursuivre des objectifs d'intérêt général prévus dans le droit national, le cas échéant;

c) exercer ses activités dans un but non lucratif et être juridiquement indépendante de toute entité exerçant des activités dans un but lucratif;

d) mener ses activités altruistes en matière de données par l'intermédiaire d'une structure qui, sur le plan fonctionnel, est distincte de ses autres activités;

e) se conformer au recueil de règles visé à l'article 22, paragraphe 1, au plus tard dix-huit mois après la date d'entrée en vigueur des actes délégués visés audit paragraphe.

Article 19
Enregistrement d'organisations altruistes en matière de données reconnues

Enregistrement d'organisations altruistes

1. Une entité qui satisfait aux exigences énoncées à l'article 18 peut présenter une demande d'enregistrement dans le registre public national des organisations altruistes en matière de données reconnues dans l'État membre dans lequel elle est établie.

2. Une entité qui satisfait aux exigences énoncées à l'article 18 et a des établissements dans plusieurs États membres peut présenter une demande d'enregistrement dans le registre public national des organisations altruistes en matière de données reconnues dans l'État membre dans lequel elle a son établissement principal.

3. Une entité qui satisfait aux exigences énoncées à l'article 18 mais qui n'est pas établie dans l'Union désigne un représentant légal dans l'un des États membres dans lesquels les services fondés sur l'altruisme en matière de données sont proposés.

Aux fins de garantir le respect du présent règlement, le représentant légal est mandaté par l'entité pour être contacté, en plus de ladite entité ou à sa place, par les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ou les personnes concernées et les détenteurs de données, sur toutes les questions liées à ladite entité. Le représentant légal coopère avec les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par l'entité pour garantir le respect du présent règlement.

L'entité est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son représentant légal. Une telle entité peut présenter une demande d'enre-

gistrement dans le registre public national des organisations altruistes en matière de données reconnues dans cet État membre. La désignation d'un représentant légal par l'entité est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité.

4. Les demandes d'enregistrement visées aux paragraphes 1, 2 et 3 comportent les renseignements suivants:

a) le nom de l'entité;

b) le statut juridique et la forme de l'entité ainsi que, lorsque l'entité est enregistrée dans un registre public national, son numéro d'enregistrement;

c) les statuts de l'entité, le cas échéant;

d) les sources de revenus de l'entité;

e) l'adresse de l'éventuel établissement principal de l'entité dans l'Union et, le cas échéant, de toute succursale dans un autre État membre, ou l'adresse du représentant légal;

f) un site internet public contenant des informations complètes et à jour sur l'entité et ses activités, y compris au minimum les renseignements visés aux points a), b), d), e) et h);

g) les personnes de contact et les coordonnées de l'entité;

h) les objectifs d'intérêt général qu'elle entend promouvoir par la collecte de données;

i) la nature des données que l'entité entend contrôler ou traiter et, dans le cas des données à caractère personnel, une indication des catégories de données à caractère personnel;

j) tout autre document démontrant qu'il est satisfait aux exigences énoncées à l'article 18.

5. Lorsque l'entité a fourni tous les renseignements nécessaires en vertu du paragraphe 4 et après que l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données a évalué la demande d'enregistrement et établi que l'entité satisfait aux exigences énoncées à l'article 18, ladite autorité enregistre l'entité dans le registre public national des organisations altruistes en matière de données reconnues, dans un délai de douze semaines suivant la date de réception de la demande d'enregistrement. L'enregistrement est valable dans tous les États membres.

L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données notifie tout enregistrement à la Commission. La Commission fait figurer l'enregistrement concerné dans le registre public de l'Union des organisations altruistes en matière de données reconnues.

6. Les renseignements visés au paragraphe 4, points a), b), f), g) et h), sont publiés dans le registre public national des organisations altruistes en matière de données reconnues concerné.

7. L'organisation altruiste en matière de données reconnue notifie à l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée toute modification des renseignements communiqués en vertu du paragraphe 4 dans un délai de quatorze jours à compter de la date de la modification.

L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données notifie à la Commission, sans retard et par voie électronique, chaque notification de ce type. Sur la base d'une telle notification, la Commission met à jour, sans retard, le registre public de l'Union des organisations altruistes en matière de données reconnues.

Article 20
Obligations de transparence

Transparence

1. L'organisation altruiste en matière de données reconnue tient des registres complets et exacts concernant:

a) toutes les personnes physiques ou morales qui se sont vu offrir la possibilité de traiter des données détenues par cette organisation altruiste en matière de données reconnue, ainsi que leurs coordonnées;

b) la date ou la durée du traitement des données à caractère personnel ou de l'utilisation des données à caractère non personnel;

c) la finalité du traitement, telle qu'elle a été déclarée par la personne physique ou morale qui s'est vu offrir la possibilité d'effectuer ce traitement;

d) les éventuelles redevances acquittées par les personnes physiques ou morales traitant les données.

2. L'organisation altruiste en matière de données reconnue établit et transmet à l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée un rapport annuel d'activité qui contient au moins les éléments suivants:

a) des informations sur les activités de l'organisation altruiste en matière de données reconnue;

b) une description de la manière dont les objectifs d'intérêt général pour lesquels des données ont été collectées ont été promus pendant l'exercice considéré;

c) une liste de toutes les personnes physiques et morales qui ont été autorisées à traiter des données qu'elle détient, assortie d'une description sommaire des objectifs d'intérêt général poursuivis par ce traitement de données et de la description des moyens techniques employés en vue de cette utilisation, y compris une description des techniques appliquées pour préserver la vie privée et la protection des données;

d) une synthèse des résultats du traitement des données autorisé par l'organisation altruiste en matière de données reconnue, s'il y a lieu;

e) des informations sur les sources de recettes de l'organisation altruiste en matière de données reconnue, en particulier toutes les recettes résultant de l'autorisation d'accès aux données, et sur les dépenses.

Article 21
Exigences spécifiques visant à préserver les droits et intérêts des personnes concernées et des détenteurs de données quant à leurs données

Droits et intéreêts des personnes concernées et des détenteurs de données

1. L'organisation altruiste en matière de données reconnue informe les personnes concernées ou les détenteurs de données préalablement à tout traitement de leurs données d'une manière claire et aisément intelligible:

a) des objectifs d'intérêt général et, le cas échéant, de la finalité déterminée, explicite et légitime pour laquelle les données à caractère personnel doivent être traitées et pour laquelle elle autorise le traitement de données les concernant par un utilisateur de données;

b) de la localisation de tout traitement effectué dans un pays tiers et des objectifs d'intérêt général pour lesquels elle autorise ledit traitement, lorsque le traitement est effectué par l'organisation altruiste en matière de données reconnue.

2. L'organisation altruiste en matière de données reconnue n'utilise pas les données pour des objectifs autres que ceux d'intérêt général pour lesquels la personne concernée ou le détenteur des données autorise le traitement. L'organisation altruiste en matière de données reconnue ne recourt pas à des pratiques commerciales trompeuses pour solliciter la fourniture de données.

3. L'organisation altruiste en matière de données reconnue fournit des outils permettant d'obtenir le consentement des personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données. L'organisation altruiste en matière de données reconnue fournit également des outils permettant de retirer facilement ce consentement ou cette autorisation.

4. L'organisation altruiste en matière de données reconnue prend des mesures pour assurer un niveau de sécurité approprié pour le stockage et le traitement des données à caractère non personnel qu'elle a collectées sur le fondement de l'altruisme en matière de données.

5. L'organisation altruiste en matière de données reconnue informe, sans retard, les détenteurs de données de tout transfert, de tout accès ou de toute utilisation non autorisés portant sur les données à caractère non personnel qu'elle a partagées.

6. Lorsque l'organisation altruiste en matière de données reconnue facilite le traitement de données par des tiers, y compris en fournissant des outils permettant d'obtenir le consentement de personnes concernées ou l'autorisation de traiter des données mises à disposition par des détenteurs de données, elle précise, le cas échéant, la juridiction du pays tiers où l'utilisation des données est prévue.

Article 22
Recueil de règles

Recueil de règles

1. La Commission adopte des actes délégués conformément à l'article 32 afin de compléter le présent règlement en établissant un recueil de règles fixant:

a) des exigences appropriées en matière d'information pour veiller à ce que les personnes concernées et les détenteurs de données reçoivent, avant qu'un consentement ou une autorisation ne soit donné pour l'altruisme en matière de données, des informations suffisamment détaillées, claires et transparentes concernant l'utilisation des données, les outils permettant de donner et de retirer le consentement ou l'autorisation, et les mesures prises pour éviter une mauvaise utilisation des données partagées avec l'organisation altruiste en matière de données;

b) des exigences techniques et de sécurité appropriées pour garantir un niveau de sécurité approprié pour le stockage et le traitement des données, ainsi que pour les outils permettant de donner et de retirer le consentement ou l'autorisation;

c) des feuilles de route en matière de communication adoptant une approche pluridisciplinaire pour sensibiliser à l'altruisme en matière de données, à la désignation en tant que «organisation altruiste en matière de données reconnue dans l'Union» et au recueil de règles les parties prenantes concernées, notamment les détenteurs de données et les personnes concernées pouvant potentiellement partager leurs données;

d) des recommandations relatives aux normes d'interopérabilité pertinentes.

2. Le recueil de règles visé au paragraphe 1 est élaboré en étroite coopération avec les organisations altruistes en matière de données et les parties prenantes concernées.

Article 23
Autorités compétentes pour l'enregistrement des organisations altruistes en matière de données

Autorités d'enregistrement des organisations altruistes

1. Chaque État membre désigne une ou plusieurs autorités compétentes responsables de son registre public national des organisations altruistes en matière de données reconnues.

Les autorités compétentes pour l'enregistrement d'organisations altruistes en matière de données respectent les exigences énoncées à l'article 26.

2. Chaque État membre notifie à la Commission l'identité de leurs autorités compétentes pour l'enregistrement des organisations altruistes en matière de données au plus tard le 24 septembre 2023. Chaque État membre notifie également à la Commission toute modification ultérieure de l'identité desdites autorités compétentes.

3. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données d'un État membre accomplit ses tâches en coopération avec l'autorité chargée de la protection des données concernée, lorsque ces tâches se rapportent au traitement de données à caractère personnel, et avec les autorités sectorielles concernées dudit État membre.

Coopération avec l'autorité de protection des données.

Article 24
Contrôle du respect des dispositions

Contrôle du respect des dispositions

1. Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données contrôlent et surveillent le respect, par les organisations altruistes en matière de données reconnues, des exigences énoncées dans le présent chapitre. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données peut également contrôler et surveiller le respect par de telles organisations altruistes en matière de données reconnues de leurs obligations sur la base d'une demande présentée par une personne physique ou morale.

2. Les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ont le pouvoir de demander aux organisations altruistes en matière de données reconnues les informations qui lui sont nécessaires pour vérifier qu'elles respectent les exigences énoncées dans le présent chapitre. Toute demande d'information est proportionnée à l'accomplissement de la tâche et est motivée.

3. Lorsque l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données constate qu'une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre, elle notifie ces constatations à l'organisation altruiste en matière de données reconnue et lui donne la possibilité d'exposer son point de vue dans un délai de trente jours à compter de la réception de la notification.

4. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données a le pouvoir d'exiger qu'il soit mis fin à l'infraction visée au paragraphe 3, soit immédiatement soit dans un délai raisonnable, et prend des mesures appropriées et proportionnées pour garantir le respect des dispositions.

5. Si une organisation altruiste en matière de données reconnue ne respecte pas une ou plusieurs des exigences énoncées dans le présent chapitre même après avoir reçu une notification de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données conformément au paragraphe 3, ladite organisation altruiste en matière de données reconnue:

a) perd le droit d'utiliser le label d'«organisation altruiste en matière de données reconnue dans l'Union» dans toute communication écrite et orale;

b) est radiée du registre public national des organisations altruistes en matière de données reconnues concerné et du registre public de l'Union des organisations altruistes en matière de données reconnues.

Toute décision révoquant le droit d'utiliser le label d'«organisation altruiste en matière de données reconnue dans l'Union» prévue au premier alinéa, point a), est rendue publique par l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données.

6. Si une organisation altruiste en matière de données reconnue a son établissement principal ou son représentant légal dans un État membre mais qu'elle exerce des activités dans d'autres États membres, l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données de l'État membre où est situé l'établissement principal ou dans lequel se trouve le représentant légal et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de ces autres États membres coopèrent et se prêtent assistance. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données concernées aux fins de l'accomplissement de leurs tâches au titre du présent règlement et sur les demandes motivées de prendre les mesures visées au présent article.

Lorsqu'une autorité compétente pour l'enregistrement des organisations altruistes en matière de données dans un État membre sollicite l'assistance d'une autorité compétente pour l'enregistrement des organisations altruistes en matière de données dans un autre État membre, elle présente une demande motivée. L'autorité compétente pour l'enregistrement des organisations altruistes en matière de données veille, à la suite d'une telle demande, à fournir une réponse sans retard et dans des délais proportionnés à l'urgence de la demande.

Toutes les informations échangées dans le cadre de la demande d'assistance et fournies au titre du présent paragraphe ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 25
Formulaire européen de consentement à l'altruisme en matière de données

Formulaire européen de consentement pour l'altruisme

1. Afin de faciliter la collecte de données fondée sur l'altruisme en matière de données, la Commission adopte des actes d'exécution établissant et développant un formulaire européen de consentement à l'altruisme en matière de données, après consultation du comité européen de la protection des données, en tenant compte des avis du comité européen de l'innovation dans le domaine des données et en associant dûment les parties prenantes concernées. Le formulaire permet de recueillir le consentement ou l'autorisation dans tous les États membres selon un format uniforme. Ces actes d'exécution sont adoptés en conformité avec la procédure consultative visée à l'article 33, paragraphe 2.

Consultation du CEPD/EDPB

2. Le formulaire européen de consentement à l'altruisme en matière de données est conçu selon une approche modulaire permettant son adaptation à des secteurs particuliers et à des fins différentes.

3. Lorsque des données à caractère personnel sont communiquées, le formulaire européen de consentement à l'altruisme en matière de données garantit que les personnes concernées sont en mesure de donner et de retirer leur consentement à une opération particulière de traitement de données en conformité avec les exigences du règlement (UE) 2016/679.

cf. RGPD. Formulaire de consentement et retrait du consentement.

4. Le formulaire est disponible de manière à pouvoir être imprimé sur papier tout en étant facile à comprendre, ainsi que sous une forme électronique lisible par machine.

CHAPITRE V
Autorités compétentes et dispositions procédurales

Article 26
Exigences relatives aux autorités compétentes

Exigences relatives aux autorités compétentes

1. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données sont juridiquement distinctes et fonctionnellement indépendantes de tout prestataire de services d'intermédiation de données ou de toute organisation altruiste en matière de données reconnue. Les fonctions des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données peuvent être exercées par la même autorité. Les États membres peuvent soit établir une ou plusieurs nouvelles autorités à ces fins, soit s'appuyer sur des autorités existantes.

2. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données accomplissent leurs tâches de manière impartiale, transparente, cohérente, fiable et rapide. Dans l'exercice de leurs tâches, elles préservent une concurrence loyale et veillent à l'absence de discrimination.

Les autorités compétentes doivent être : indépendantes, impartiales, transparentes, cohérentes, fiables, rapides.

3. Les cadres supérieurs et le personnel chargé d'accomplir les tâches concernées des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ne peuvent pas être le concepteur, le fabricant, le fournisseur, l'installateur,

l'acheteur, le propriétaire, l'utilisateur ou le responsable de la maintenance des services qu'ils évaluent, ni le représentant autorisé d'aucune de ces parties. Cela n'exclut pas l'utilisation de services évalués qui sont nécessaires au fonctionnement de l'autorité compétente en matière de services d'intermédiation de données et de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données, ou l'utilisation de ces services à des fins personnelles.

4. Les cadres supérieurs et le personnel des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données ne participent à aucune activité susceptible d'entrer en conflit avec l'indépendance de leur jugement ou leur intégrité en lien avec les activités d'évaluation qui leur sont assignées.

5. Les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données disposent des ressources humaines et financières suffisantes, y compris des connaissances et ressources techniques nécessaires, pour mener à bien les tâches qui leur sont assignées.

6. Sur demande motivée et sans retard, les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données d'un État membre fournissent à la Commission et aux autorités compétentes en matière de services d'intermédiation de données et aux autorités compétentes pour l'enregistrement des organisations altruistes en matière de données d'autres États membres les informations nécessaires à l'accomplissement des tâches qui leur incombent au titre du présent règlement. Lorsqu'une autorité compétente en matière de services d'intermédiation de données ou une autorité compétente pour l'enregistrement des organisations altruistes en matière de données considère que les informations demandées sont confidentielles selon les dispositions du droit de l'Union et du droit national relatives à la confidentialité commerciale et au secret professionnel, la Commission et toutes les autres autorités compétentes en matière de services d'intermédiation de données ou les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données concernées garantissent cette confidentialité et ce secret.

Article 27
Droit d'introduire une réclamation

Réclamations

1. Les personnes physiques et morales ont le droit d'introduire une réclamation concernant toute question relevant du champ d'application du présent règlement, individuellement ou, le cas échéant, collectivement, auprès de l'autorité compétente en matière de services d'intermédiation de données concernée contre un prestataire de services d'intermédiation de données ou auprès de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données concernée contre une organisation altruiste en matière de données reconnue.

2. L'autorité compétente en matière de services d'intermédiation de données ou l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation:

a) de l'état d'avancement de la procédure et de la décision prise; et

b) des recours juridictionnels prévus à l'article 28.

Article 28
Droit à un recours juridictionnel effectif

Recours juridictionnel

1. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, toute personne physique ou morale lésée dispose du droit à un recours juridictionnel effectif en ce qui concerne les décisions juridiquement contraignantes visées à l'article 14 prises par les autorités compétentes en matière de services d'intermédiation de données dans le domaine de la gestion, du contrôle et de la mise en œuvre du régime de notification pour les prestataires de services d'intermédiation de données et les décisions juridiquement contraignantes visées aux articles 19 et 24 prises par les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données

dans le domaine du contrôle des organisations altruistes en matière de données reconnues.

2. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre de l'autorité compétente en matière de services d'intermédiation de données ou de l'autorité compétente pour l'enregistrement des organisations altruistes en matière de données contre laquelle le recours juridictionnel a été formé individuellement ou, le cas échéant, collectivement par les représentants d'une ou de plusieurs personnes physiques ou morales.

3. Lorsqu'une autorité compétente en matière de services d'intermédiation de données ou une autorité compétente pour l'enregistrement des organisations altruistes en matière de données ne donne pas suite à une réclamation, toute personne physique ou morale lésée a, conformément au droit national, soit le droit à un recours juridictionnel effectif, soit accès à un réexamen réalisé par un organe impartial doté des compétences appropriées.

CHAPITRE VI
Comité européen de l'innovation dans le domaine des données

Comité européen de l'innovation dans le domaine des données

Article 29
Comité européen de l'innovation dans le domaine des données

1. La Commission institue un comité européen de l'innovation dans le domaine des données sous la forme d'un groupe d'experts, qui se compose de représentants des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données de tous les États membres, du comité européen de la protection des données, du Contrôleur européen de la protection des données, de l'ENISA, de la Commission, du représentant de l'UE pour les PME ou d'un représentant désigné par le réseau des représentants des PME, et d'autres représentants d'organismes compétents dans des secteurs particuliers ainsi que d'organismes disposant d'une expertise particulière. Lorsqu'elle nomme des experts individuels, la Commission s'efforce de parvenir à un équilibre entre les hommes et les femmes ainsi qu'à un équilibre géographique parmi les membres du groupe d'experts.

CEIDD :
- ACSID
- ACEOAMD
- CEPD/EDPB
- CEPD/EDPS
- ENISA
- ...

2. Le comité européen de l'innovation dans le domaine des données se compose au moins des trois sous-groupes suivants:

a) un sous-groupe composé des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en vue de s'acquitter des missions prévues à l'article 30, points a), c), j) et k);

b) un sous-groupe chargé des discussions techniques sur la normalisation, la portabilité et l'interopérabilité conformément à l'article 30, points f) et g);

c) un sous-groupe chargé de la participation des parties prenantes, composé de représentants pertinents de l'industrie, de la recherche, des milieux universitaires, de la société civile, des organismes de normalisation, des espaces européens communs de données pertinents et d'autres parties prenantes concernées et de tiers qui conseillent le comité européen de l'innovation dans le domaine des données sur les missions prévues à l'article 30, points d), e), f), g) et h).

3. La Commission préside les réunions du comité européen de l'innovation dans le domaine des données.

4. Le comité européen de l'innovation dans le domaine des données est assisté par un secrétariat assuré par la Commission.

Article 30
Missions du comité européen de l'innovation dans le domaine des données

Missions du comité européen de l'innovation dans le domaine des données

Le comité européen de l'innovation dans le domaine des données s'acquitte des missions suivantes:

a) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente des organismes du secteur public et des organismes compétents visés à l'article 7, paragraphe 1, pour la gestion des demandes de réutilisation des catégories de données visées à l'article 3, paragraphe 1;

b) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente pour l'altruisme en matière de données dans l'ensemble de l'Union;

c) conseiller et assister la Commission en ce qui concerne l'élaboration d'une pratique cohérente des autorités compétentes en matière de services d'intermédiation de données et des autorités compétentes pour l'enregistrement des organisations altruistes en matière de données quant à l'application des exigences auxquelles sont soumis les prestataires de services d'intermédiation de données et les organisations altruistes en matière de données reconnues;

d) conseiller et assister la Commission en ce qui concerne l'élaboration de lignes directrices cohérentes sur la meilleure façon de protéger, dans le cadre du présent règlement, les données à caractère non personnel commercialement sensibles, notamment les secrets d'affaires, mais aussi les données à caractère non personnel représentant des contenus protégés par des droits de propriété intellectuelle contre un accès illicite susceptible de conduire à un vol de propriété intellectuelle ou à de l'espionnage industriel;

e) conseiller et assister la Commission en ce qui concerne l'élaboration de lignes directrices cohérentes relatives aux exigences en matière de cybersécurité pour l'échange et le stockage de données;

f) conseiller la Commission, notamment en tenant compte de la contribution des organismes de normalisation, sur la hiérarchisation des normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données transsectoriel entre les espaces européens communs de données émergents, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité et les procédures d'accès, en prenant en considération les activités de normalisation transsectorielle, notamment en précisant et en distinguant les normes et pratiques transsectorielles des normes et pratiques sectorielles;

g) aider la Commission, notamment en tenant compte de la contribution des organismes de normalisation, à lutter contre la fragmentation du marché intérieur et de l'économie des données au sein du marché intérieur en améliorant l'interopérabilité transfrontalière et transsectorielle des données ainsi que les services de partage de données entre les différents secteurs et domaines, en tirant parti des normes européennes, internationales ou nationales existantes dans le but, entre autres, d'encourager la création d'espaces européens communs de données;

h) proposer des lignes directrices pour des espaces européens communs de données, à savoir des cadres interopérables pour les différentes finalités ou pour les différents secteurs ou encore transsectoriels de normes et de pratiques communes visant à partager ou à traiter conjointement des données en vue, entre autres, de la mise au point de nouveaux produits et services, de la recherche scientifique ou d'initiatives de la société civile, ces normes et pratiques communes tenant compte des normes existantes, respectant les règles de concurrence et garantissant un accès non discriminatoire à tous les participants, afin de faciliter le partage des données dans l'Union et de tirer parti du potentiel des espaces de données existants et futurs, notamment en ce qui concerne:

i) les normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données transsectoriel, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité et les procédures d'accès, en tenant compte des activités de normalisation

des différents secteurs, notamment en précisant et en distinguant les normes et pratiques transsectorielles des normes et pratiques sectorielles;

ii) les exigences visant à lutter contre les obstacles à l'entrée sur le marché et à éviter les effets de verrouillage, afin de garantir une concurrence loyale et l'interopérabilité;

iii) une protection adéquate des transferts licites de données vers des pays tiers, y compris des garanties contre tout transfert interdit par le droit de l'Union;

iv) une représentation adéquate et non discriminatoire des parties prenantes concernées dans la gouvernance d'espaces européens communs de données;

v) le respect des exigences de cybersécurité conformément au droit de l'Union;

i) faciliter la coopération entre les États membres en ce qui concerne la définition de conditions harmonisées permettant la réutilisation des catégories de données visées à l'article 3, paragraphe 1, détenues par des organismes du secteur public dans l'ensemble du marché intérieur;

j) faciliter la coopération entre les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes pour l'échange efficace d'informations relatives, d'une part, à la procédure de notification applicable aux prestataires de services d'intermédiation de données et, d'autre part, à l'enregistrement et au contrôle des organisations altruistes en matière de données reconnues, y compris la coordination en ce qui concerne la fixation de redevances ou de sanctions, ainsi que faciliter la coopération entre les autorités compétentes en matière de services d'intermédiation de données et les autorités compétentes pour l'enregistrement des organisations altruistes en matière de données en ce qui concerne l'accès international aux données et le transfert international de données;

k) conseiller et assister la Commission pour ce qui est d'évaluer si les actes d'exécution visés à l'article 5, paragraphes 11 et 12, doivent être adoptés;

l) conseiller et assister la Commission en ce qui concerne l'élaboration du formulaire européen de consentement à l'altruisme en matière de données conformément à l'article 25, paragraphe 1;

m) conseiller la Commission en ce qui concerne l'amélioration du cadre réglementaire international des données à caractère non personnel, y compris la normalisation.

CHAPITRE VII
Accès international et transfert international

Accès international et transfert international

Article 31
Accès international et transfert international

1. L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue prend toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris des arrangements contractuels, afin d'empêcher le transfert international de données à caractère non personnel détenues dans l'Union ou l'accès international des pouvoirs publics à celles-ci lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné, sans préjudice du paragraphe 2 ou 3.

2. Toute décision d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'un organisme du secteur public, d'une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, d'un prestataire de services d'intermédiation de données ou d'une organisation altruiste en matière de données reconnue qu'il ou elle transfère des données à caractère non personnel détenues dans l'Union ou y donne accès dans le

cadre du présent règlement ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou sur tout accord de ce type entre le pays tiers demandeur et un État membre.

Transfert autorisé par un accord international.

3. En l'absence d'accord international tel qu'il est visé au paragraphe 2 du présent article, lorsqu'un organisme du secteur public, une personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, un prestataire de services d'intermédiation de données ou une organisation altruiste en matière de données reconnue est destinataire d'une décision d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers de transférer des données à caractère non personnel détenues dans l'Union ou d'y donner accès dans le cadre du présent règlement, et lorsque le respect d'une telle décision risque de mettre le destinataire en conflit avec le droit de l'Union ou le droit national de l'État membre concerné, le transfert de ces données vers cette autorité d'un pays tiers ou l'accès à ces données par cette même autorité n'a lieu que si:

a) le système du pays tiers exige que les motifs et la proportionnalité de cette décision soient exposés et que cette décision revête un caractère spécifique, par exemple en établissant un lien suffisant avec certaines personnes suspectées, ou avec des infractions;

b) l'objection motivée du destinataire peut faire l'objet d'un réexamen par une juridiction compétente du pays tiers; et

c) la juridiction compétente du pays tiers qui rend la décision ou réexamine la décision d'une autorité administrative est habilitée, en vertu du droit de ce pays tiers, à prendre dûment en compte les intérêts juridiques pertinents du fournisseur des données protégées par le droit de l'Union ou par le droit national de l'État membre concerné.

4. Si les conditions prévues par le paragraphe 2 ou 3 sont réunies, l'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue fournit le volume minimal de données admissible en réponse à une demande, sur la base d'une interprétation raisonnable de la demande.

5. L'organisme du secteur public, la personne physique ou morale à laquelle le droit de réutilisation des données a été accordé en vertu du chapitre II, le prestataire de services d'intermédiation de données et l'organisation altruiste en matière de données reconnue informe le détenteur de données de l'existence d'une demande d'accès à des données le concernant qui émane d'une autorité administrative d'un pays tiers, avant d'y donner suite, sauf lorsque cette demande sert des fins répressives et aussi longtemps que cela est nécessaire pour préserver l'efficacité de l'action répressive.

CHAPITRE VIII
Délégation et comité

Délégation

Article 32
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 5, paragraphe 13, et à l'article 22, paragraphe 1, est conféré à la Commission pour une durée indéterminée à compter du 23 juin 2022.

3. La délégation de pouvoir visée à l'article 5, paragraphe 13, et à l'article 22, paragraphe 1, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 5, paragraphe 13, et de l'article 22, paragraphe 1, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 33
Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) no 182/2011 s'applique.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

CHAPITRE IX
Dispositions finales et transitoires

Article 34
Sanctions

Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations des obligations relatives aux transferts de données à caractère non personnel vers des pays tiers en vertu de l'article 5, paragraphe 14, et de l'article 31, de l'obligation de notification incombant aux prestataires de services d'intermédiation de données en vertu de l'article 11, des conditions liées à la fourniture de services d'intermédiation de données en vertu de l'article 12 et des conditions liées à l'enregistrement en tant qu'organisation altruiste en matière de données reconnue en vertu des articles 18, 20, 21 et 22, et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Dans leur régime de sanctions, les États membres tiennent compte des recommandations du comité européen de l'innovation dans le domaine des données. Les États membres informent la Commission, au plus tard le 24 septembre 2023, du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

2. Les États membres prennent en compte les critères indicatifs et non exhaustifs suivants lorsqu'il s'agit d'imposer des sanctions aux prestataires de services d'intermédiation de données et aux organisations altruistes en matière de données reconnues en cas d'infraction au présent règlement, le cas échéant:

a) la nature, la gravité, l'ampleur et la durée de l'infraction;

b) toute mesure prise par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue pour atténuer ou réparer le préjudice causé par l'infraction;

c) toute infraction antérieure commise par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données reconnue;

d) les avantages financiers obtenus ou les pertes évitées par le prestataire de services d'intermédiation de données ou l'organisation altruiste en matière de données recon-

nue en raison de l'infraction, si ces avantages ou pertes peuvent être établis de manière fiable;

e) toute autre circonstance aggravante ou atténuante applicable au cas concerné.

Article 35
Évaluation et réexamen

Au plus tard le 24 septembre 2025, la Commission procède à une évaluation du présent règlement et présente ses principales conclusions dans un rapport au Parlement européen et au Conseil ainsi qu'au Comité économique et social européen. Ce rapport est au besoin accompagné de propositions législatives.

Ce rapport porte en particulier sur:

a) l'application et le fonctionnement du régime de sanctions établi par les États membres en vertu de l'article 34;

b) le niveau de respect du présent règlement par les représentants légaux des prestataires de services d'intermédiation de données et des organisations altruistes en matière de données reconnues qui ne sont pas établis dans l'Union et le niveau d'applicabilité des sanctions imposées à ces prestataires et organisations;

c) le type d'organisations altruistes en matière de données enregistrées au titre du chapitre IV et un aperçu des objectifs d'intérêt général pour lesquels les données sont partagées en vue d'établir des critères clairs à cet égard.

Les États membres fournissent à la Commission les informations nécessaires à l'établissement de ce rapport.

Article 36
Modification du règlement (UE) 2018/1724

Dans le tableau figurant à l'annexe II du règlement (UE) 2018/1724, la mention «Démarrage et gestion d'une entreprise, et cessation d'activité» est remplacée par le texte suivant:

Événements	Procédures	Résultat escompté, sous réserve d'une évaluation de la demande par l'autorité compétente conformément au droit national, le cas échéant
Démarrage et gestion d'une entreprise, et cessation d'activité	Notification de l'activité économique, autorisation d'exercer une activité économique, modifications de l'activité économique et cessation de l'activité économique sans procédure d'insolvabilité ou de liquidation, à l'exclusion de l'enregistrement initial d'une activité économique au registre du commerce et hors procédures relatives à la constitution de sociétés ou à tout dépôt de pièces ultérieur par des sociétés au sens de l'article 54, deuxième alinéa, du traité sur le fonctionnement de l'Union européenne	Accusé de réception de la notification ou de la modification, ou de la demande d'autorisation de l'activité économique
	Enregistrement d'un employeur (personne physique) auprès d'un régime obligatoire de pension et d'assurance	Confirmation d'enregistrement ou numéro de sécurité sociale
	Enregistrement de salariés auprès de régimes obligatoires de pension et d'assurance	Confirmation d'enregistrement ou numéro de sécurité sociale
	Soumettre une déclaration d'impôt sur les sociétés	Accusé de réception de la déclaration
	Notification de la fin du contrat de travail d'un salarié au régime de sécurité sociale, à l'exclusion des procédures de licenciement collectif	Accusé de réception de la notification
	Paiement des cotisations sociales pour les salariés	Reçu ou autre mode de confirmation du paiement des cotisations sociales pour les salariés
	Notification d'un prestataire de services d'intermédiation de données	Accusé de réception de la notification
	Enregistrement en tant qu'organisation altruiste en matière de données reconnue dans l'Union	Confirmation de l'enregistrement

Aticle 37
Dispositions transitoires

Les entités fournissant les services d'intermédiation de données visés à l'article 10 au 23 juin 2022 se conforment aux obligations énoncées au chapitre III au plus tard le 24 septembre 2025.

Article 38
Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Il est applicable à partir du 24 septembre 2023.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 30 mai 2022.

Par le Parlement européen
La présidente
R. METSOLA

Par le Conseil
Le président
B. LE MAIRE

DA

DA - Data Act

RÈGLEMENT (UE) 2023/2854 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 2023

concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis de la Banque centrale européenne[1],

vu l'avis du Comité économique et social européen[2],

vu l'avis du Comité des régions[3],

statuant conformément à la procédure législative ordinaire[4],

considérant ce qui suit :

(1) Ces dernières années, les technologies fondées sur les données ont eu des effets transformateurs sur tous les secteurs de l'économie. La prolifération des produits connectés à l'internet, en particulier, a fait augmenter le volume de données et leur valeur potentielle pour les consommateurs, les entreprises et la société. Des données de qualité et interopérables provenant de différents domaines permettent d'accroître la compétitivité et l'innovation et de garantir une croissance économique pérenne. Les mêmes données peuvent être utilisées et réutilisées à diverses fins et de façon illimitée, sans perdre en qualité ni en quantité.

(2) Les obstacles au partage de données empêchent que ces données soient réparties de façon optimale dans l'intérêt de la société. Parmi ces obstacles figurent l'absence de mesures incitant les détenteurs de données à conclure volontairement des accords de partage de données, l'incertitude quant aux droits et obligations en matière de données, les coûts afférents à la passation de contrats d'interface technique et à la mise en œuvre des interfaces techniques, l'importante fragmentation des informations stockées en silos de données, une mauvaise gestion des métadonnées, l'absence de normes régissant l'interopérabilité sémantique et technique, les goulets d'étranglement qui entravent l'accès aux données, l'absence de pratiques communes de partage de données et l'exploitation abusive de déséquilibres contractuels en ce qui concerne l'accès aux données et leur utilisation.

1. JO C 402 du 19.10.2022, p. 5.
2. JO C 365 du 23.9.2022, p. 18.
3. JO C 375 du 30.9.2022, p. 112.
4. Position du Parlement européen du 9 novembre 2023 (non encore parue au Journal officiel) et décision du Conseil du 27 novembre 2023.

(3) Dans les secteurs qui comptent de nombreuses microentreprises, petites entreprises et moyennes entreprises telles qu'elles sont définies à l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission[5] (PME), on constate souvent un manque de capacités et de compétences numériques pour collecter, analyser et utiliser des données et l'accès à celles-ci est fréquemment restreint soit parce qu'elles sont détenues par un seul acteur au sein du système, soit en raison de l'absence d'interopérabilité entre les données, entre les services de données ou au-delà des frontières.

(4) Afin de répondre aux besoins de l'économie numérique et d'éliminer les obstacles au bon fonctionnement du marché intérieur des données, il est nécessaire d'établir un cadre harmonisé précisant qui dispose du droit d'utiliser les données relatives au produit ou les données relatives au service connexe, dans quelles conditions et sur quel fondement. Par conséquent, les États membres ne devraient pas adopter ou conserver des exigences nationales supplémentaires en ce qui concerne les questions relevant du champ d'application du présent règlement, sauf disposition expresse de ce dernier, car cela porterait atteinte à son application directe et uniforme. De plus, une action au niveau de l'Union devrait être sans préjudice des obligations et des engagements prévus dans les accords commerciaux internationaux conclus par l'Union.

Objectifs

(5) Il est fait en sorte par le présent règlement que les utilisateurs d'un produit connecté ou d'un service connexe dans l'Union puissent avoir accès, en temps utile, aux données générées par l'utilisation de ce produit connecté ou de ce service connexe et que ces utilisateurs puissent se servir de ces données, y compris en les partageant avec des tiers de leur choix. Le présent règlement impose aux détenteurs de données l'obligation, dans certaines circonstances, de mettre des données à la disposition des utilisateurs et des tiers choisis par un utilisateur. Il prévoit également que les détenteurs de données mettent des données à la disposition des destinataires de données dans l'Union selon des modalités et conditions équitables, raisonnables et non discriminatoires ainsi que de manière transparente. Les règles de droit privé sont essentielles dans le cadre général du partage de données. En conséquence, le présent règlement adapte les règles du droit des contrats et empêche que ne soient exploités des déséquilibres contractuels qui entravent l'équité de l'accès aux données et de l'utilisation des données. Le présent règlement prévoit également qu'en cas de besoin exceptionnel, les détenteurs de données mettent à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union les données nécessaires à l'exécution d'une mission spécifique d'intérêt public. Le présent règlement vise en outre à faciliter le changement de services de traitement de données et à améliorer l'interopérabilité des données ainsi que des mécanismes et services de partage de données dans l'Union. Il convient de ne pas interpréter le présent règlement comme reconnaissant ou conférant aux détenteurs de données un droit nouveau d'utiliser les données générées par l'utilisation d'un produit connecté ou d'un service connexe.

(6) Les données sont générées sous l'effet des actions d'au moins deux acteurs, notamment le concepteur ou fabricant d'un produit connecté, qui peut être dans de nombreux cas également un fournisseur de services connexes, et l'utilisateur du produit connecté ou du service connexe. La génération de données soulève des questions d'équité dans l'économie numérique étant donné que les données enregistrées par les produits connectés ou les services connexes constituent un apport important pour les services après-vente, les services auxiliaires et autres. Pour concrétiser les avantages économiques importants que recèlent les données, y compris par le partage de données sur la base d'accords volontaires et le développement de la création de valeur fondée sur les données par les entreprises de l'Union, une approche générale de l'attribution de droits relatifs à l'accès aux données et à l'utilisation de données est préférable à l'octroi de droits exclusifs d'accès et d'utilisation. Le présent règlement prévoit des règles horizontales qui pourraient être suivies par des dispositions du droit de l'Union ou du droit national qui règlent les situations spécifiques des secteurs concernés.

(7) Le droit fondamental à la protection des données à caractère personnel est garanti notamment par les règlements (UE) 2016/679[6] et (UE) 2018/1725[7] du Parlement euro-

Articulation avec le RGPD

cf. RGPD

5. Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).
6. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

péen et du Conseil. En outre, la directive 2002/58/CE du Parlement européen et du Conseil[8] protège la vie privée et la confidentialité des communications, notamment en prévoyant des conditions régissant tout stockage de données à caractère personnel et à caractère non personnel dans un équipement terminal et tout accès à ces données à partir dudit équipement. Ces actes législatifs de l'Union servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel. Le présent règlement complète, sans y porter atteinte, les dispositions du droit de l'Union relatives à la protection des données à caractère personnel et à la vie privée, en particulier les règlements (UE) 2016/679 et (UE) 2018/1725, et la directive 2002/58/CE. Aucune disposition du présent règlement ne devrait être appliquée ou interprétée de manière à réduire ou à limiter le droit à la protection des données à caractère personnel ou le droit à la vie privée et à la confidentialité des communications. Tout traitement de données à caractère personnel effectué au titre du présent règlement devrait respecter le droit de l'Union en matière de protection des données, y compris l'exigence d'une base juridique valable pour un traitement relevant de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, les conditions de l'article 9 dudit règlement et de l'article 5, paragraphe 3, de la directive 2002/58/CE. Le présent règlement ne constitue pas une base juridique pour la collecte ou la génération de données à caractère personnel par le détenteur de données. Le présent règlement impose aux détenteurs de données l'obligation de mettre des données personnelles à la disposition des utilisateurs ou de tiers choisis par un utilisateur à la demande dudit utilisateur. Un tel accès devrait être donné aux données à caractère personnel qui sont traitées par le détenteur de données sur le fondement de l'une des bases juridiques mentionnées à l'article 6 du règlement (UE) 2016/679. Lorsque l'utilisateur n'est pas la personne concernée, le présent règlement ne crée pas de base juridique permettant de donner l'accès à des données à caractère personnel ou de mettre des données à caractère personnel à la disposition d'un tiers et il ne devrait pas être interprété comme conférant au détenteur de données un droit nouveau d'utiliser les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe. En pareils cas, il pourrait être dans l'intérêt de l'utilisateur de faciliter le respect des exigences de l'article 6 du règlement (UE) 2016/679. Étant donné que le présent règlement ne devrait pas porter atteinte aux droits des personnes concernées en matière de protection des données, le détenteur de données peut donner suite aux demandes en pareils cas, entre autres, en anonymisant les données à caractère personnel ou, lorsque les données facilement accessibles contiennent les données à caractère personnel de plusieurs personnes concernées, en ne transmettant que des données à caractère personnel relatives à l'utilisateur.

cf. Directive e-Privacy

cf. RGPD

cf. Directive e-Privacy

cf. RGPD

cf. RGPD

(8) Les principes de la minimisation des données ainsi que de la protection des données dès la conception et de la protection des données par défaut sont essentiels lorsque le traitement comporte des risques importants pour les droits fondamentaux des personnes. Compte tenu de l'état des connaissances, toutes les parties au partage de données, y compris le partage de données relevant du champ d'application du présent règlement, devraient mettre en œuvre des mesures techniques et organisationnelles pour protéger ces droits. Des mesures de ce type incluent non seulement la pseudonymisation et le chiffrement, mais aussi le recours à des technologies de plus en plus disponibles qui permettent d'appliquer des algorithmes aux données et d'obtenir des informations précieuses sans transmission entre les parties ni copie inutile des données brutes ou des données structurées elles-mêmes.

Articulation avec le droit des contrats

(9) Sauf disposition contraire de celui-ci, le présent règlement n'affecte pas le droit national des contrats, y compris les règles relatives à la formation, à la validité ou aux effets des contrats, ni les conséquences de la résiliation d'un contrat. Le présent règlement complète, sans y porter atteinte, le droit de l'Union qui vise à promouvoir les intérêts des consommateurs et à assurer un niveau élevé de protection des consommateurs, ainsi qu'à protéger leur santé, leur sécurité et leurs intérêts économiques, en par-

7. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).
8. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

ticulier la directive 93/13/CEE du Conseil[9] et les directives 2005/29/CE[10] et 2011/83/UE[11] du Parlement européen et du Conseil.

(10) Le présent règlement est sans préjudice des actes juridiques de l'Union et des actes juridiques nationaux qui prévoient le partage de données, l'accès aux données et l'utilisation de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, ou à des fins douanières et fiscales, quelle que soit la base juridique prévue par le traité sur le fonctionnement de l'Union européenne sur laquelle ces actes juridiques de l'Union ont été adoptés, et sans préjudice de la coopération internationale dans ce domaine fondée, en particulier, sur la convention du Conseil de l'Europe sur la cybercriminalité, (STE n° 185), signée à Budapest le 23 novembre 2001. Il s'agit notamment des règlements (UE) 2021/784[12], (UE) 2022/2065[13] et (UE) 2023/1543[14] du Parlement européen et du Conseil et de la directive (UE) 2023/1544 du Parlement européen et du Conseil[15]. Le présent règlement ne s'applique pas à la collecte ou au partage de données, à l'accès aux données ou à l'utilisation de données au titre du règlement (UE) 2015/847 du Parlement européen et du Conseil[16] et de la directive (UE) 2015/849 du Parlement européen et du Conseil[17]. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en ce qui concerne la sécurité publique, la défense ou la sécurité nationale, les douanes et l'administration fiscale ou la santé et la sécurité des citoyens, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétences.

cf. DSA

(11) Sauf disposition expresse spécifique de celui-ci, le présent règlement ne devrait pas avoir d'incidence sur les dispositions du droit de l'Union qui fixent des exigences en matière de conception physique et de données que les produits doivent remplir pour pouvoir être mis sur le marché de l'Union.

(12) Le présent règlement complète, sans y porter atteinte, les dispositions du droit de l'Union qui visent à établir des exigences en matière d'accessibilité applicables à certains produits et services, en particulier la directive (UE) 2019/882 du Parlement européen et du Conseil[18].

(13) Le présent règlement n'a pas d'incidence sur les actes juridiques de l'Union et nationaux prévoyant la protection des droits de propriété intellectuelle, notamment les directives 2001/29/CE[19], 2004/48/CE[20] et (UE) 2019/790[21] du Parlement européen et du Conseil.

9. Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs (JO L 95 du 21.4.1993, p. 29).
10. Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil ("directive sur les pratiques commerciales déloyales") (JO L 149 du 11.6.2005, p. 22).
11. Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil (JO L 304 du 22.11.2011, p. 64).
12. Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (JO L 172 du 17.5.2021, p. 79).
13. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).
14. Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves électroniques, dans les procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).
15. Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de la collecte de preuves électroniques en matière pénale (JO L 191 du 28.7.2023, p. 181).
16. Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 (JO L 141 du 5.6.2015, p. 1).

(14) Les produits connectés qui, au moyen de leurs composants ou systèmes d'exploitation, obtiennent, génèrent ou collectent des données concernant leur performance, leur utilisation ou leur environnement et qui sont en mesure de communiquer ces données par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un accès sur un appareil, souvent appelés "l'internet des objets", devraient relever du champ d'application du présent règlement, à l'exception des prototypes. Parmi les exemples de tels services de communications électroniques, on peut citer notamment les réseaux téléphoniques terrestres, les réseaux câblés de télévision, les réseaux par satellite et les réseaux de communication en champ proche. Les produits connectés sont présents dans tous les domaines de l'économie et de la société, notamment dans les infrastructures privées, civiles ou commerciales, les véhicules, les équipements de santé et de bien-être, les navires, les avions, les équipements domestiques et les biens de consommation, les dispositifs médicaux et sanitaires, ou encore les machines agricoles et industrielles. Les choix de conception des fabricants et, le cas échéant, les dispositions du droit de l'Union ou du droit national qui répondent aux besoins et aux objectifs propres à un secteur ou les décisions pertinentes des autorités compétentes devraient déterminer les données qu'un produit connecté peut mettre à disposition.

Typologie des données

(15) Les données représentent la numérisation des actions de l'utilisateur et des événements et devraient, dès lors, être accessibles à l'utilisateur. Les règles relatives à l'accès aux données provenant de produits connectés et de services connexes et à l'utilisation de ces données au titre du présent règlement concernent à la fois les données relatives au produit et les données relatives au service connexe. Les données relatives au produit désignent les données générées par l'utilisation d'un produit connecté que le fabricant a conçues pour pouvoir être extraites du produit connecté par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant. Les données relatives au service connexe désignent les données représentant également la numérisation des actions de l'utilisateur ou des événements liés au produit connecté qui sont générées lors de la fourniture d'un service connexe par le fournisseur. Les données générées par l'utilisation d'un produit connecté ou d'un service connexe devraient s'entendre comme comprenant les données enregistrées intentionnellement ou les données qui résultent indirectement de l'action de l'utilisateur, telles que les données relatives à l'environnement ou aux interactions du produit connecté. Cela devrait inclure les données sur l'utilisation d'un produit connecté générées par une interface utilisateur ou par l'intermédiaire d'un service connexe, et ne devraient pas se limiter à l'information indiquant qu'une telle utilisation a eu lieu, mais devraient inclure toutes les données générées par le produit connecté à la suite de cette utilisation, telles que les données générées automatiquement par des capteurs et les données enregistrées par des applications intégrées, y compris les applications indiquant l'état du matériel et les dysfonctionnements. Cela devrait également inclure les données générées par le produit connecté ou le service connexe en période d'inaction de l'utilisateur, par exemple lorsque l'utilisateur choisit de ne pas utiliser un produit connecté pendant une période donnée et de le maintenir en mode veille, voire éteint, étant donné que le statut d'un produit connecté ou de ses composants, par exemple ses batteries, peut varier lorsque le produit connecté est en mode veille ou éteint. Relèvent du champ d'application du présent règlement les données qui ne sont pas substantiellement modifiées, c'est-à-dire les données sous forme brute, également appelées "données sources" ou "données primaires", désignant des points de données qui sont générés automatiquement sans autre forme de traitement, ainsi que les données qui ont été prétraitées dans le but de les rendre compréhensibles et utilisables avant leur traitement et leur analyse ultérieurs.

17. Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (JO L 141 du 5.6.2015, p. 73).
18. Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).
19. Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO L 167 du 22.6.2001, p. 10).
20. Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle (JO L 157 du 30.4.2004, p. 45).
21. Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

Ces données comprennent les données collectées à partir d'un capteur unique ou d'un groupe de capteurs connecté dans le but de rendre les données collectées compréhensibles pour les cas d'utilisation plus larges en déterminant une grandeur ou une qualité physique ou la modification d'une grandeur physique, telle que la température, la pression, le débit, l'audio, la valeur de pH, le niveau de liquide, la position, l'accélération ou la vitesse. L'expression "données prétraitées" ne devrait pas être interprétée de manière à imposer au détenteur de données l'obligation de réaliser des investissements substantiels dans le nettoyage et la transformation des données. Les données qui doivent être mises à disposition devraient inclure les métadonnées pertinentes, y compris leur contexte de base et leur horodatage, pour rendre les données utilisables, combinées à d'autres données, telles que les données triées et classifiées avec d'autres points de données les concernant, ou reformatées dans un format couramment utilisé. De telles données sont potentiellement précieuses pour l'utilisateur et favorisent l'innovation et le développement de services numériques et d'autres services en faveur de la protection de l'environnement, de la santé et de l'économie circulaire, notamment en facilitant l'entretien et la réparation des produits connectés en question. À l'inverse, les informations dérivées ou déduites de ces données, qui sont le résultat d'investissements supplémentaires dans l'attribution de valeurs ou d'informations tirées des données, en particulier au moyen d'algorithmes complexes et propriétaires, y compris ceux qui font partie d'un logiciel propriétaire, ne devraient pas être considérées comme relevant du champ d'application du présent règlement et ne devraient donc pas être soumises à l'obligation pour un détenteur de données de les mettre à la disposition d'un utilisateur ou d'un destinataire de données, sauf accord contraire entre l'utilisateur et le détenteur de données. Ces données pourraient comprendre en particulier les informations obtenues au moyen de la fusion de capteurs, qui infère ou déduit des données provenant de capteurs multiples, collectées dans le produit connecté, au moyen d'algorithmes complexes et propriétaires, et qui pourraient être soumises à des droits de propriété intellectuelle.

(16) Le présent règlement permet aux utilisateurs de produits connectés de bénéficier de services après-vente, auxiliaires et autres sur la base de données collectées par des capteurs intégrés dans ces produits, la collecte de ces données étant potentiellement utile pour améliorer la performance des produits connectés. Il importe de délimiter, d'une part, les marchés de fourniture de ces produits connectés équipés de capteurs et de fourniture de services connexes et, d'autre part, les marchés de logiciels et de contenus non connexes, tels que les contenus textuels, audio ou audiovisuels, souvent couverts par des droits de propriété intellectuelle. Dès lors, les données que ces produits connectés équipés de capteurs génèrent lorsque l'utilisateur enregistre, transmet, affiche ou lit du contenu, ainsi que le contenu lui-même, qui est souvent couvert par des droits de propriété intellectuelle, entre autres pour une utilisation par un service en ligne, ne devraient pas être couvertes par le présent règlement. Le présent règlement ne devrait pas non plus couvrir les données qui ont été obtenues, générées ou auxquelles il est accédé à partir du produit connecté, ou qui lui ont été transmises, à des fins de stockage ou d'autres opérations de traitement pour le compte d'autres parties, qui ne sont pas l'utilisateur, comme cela peut être le cas pour des serveurs ou des infrastructures en nuage exploités par leurs propriétaires entièrement pour le compte de tiers, entre autres en vue de leur utilisation par un service en ligne.

Service connexe

(17) Il est nécessaire de fixer des règles concernant les produits qui sont connectés à un service connexe au moment de l'achat, de la location ou de la conclusion du crédit-bail d'une manière telle que l'absence de ce service empêcherait le produit connecté de remplir une ou plusieurs de ses fonctions, ou un service connexe qui est ensuite connecté au produit par le fabricant ou un tiers afin de compléter ou d'adapter la fonctionnalité du produit connecté. Ces services connexes impliquent l'échange de données entre le produit connecté et le fournisseur de services et devraient être compris comme étant explicitement liés à l'utilisation des fonctions du produit connecté, tels que des services qui, le cas échéant, transmettent au produit connecté des commandes qui peuvent avoir une incidence sur son action ou son comportement. Les services qui n'ont pas d'incidence sur le fonctionnement du produit connecté et qui n'impliquent pas la transmission de données ou de commandes au produit connecté par le fournisseur de services ne devraient pas être considérés comme des services connexes. De tels services pourraient inclure, par exemple, des services auxiliaires de conseil, d'analyse ou des services financiers, ou des services réguliers de réparation et d'entretien. Les services connexes peuvent être proposés dans le cadre du contrat d'achat, de location ou de crédit-bail. Des services connexes pourraient aussi être fournis pour des produits du même type et les utilisateurs pourraient raisonnablement s'attendre à ce

qu'ils soient fournis en tenant compte de la nature du produit connecté et de toute déclaration publique faite par le vendeur, le loueur, le bailleur ou d'autres personnes situées en amont de la chaîne de transactions, y compris le fabricant, ou pour leur compte. Ces services connexes peuvent eux-mêmes générer des données de valeur pour l'utilisateur indépendamment des capacités de collecte de données du produit connecté avec lequel ils sont interconnectés. Le présent règlement devrait également s'appliquer à un service connexe qui n'est pas fourni par le vendeur, le loueur ou le bailleur lui-même, mais qui est fourni par un tiers. En cas de doute sur la question de savoir si le service est ou non fourni dans le cadre du contrat d'achat, de location ou de crédit-bail, le présent règlement devrait s'appliquer. Ni la fourniture d'énergie ni la fourniture de connectivité ne doivent être interprétées comme étant des services connexes au titre du présent règlement.

Notion d'utilisateur

(18) Il convient d'entendre par utilisateur d'un produit connecté une personne physique ou morale, telle qu'une entreprise, un consommateur ou un organisme du secteur public, qui est le propriétaire d'un produit connecté, a reçu certains droits temporaires, par exemple en vertu d'un contrat de location ou de crédit-bail, d'accéder aux données obtenues à partir du produit connecté ou de les utiliser, ou reçoit des services connexes pour le produit connecté. Ces droits d'accès ne devraient en aucun cas modifier les droits des personnes concernées qui peuvent interagir avec un produit connecté ou un service connexe en ce qui concerne les données à caractère personnel générées par le produit connecté ou pendant la fourniture du service connexe, ni interférer avec ces droits. L'utilisateur supporte les risques et bénéficie des avantages que présente l'utilisation du produit connecté et devrait également bénéficier de l'accès aux données que ce produit génère. L'utilisateur devrait par conséquent avoir le droit de tirer parti des données générées par ce produit connecté et par tout service connexe. Les propriétaires, les loueurs ou les bailleurs devraient également être considérés comme des utilisateurs, y compris lorsque plusieurs entités peuvent être considérées comme des utilisateurs. Dans le cas d'utilisateurs multiples, chaque utilisateur peut contribuer de manière différente à la production de données et avoir un intérêt dans plusieurs formes d'utilisation, telles que la gestion de flotte pour une entreprise de crédit-bail ou des solutions de mobilité pour les particuliers utilisant un service de partage de véhicule.

Éducation aux données

(19) L'éducation aux données renvoie aux compétences, aux connaissances et à la compréhension permettant aux utilisateurs, consommateurs et entreprises, en particulier les PME relevant du champ d'application du présent règlement, d'être sensibilisés à la valeur potentielle des données qu'ils génèrent, produisent et partagent et qu'ils sont disposés à offrir et auxquelles ils sont prêts à donner accès, conformément aux règles juridiques applicables. L'éducation aux données devrait aller au-delà de l'apprentissage des outils et technologies et avoir pour objectif de donner aux citoyens et entreprises la capacité et le pouvoir de bénéficier d'un marché des données inclusif et équitable. L'application de mesures en matière d'éducation aux données et l'introduction d'actions de suivi appropriées pourraient contribuer à améliorer les conditions de travail et, en fin de compte, soutenir la consolidation de l'économie des données dans l'Union et son potentiel en matière d'innovation. Les autorités compétentes devraient promouvoir des outils et adopter des mesures visant à faire progresser l'éducation aux données parmi les utilisateurs et les entités relevant du champ d'application du présent règlement, ainsi qu'à les sensibiliser à leurs droits et obligations au titre de celui-ci.

Données facilement accessibles

(20) En pratique, les données générées par des produits connectés ou des services connexes ne sont pas toutes facilement accessibles à leurs utilisateurs et les possibilités en ce qui concerne la portabilité des données générées par les produits connectés à l'internet sont souvent limitées. Les utilisateurs ne sont pas en mesure d'obtenir les données nécessaires pour recourir à des fournisseurs de services de réparation et d'autres services, tandis que les entreprises sont dans l'impossibilité de lancer des services innovants, pratiques et plus efficaces. Dans de nombreux secteurs, les fabricants peuvent déterminer, par le contrôle qu'ils exercent sur la conception technique des produits connectés ou des services connexes, les données qui sont générées et les modalités d'accès à ces données, même s'ils n'ont légalement aucun droit sur ces données. Il est par conséquent nécessaire de veiller à ce que les produits connectés soient conçus et fabriqués, et à ce que les services connexes soient conçus et fournis, de telle manière que l'utilisateur dispose toujours d'un accès facile et sécurisé aux données relatives au produit et aux données relatives au service connexe, y compris aux métadonnées correspondantes nécessaires pour interpréter et utiliser ces données, notamment aux fins d'extraction, d'utilisation ou de partage des données, et ce gratuitement, dans un format complet, structuré, couramment utilisé et lisible par machine. On entend par "données

facilement accessibles" les données relatives au produit et au service connexe qu'un détenteur de données obtient ou peut obtenir légalement du produit connecté ou du service connexe, par exemple au moyen de la conception du produit connecté, du contrat passé entre le détenteur de données et l'utilisateur pour la fourniture de services connexes et des moyens techniques d'accès aux données dont le détenteur de données dispose, sans effort disproportionné. Les données facilement accessibles ne comprennent pas les données générées par l'utilisation d'un produit connecté lorsque la conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble. Le présent règlement ne devrait donc pas s'entendre comme imposant une obligation de stocker des données dans l'unité informatique centrale d'un produit connecté. L'absence d'une telle obligation ne devrait pas empêcher le fabricant ou le détenteur de données de convenir volontairement avec l'utilisateur de procéder à de telles adaptations. Les obligations en matière de conception prévues par le présent règlement sont également sans préjudice du principe de minimisation des données énoncé à l'article 5, paragraphe 1, point c), du règlement (UE) 2016/679 et ne devraient pas être interprétées comme imposant une obligation de concevoir des produits connectés et des services connexes de telle manière qu'ils stockent ou traitent d'une autre manière des données à caractère personnel autres que les données à caractère personnel nécessaires en ce qui concerne les finalités pour lesquelles elles sont traitées. Des dispositions du droit de l'Union ou du droit national pourraient être introduites pour définir d'autres spécificités, telles que les données relatives aux produits qui devraient être accessibles à partir de produits connectés ou de services connexes, étant donné que ces données peuvent être essentielles au fonctionnement, à la réparation ou à l'entretien efficaces de ces produits connectés ou services connexes. Lorsque des mises à jour ou des modifications ultérieures d'un produit connecté ou d'un service connexe, par le fabricant ou une autre partie, aboutissent à une augmentation des données accessibles ou à une limitation des données initialement accessibles, ces modifications devraient être communiquées à l'utilisateur dans le cadre de la mise à jour ou de la modification.

cf. RGPD

Utilisateurs multiples

(21) Lorsque plusieurs personnes ou entités sont considérées comme étant des utilisateurs, par exemple en cas de copropriété ou lorsqu'un propriétaire, un loueur ou un bailleur partage des droits d'accès aux données ou d'utilisation de données, la conception du produit connecté ou du service connexe, ou l'interface pertinente, devrait permettre à chaque utilisateur d'avoir accès aux données qu'ils génèrent. L'utilisation de produits connectés qui génèrent des données nécessite généralement la création d'un compte d'utilisateur. Un tel compte permet l'identification de l'utilisateur par le détenteur de données, qui peut être le fabricant. Il peut également être utilisé comme moyen de communication et pour introduire et traiter des demandes d'accès aux données. Lorsque plusieurs fabricants ou fournisseurs de services connexes ont vendu ou loué des produits connectés à un même utilisateur ou conclu un crédit-bail ayant pour objet de tels produits avec un même utilisateur, ou fourni des services connexes à un même utilisateur, ces produits et services étant intégrés ensemble, l'utilisateur devrait s'adresser à chacune des parties avec lesquelles il a conclu un contrat. Les fabricants ou concepteurs d'un produit connecté qui est généralement utilisé par plusieurs personnes devraient mettre en place les mécanismes nécessaires permettant la coexistence de comptes d'utilisateur distincts pour différentes personnes, le cas échéant, ou permettant à plusieurs personnes d'utiliser le même compte d'utilisateur. Les solutions de compte devraient permettre aux utilisateurs de supprimer leurs comptes et d'effacer les données qui s'y rapportent et pourraient permettre aux utilisateurs de mettre fin à l'accès aux données, à l'utilisation ou au partage de données, ou de présenter des demandes de résiliation, compte tenu notamment des situations dans lesquelles la propriété ou l'utilisation du produit connecté change. L'accès devrait être accordé à l'utilisateur sur la base d'un mécanisme de simple demande permettant l'exécution automatique, sans que le fabricant ou le détenteur de données ne soit tenu d'examiner ou d'approuver la demande. Cela signifie que les données ne devraient être mises à disposition que lorsque l'utilisateur souhaite effectivement y avoir accès. Lorsqu'il n'est pas possible de procéder à l'exécution automatique de la demande concernant l'accès aux données, par exemple au moyen d'un compte d'utilisateur ou d'une application mobile correspondante fournie avec le produit connecté ou le service connexe, le fabricant devrait informer l'utilisateur des modalités d'accès aux données.

(22) Les produits connectés peuvent être conçus de façon que certaines données soient directement accessibles à partir d'un dispositif de stockage de données intégré à l'appareil ou d'un serveur distant auquel les données sont communiquées. L'accès à ce dispo-

sitif de stockage de données intégré à l'appareil peut être rendu possible par l'intermédiaire de réseaux locaux câblés ou sans fil connectés soit à un service de communications électroniques accessible au public, soit à un réseau mobile. Pour ce qui est du serveur, il peut s'agir de la propre capacité du serveur local du fabricant ou de celle d'un tiers ou d'un fournisseur de services d'informatique en nuage. Les sous-traitants tels qu'ils sont définis à l'article 4, point 8), du règlement (UE) 2016/679 ne sont pas considérés comme agissant en qualité de détenteurs de données. Toutefois, ils peuvent être spécifiquement chargés, par le responsable du traitement tel qu'il est défini à l'article 4, point 7), du règlement (UE) 2016/679, de mettre les données à disposition. Les produits connectés peuvent être conçus pour permettre à l'utilisateur ou à un tiers de traiter les données dans le produit connecté, sur une instance informatique du fabricant ou dans un environnement des technologies de l'information et de la communication (TIC) choisi par l'utilisateur ou le tiers.

cf. RGPD

Assistants virtuels

(23) Les assistants virtuels jouent un rôle croissant dans la dématérialisation de l'environnement des consommateurs et des professionnels, et servent d'interface facile à utiliser pour lire des contenus, obtenir des informations ou activer des produits connectés à l'internet. Ils peuvent servir de portail unique dans un environnement domestique intelligent, par exemple, et enregistrer des quantités importantes de données utiles sur la manière dont les utilisateurs interagissent avec les produits connectés à l'internet, dont ceux fabriqués par d'autres parties, et ils peuvent remplacer l'utilisation d'interfaces fournies par le fabricant telles que des écrans tactiles ou des applications pour smartphones. L'utilisateur pourrait souhaiter mettre ces données à la disposition de fabricants tiers et ainsi permettre l'avènement de nouveaux services intelligents. Les assistants virtuels devraient être couverts par les droits d'accès aux données prévus par le présent règlement. Les données générées lorsqu'un utilisateur interagit avec un produit connecté par l'intermédiaire d'un assistant virtuel fourni par une entité autre que le fabricant du produit connecté devraient également être couvertes par les droits d'accès aux données prévus par le présent règlement. Toutefois, seules les données résultant de l'interaction entre l'utilisateur et un produit connecté ou un service connexe par l'intermédiaire de l'assistant virtuel devraient être couvertes par le présent règlement. Les données produites par l'assistant virtuel qui sont sans rapport avec l'utilisation d'un produit connecté ou d'un service connexe ne sont pas couvertes par le présent règlement.

Information de l’utilisateur

(24) Avant la conclusion d'un contrat d'achat, de location ou de crédit-bail relatif à un produit connecté, le vendeur, le loueur ou le bailleur, qui peut être le fabricant, devrait fournir à l'utilisateur des informations concernant les données relatives au produit qui peuvent être générées par le produit connecté, y compris le type, le format et le volume estimé de ces données, de manière claire et compréhensible. Cela devrait inclure des informations sur les structures de données, les formats de données, les vocabulaires, les systèmes de classification, les taxinomies et les listes de codes, le cas échéant, ainsi que des informations claires et suffisantes utiles pour l'exercice des droits de l'utilisateur sur les modalités de stockage, d'extraction ou d'accès aux données, y compris les conditions d'utilisation et la qualité du service des interfaces de programmation d'applications ou, le cas échéant, la fourniture de kits de développement logiciel. Cette obligation permet de garantir la transparence quant aux données relatives au produit générées et accroît la facilité d'accès pour l'utilisateur. L'obligation d'information pourrait être satisfaite, par exemple, en utilisant un localisateur uniforme de ressources (adresse URL) stable sur l'internet, qui peut être diffusé sous forme de lien internet ou de code QR redirigeant vers les informations pertinentes, que le vendeur, le loueur ou le bailleur, qui peut être le fabricant, peut fournir à l'utilisateur avant la conclusion du contrat d'achat, de location ou de crédit-bail relatif à un produit connecté. Il est en tout cas nécessaire que l'utilisateur ait la possibilité de stocker les informations de manière à pouvoir les retrouver ultérieurement et les reproduire à l'identique. On ne peut attendre du détenteur de données qu'il stocke indéfiniment les données en vue de répondre aux besoins de l'utilisateur du produit connecté, mais il devrait mettre en œuvre une politique raisonnable de conservation des données, le cas échéant, en conformité avec le principe de limitation de la conservation prévu à l'article 5, paragraphe 1, point e), du règlement (UE) 2016/679, qui permet l'application effective des droits d'accès aux données prévus par le présent règlement. L'obligation de fournir des informations ne porte pas atteinte à l'obligation incombant au responsable du traitement de fournir des informations à la personne concernée en application des articles 12, 13 et 14 du règlement (UE) 2016/679. L'obligation de fournir des informations avant de conclure un contrat de fourniture d'un service connexe devrait incomber au détenteur de données potentiel, que celui-ci conclue ou non un contrat d'achat, de loca-

cf. RGPD

tion ou de crédit-bail relatif à un produit connecté. Lorsque des informations changent au cours de la durée de vie du produit connecté ou de la période contractuelle pour le service connexe, y compris lorsque la finalité pour laquelle ces données doivent être utilisées change par rapport à la finalité initialement spécifiée, elles devraient également être fournies à l'utilisateur.

(25) Le présent règlement ne devrait pas être interprété comme conférant aux détenteurs de données un droit nouveau d'utiliser les données relatives à un produit ou un service connexe. Lorsque le fabricant d'un produit connecté est un détenteur de données, l'utilisation de données à caractère non personnel par le fabricant devrait être fondée sur un contrat entre le fabricant et l'utilisateur. Un tel contrat pourrait faire partie d'un accord pour la fourniture du service connexe, qui pourrait être fourni en même temps que le contrat d'achat, de location ou de crédit-bail relatif au produit connecté. Toute clause contractuelle stipulant que le détenteur de données peut utiliser les données relatives à un produit ou à un service connexe devrait être transparente pour l'utilisateur, y compris en ce qui concerne les finalités pour lesquelles le détenteur de données a l'intention d'utiliser ces données. Ces finalités pourraient inclure l'amélioration du fonctionnement du produit connecté ou des services connexes, le développement de nouveaux produits ou services, ou l'agrégation de données dans le but de mettre les données déduites qui en résultent à la disposition de tiers, pour autant que ces données déduites ne permettent pas d'identifier des données spécifiques transmises au détenteur de données à partir du produit connecté, ou ne permettent pas à un tiers de déduire ces données de l'ensemble de données. Toute modification du contrat devrait dépendre de l'accord éclairé de l'utilisateur. Le présent règlement n'empêche pas les parties de s'accorder sur des clauses contractuelles ayant pour effet d'exclure ou de limiter l'utilisation de données à caractère non personnel, ou de certaines catégories d'entre elles, par le détenteur de données. Il n'empêche pas non plus les parties de convenir de mettre des données relatives au produit ou des données relatives au service connexe à la disposition de tiers, que ce soit directement ou indirectement, y compris, le cas échéant, par l'intermédiaire d'un autre détenteur de données. De plus, le présent règlement ne fait pas non plus obstacle aux exigences réglementaires sectorielles prévues par le droit de l'Union, ou par le droit national compatible avec le droit de l'Union, qui excluraient ou limiteraient l'utilisation de certaines de ces données par le détenteur de données pour des motifs d'ordre public bien définis. Le présent règlement n'empêche pas les utilisateurs, dans le cas de relations entre entreprises, de mettre des données à la disposition de tiers ou de détenteurs de données en vertu de toute disposition contractuelle légale, y compris en acceptant de limiter ou de restreindre le partage ultérieur de ces données, ou d'être indemnisés proportionnellement, par exemple en échange d'une renonciation à leur droit d'utiliser ou de partager ces données. Bien que la notion de "détenteur de données" n'inclue généralement pas les organismes du secteur public, elle peut inclure les entreprises publiques.

Partage de données

(26) Pour favoriser l'émergence de marchés liquides, équitables et efficaces pour les données à caractère non personnel, les utilisateurs de produits connectés devraient avoir la possibilité de partager des données avec d'autres personnes, notamment à des fins commerciales, sans grands efforts juridiques et techniques. À l'heure actuelle, il est souvent difficile pour les entreprises de justifier les frais de personnel ou informatiques qui sont nécessaires pour préparer des ensembles de données à caractère non personnel ou des produits de données et les proposer à des cocontractants potentiels par le biais de services d'intermédiation de données, y compris des places de marché de données. Un obstacle majeur au partage de données à caractère non personnel par les entreprises résulte donc du manque de prévisibilité en ce qui concerne la rentabilité économique des investissements dans la conservation et la mise à disposition d'ensembles de données ou de produits de données. Pour permettre l'émergence de marchés liquides, équitables et efficaces pour les données à caractère non personnel dans l'Union, la partie qui a le droit de proposer ces données sur un marché doit être précisée. Les utilisateurs devraient par conséquent avoir le droit de partager des données à caractère non personnel avec des destinataires de données à des fins commerciales et non commerciales. Un tel partage de données pourrait être assuré directement par l'utilisateur, à la demande de l'utilisateur par l'intermédiaire d'un détenteur de données, ou par le biais de services d'intermédiation de données. Les services d'intermédiation de données, tels qu'ils sont réglementés par le règlement (UE) 2022/868 du Parlement européen et du Conseil[22], pourraient favoriser une économie fondée sur les données en établissant des relations commerciales entre les utilisateurs, les destinataires de données et les tiers, et peuvent aider les utilisateurs à exercer leur droit d'uti-

cf. DGA

liser les données, par exemple en garantissant l'anonymisation des données à caractère personnel ou l'agrégation de l'accès aux données de plusieurs utilisateurs individuels. Lorsque l'obligation, pour un détenteur de données, de mettre celles-ci à la disposition d'utilisateurs ou de tiers ne s'applique pas à certaines données, l'éventail des données en question pourrait être défini dans le contrat conclu entre l'utilisateur et le détenteur de données pour la fourniture d'un service connexe de telle manière que les utilisateurs puissent facilement déterminer les données qui leur sont accessibles en vue d'être partagées avec des destinataires de données ou des tiers. Les détenteurs de données ne devraient pas mettre à la disposition de tiers des données à caractère non personnel relatives aux produits à des fins commerciales ou non commerciales autres que l'exécution de leur contrat avec l'utilisateur, sans préjudice des exigences légales en vertu du droit de l'Union ou du droit national imposant à un détenteur de données de mettre des données à disposition. Le cas échéant, les détenteurs de données devraient obliger contractuellement les tiers à ne pas partager les données reçues de leur part.

(27) Dans les secteurs caractérisés par la concentration d'un petit nombre de fabricants qui fournissent des produits connectés aux utilisateurs finaux, les utilisateurs peuvent ne disposer que d'options limitées en matière d'accès aux données et d'utilisation et de partage des données. En pareilles circonstances, il se peut que les contrats ne suffisent pas pour atteindre l'objectif de responsabilisation de l'utilisateur, de sorte qu'il est difficile pour les utilisateurs d'obtenir de la valeur à partir des données générées par le produit connecté qu'ils achètent, qu'ils louent ou qu'ils détiennent en crédit-bail. En conséquence, la possibilité pour les petites entreprises innovantes de proposer des solutions fondées sur les données de manière compétitive et en faveur d'une économie des données diversifiée dans l'Union est limitée. Le présent règlement devrait par conséquent s'appuyer sur les évolutions récentes survenues dans certains secteurs, telles que le code de conduite pour le partage des données agricoles par contrat. Des dispositions du droit de l'Union ou du droit national peuvent être adoptées pour répondre à des besoins et objectifs sectoriels. De surcroît, les détenteurs de données ne pas devraient pas utiliser de données facilement accessibles qui sont des données à caractère non personnel afin d'obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation que ce dernier en fait, d'une quelconque autre manière qui puisse porter atteinte à la position commerciale dudit utilisateur sur les marchés où celui-ci exerce ses activités. Cela pourrait inclure l'utilisation des connaissances relatives aux performances globales d'une entreprise ou d'une exploitation agricole à l'occasion de négociations contractuelles avec l'utilisateur sur l'acquisition potentielle de produits ou de produits agricoles de l'utilisateur au détriment de ce dernier ou l'utilisation de ces informations pour alimenter des bases de données plus vastes relatives à certains marchés dans l'ensemble, par exemple, des bases de données sur les rendements des cultures pour la prochaine saison de récolte, parce qu'une telle utilisation pourrait avoir des répercussions négatives indirectes sur l'utilisateur. Il convient de doter l'utilisateur de l'interface technique nécessaire pour lui permettre de gérer les autorisations, qui comprendrait de préférence des options d'autorisation par niveau, telles que "autoriser une fois" ou "autoriser lors de l'utilisation de cette application ou de ce service", y compris l'option de retirer ces autorisations.

(28) En ce qui concerne les contrats conclus entre un détenteur de données et un consommateur en tant qu'utilisateur d'un produit connecté ou d'un service connexe générant des données, le droit de l'Union en matière de protection des consommateurs, en particulier les directives 93/13/CEE et 2005/29/CE, s'applique afin de garantir que le consommateur ne soit pas soumis à des clauses contractuelles abusives. Aux fins du présent règlement, les clauses contractuelles abusives imposées unilatéralement à une entreprise ne devraient pas lier ladite entreprise.

Contrôle du droit d’accéder aux données

(29) Les détenteurs de données peuvent exiger une identification appropriée de l'utilisateur pour vérifier que ce dernier a le droit d’accéder aux données. Dans le cas de données à caractère personnel traitées par un sous-traitant pour le compte du responsable du traitement, les détenteurs de données devraient veiller à ce que la demande d'accès soit reçue et traitée par le sous-traitant.

22. Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

(30) L'utilisateur devrait être libre d'utiliser les données à toutes fins licites. Il peut notamment s'agir de transmettre les données que l'utilisateur a reçues tout en exerçant ses droits prévus par le présent règlement à un tiers proposant un service après-vente qui peut être en concurrence avec un service fourni par un détenteur de données, ou de donner instruction au détenteur de données de le faire. La demande devrait être présentée par l'utilisateur ou par un tiers autorisé à agir pour le compte d'un utilisateur, y compris un fournisseur d'un service d'intermédiation de données. Le détenteur de données devrait veiller à ce que les données mises à la disposition du tiers soient aussi exactes, complètes, fiables, pertinentes et à jour que les données auxquelles lui-même peut accéder ou a le droit d'accéder du fait de l'utilisation du produit connecté ou du service connexe. Tout droit de propriété intellectuelle devrait être respecté lors du traitement des données. Il importe de préserver les incitations à investir dans des produits dotés de fonctionnalités fondées sur l'utilisation de données provenant de capteurs intégrés dans ces produits.

Secret des affaires

(31) La directive (UE) 2016/943 du Parlement européen et du Conseil[23] prévoit que l'obtention, l'utilisation ou la divulgation d'un secret d'affaires est considérée comme licite, entre autres, lorsque cette obtention, cette utilisation ou cette divulgation est requise ou autorisée par le droit de l'Union ou le droit national. Bien que le présent règlement impose aux détenteurs de données de divulguer certaines données aux utilisateurs, ou à des tiers choisis par un utilisateur, même lorsque ces données répondent aux conditions pour être protégées en tant que secrets d'affaires, il devrait être interprété de manière à préserver la protection accordée aux secrets d'affaires au titre de la directive (UE) 2016/943. Dans ce contexte, les détenteurs de données devraient pouvoir exiger des utilisateurs ou des tiers choisis par un utilisateur de préserver la confidentialité des données considérées comme étant des secrets d'affaires. À cette fin, les détenteurs de données devraient identifier les secrets d'affaires avant la divulgation et avoir la possibilité de convenir avec les utilisateurs, ou des tiers choisis par un utilisateur, de mesures nécessaires pour préserver leur confidentialité, y compris par l'utilisation de clauses contractuelles types, d'accords de confidentialité, de protocoles d'accès stricts, de normes techniques et de l'application de codes de conduite. Outre l'utilisation de clauses contractuelles types qui doivent être élaborées et recommandées par la Commission, l'établissement de codes de conduite et de normes techniques relatives à la protection des secrets d'affaires dans le traitement des données pourrait contribuer à la réalisation de l'objectif du présent règlement et devrait être encouragé. En l'absence d'accord sur les mesures nécessaires, ou lorsqu'un utilisateur ou les tiers choisis par un utilisateur ne mettent pas en œuvre les mesures convenues ou compromettent la confidentialité des secrets d'affaires, le détenteur de données devrait pouvoir bloquer ou suspendre le partage de données définies comme secrets d'affaires. En pareils cas, le détenteur de données devrait fournir la décision par écrit à l'utilisateur ou au tiers sans retard injustifié et notifier à l'autorité compétente de l'État membre dans lequel le détenteur de données est établi qu'il a bloqué ou suspendu le partage de données et indiquer les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise. Les détenteurs de données ne peuvent pas, en principe, refuser une demande d'accès aux données présentée au titre du présent règlement au seul motif que certaines données sont considérées comme étant des secrets d'affaires, car cela irait à l'encontre des effets attendus du présent règlement. Toutefois, dans des circonstances exceptionnelles, un détenteur de données qui est un détenteur de secrets d'affaires devrait pouvoir, au cas par cas, rejeter une demande portant sur les données spécifiques en question s'il peut démontrer à l'utilisateur ou au tiers que, malgré les mesures techniques et organisationnelles prises par l'utilisateur ou par le tiers, la divulgation de ce secret d'affaires risque fortement de causer un préjudice économique grave. Le préjudice économique grave implique une perte économique grave et irréparable. Le détenteur de données devrait dûment motiver son refus par écrit, sans retard injustifié, à l'utilisateur ou au tiers et en informer l'autorité compétente. Une telle motivation devrait être fondée sur des éléments objectifs, démontrant le risque concret de préjudice économique grave qui devrait résulter d'une divulgation de données spécifiques et les raisons pour lesquelles les mesures prises pour protéger les données demandées ne sont pas considérées comme étant suffisantes. Une éventuelle incidence négative sur la cybersécurité peut être prise en compte dans ce contexte. Sans préjudice du droit de former un recours devant une juri-

23. Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

diction d'un État membre, lorsque l'utilisateur ou un tiers souhaite contester la décision du détenteur de données de refuser ou de bloquer ou suspendre le partage de données, l'utilisateur ou le tiers peut introduire une réclamation auprès de l'autorité compétente, laquelle devrait décider, sans retard injustifié, si et dans quelles conditions le partage de données devrait commencer ou reprendre, ou peut convenir avec le détenteur de données de saisir un organe de règlement des litiges. Les exceptions aux droits d'accès aux données prévues par le présent règlement ne devraient en aucun cas limiter le droit d'accès et le droit de portabilité des données des personnes concernées au titre du règlement (UE) 2016/679.

cf. RGPD

(32) Le présent règlement n'a pas seulement pour objectif de favoriser le développement de nouveaux produits connectés et services connexes innovants et de stimuler l'innovation sur les marchés de l'après-vente, mais aussi de favoriser le développement de services entièrement nouveaux utilisant les données concernées, y compris sur la base de données provenant de divers produits connectés ou services connexes. Le présent règlement vise dans le même temps à éviter que les incitations à l'investissement soient fragilisées pour le type de produit connecté à partir duquel les données sont obtenues, par exemple du fait de l'utilisation des données pour développer un produit connecté concurrent considéré comme interchangeable ou substituable par les utilisateurs, en particulier sur la base des caractéristiques du produit connecté, de son prix et de son usage prévu. Le présent règlement ne prévoit aucune interdiction de développer un service connexe utilisant des données obtenues en vertu du présent règlement, car cela aurait un effet dissuasif indésirable sur l'innovation. L'interdiction d'utiliser les données auxquelles il est accédé au titre du présent règlement pour développer un produit connecté concurrent protège les efforts d'innovation des détenteurs de données. La question de savoir si un produit connecté est en concurrence avec le produit connecté dont proviennent les données dépend de la question de savoir si les deux produits connectés sont en concurrence sur le même marché de produits. Cela doit être déterminé sur la base des principes établis du droit de la concurrence de l'Union pour définir le marché de produits en cause. Cependant, des finalités licites de l'utilisation des données pourraient inclure l'ingénierie inverse, pour autant qu'elle respecte les exigences prévues par le présent règlement ainsi que par le droit de l'Union ou le droit national. Cela peut être le cas aux fins de la réparation ou de la prolongation de la durée de vie d'un produit connecté ou de la fourniture de services après-vente pour des produits connectés.

Développement de nouveaux services

(33) Lorsque des données sont mises à la disposition d'un tiers, ce tiers peut être une personne physique ou morale, telle qu'un consommateur, une entreprise, un organisme de recherche, un organisme à but non lucratif ou une entité agissant à titre professionnel. En mettant les données à la disposition du tiers, le détenteur de données devrait s'abstenir d'abuser de sa position pour rechercher un avantage concurrentiel sur des marchés où lui-même et le tiers peuvent être en concurrence directe. Le détenteur de données ne devrait donc utiliser aucune donnée facilement accessible pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers, ou sur l'utilisation que ce dernier en fait, d'une quelconque autre manière qui puisse porter atteinte à la position commerciale du tiers sur les marchés où celui-ci exerce ses activités. L'utilisateur devrait pouvoir partager, à des fins commerciales, des données à caractère non personnel avec des tiers. Avec l'accord de l'utilisateur, et sous réserve des dispositions du présent règlement, des tiers devraient pouvoir transférer à d'autres tiers les droits d'accès aux données accordés par l'utilisateur, y compris en échange d'une compensation. Les intermédiaires de données entre entreprises et les systèmes de gestion des informations personnelles (PIMS), appelés "services d'intermédiation de données" dans le règlement (UE) 2022/868, peuvent aider les utilisateurs ou les tiers à établir des relations commerciales avec un nombre indéterminé de contreparties potentielles à des fins licites relevant du champ d'application du présent règlement. Ils pourraient jouer un rôle essentiel dans l'agrégation de l'accès aux données afin de faciliter les analyses de mégadonnées ou l'apprentissage automatique, pour autant que les utilisateurs gardent totalement le contrôle sur l'opportunité de fournir ou de ne pas fournir leurs données à une telle agrégation et sur les conditions commerciales encadrant l'utilisation de leurs données.

(34) L'utilisation d'un produit connecté ou d'un service connexe peut, en particulier lorsque l'utilisateur est une personne physique, générer des données se rapportant à la personne concernée. Le traitement de ces données est soumis aux règles établies par le règlement (UE) 2016/679, y compris lorsque les données à caractère personnel et non personnel figurant dans un ensemble de données sont inextricablement liées. La per-

Traitement de données personnelles

cf. RGPD

sonne concernée peut être l'utilisateur ou une autre personne physique. Les données à caractère personnel ne peuvent être demandées que par un responsable du traitement ou une personne concernée. Au titre du règlement (UE) 2016/679, un utilisateur qui est la personne concernée a le droit, dans certaines circonstances, d'accéder aux données à caractère personnel concernant ledit utilisateur, et le présent règlement ne porte pas atteinte à ce droit. Au titre du présent règlement, l'utilisateur qui est une personne physique a également le droit d'accéder à toutes les données générées par l'utilisation d'un produit connecté, qu'elles soient à caractère personnel ou non personnel. Lorsque l'utilisateur n'est pas la personne concernée mais une entreprise, y compris un entrepreneur individuel, et sauf en cas d'usage domestique partagé du produit connecté, l'utilisateur est considéré comme le responsable du traitement. Dès lors, un tel utilisateur qui, en tant que responsable du traitement, a l'intention de demander des données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe, est tenu de disposer d'une base juridique pour le traitement des données ainsi que l'exige l'article 6, paragraphe 1, du règlement (UE) 2016/679, comme le consentement de la personne concernée ou l'exécution d'un contrat auquel la personne concernée est partie. Un tel utilisateur devrait veiller à ce que la personne concernée soit dûment informée des finalités déterminées, explicites et légitimes du traitement de ces données et de la manière dont la personne concernée peut exercer effectivement ses droits. Lorsque le détenteur de données et l'utilisateur sont des responsables conjoints du traitement au sens de l'article 26 du règlement (UE) 2016/679, ils sont tenus de déterminer, de manière transparente, au moyen d'un accord entre eux, leurs obligations respectives aux fins du respect dudit règlement. Il convient de comprendre qu'un tel utilisateur, une fois que les données ont été mises à disposition, peut à son tour devenir un détenteur de données s'il remplit les critères prévus par le présent règlement et il est alors soumis aux obligations de mise à disposition de données prévues par le présent règlement.

cf. RGPD

cf. RGPD

cf. RGPD

(35) Les données relatives à un produit ou les données relatives à un service connexe ne devraient être mises à la disposition d'un tiers qu'à la demande de l'utilisateur. Le présent règlement complète en conséquence le droit, prévu à l'article 20 du règlement (UE) 2016/679, des personnes concernées de recevoir les données à caractère personnel les concernant dans un format structuré, couramment utilisé et lisible par machine, et de porter ces données vers un autre responsable du traitement, lorsque ces données sont traitées par des procédés automatisés sur la base de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur la base d'un contrat en application de l'article 6, paragraphe 1, point b), dudit règlement. Les personnes concernées ont également le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, mais uniquement lorsque cela est techniquement possible. L'article 20 du règlement (UE) 2016/679 indique qu'il porte sur les données fournies par la personne concernée, mais ne précise pas si cela nécessite un comportement actif de la part de la personne concernée ou s'il s'applique également aux situations dans lesquelles un produit connecté ou un service connexe, par sa conception, observe le comportement d'une personne concernée ou d'autres informations relatives à une personne concernée de manière passive. Les droits prévus par le présent règlement complètent de plusieurs manières le droit de recevoir et de porter des données à caractère personnel prévu à l'article 20 du règlement (UE) 2016/679. Le présent règlement accorde aux utilisateurs le droit d'accéder à toutes données relatives à un produit ou données relatives à un service connexe et de mettre celles-ci à la disposition d'un tiers, quelle que soit leur nature en tant que données à caractère personnel, sans distinction entre les données fournies activement et les données observées passivement, et quelle que soit la base juridique du traitement. À la différence de l'article 20 du règlement (UE) 2016/679, le présent règlement impose et garantit la faisabilité technique de l'accès des tiers à tous les types de données relevant de son champ d'application, qu'elles soient à caractère personnel ou non personnel, garantissant ainsi que les obstacles techniques n'entravent plus ou n'empêchent plus l'accès à ces données. Il permet également aux détenteurs de données de fixer une compensation raisonnable à la charge des tiers, mais pas de l'utilisateur, pour les frais encourus liés à l'octroi d'un accès direct aux données générées par le produit connecté de l'utilisateur. Si un détenteur de données et un tiers ne sont pas en mesure de s'entendre sur les conditions d'un tel accès direct, la personne concernée ne devrait en aucun cas être empêchée d'exercer les droits prévus par le règlement (UE) 2016/679, y compris le droit à la portabilité des données, en introduisant un recours conformément audit règlement. Il convient de comprendre dans ce contexte que, conformément au règlement (UE) 2016/679, un contrat ne permet pas le traitement de catégories particulières de données à caractère personnel par le détenteur de données ou le tiers.

Portabilité

cf. RGPD

cf. RGPD

cf. RGPD

cf. RGPD

Garantie de faisabilité technique de l'accès des tiers

cf. RGPD

(36) L'accès à toutes les données stockées dans les équipements terminaux et auxquelles il est accédé à partir de ces derniers est soumis à la directive 2002/58/CE et requiert le consentement de l'abonné ou de l'utilisateur au sens de ladite directive, à moins qu'il ne soit strictement nécessaire à la fourniture d'un service de la société de l'information expressément demandé par l'utilisateur ou par l'abonné ou aux seules fins de la transmission d'une communication. La directive 2002/58/CE protège l'intégrité de l'équipement terminal d'un utilisateur en ce qui concerne l'utilisation des capacités de traitement et de stockage et la collecte d'informations. Les équipements de l'internet des objets sont considérés comme étant des équipements terminaux s'ils sont directement ou indirectement connectés à un réseau de communications public.

(37) Afin d'empêcher l'exploitation des utilisateurs, les tiers au profit desquels des données ont été mises à disposition à la demande de l'utilisateur ne devraient traiter ces données qu'aux fins convenues avec l'utilisateur et ne les partager avec un autre tiers que si l'utilisateur a donné son accord à ce partage de données.

Autorisation d’accès aux données

(38) Conformément au principe de minimisation des données, les tiers ne devraient avoir accès qu'aux informations nécessaires à la fourniture du service demandé par l'utilisateur. Après avoir obtenu l'accès aux données, le tiers devrait traiter celles-ci aux fins convenues avec l'utilisateur, sans ingérence du détenteur des données. Il devrait être aussi facile pour l'utilisateur de refuser ou d'interrompre l'accès aux données par le tiers que d'autoriser cet accès. Ni les tiers ni les détenteurs de données ne devraient rendre indûment difficile pour l'utilisateur le fait d'effectuer des choix ou d'exercer des droits, notamment en proposant des choix à l'utilisateur d'une manière qui n'est pas neutre, ou en contraignant, trompant ou manipulant l'utilisateur, ou en réduisant ou en compromettant l'autonomie, la prise de décision ou les choix de l'utilisateur, y compris au moyen d'une interface numérique utilisateur ou d'une partie de celle-ci. Dans ce contexte, les tiers ou les détenteurs de données devraient s'abstenir de recourir à des interfaces trompeuses lors de la conception de leurs interfaces numériques. Les interfaces trompeuses sont des techniques de conception qui poussent les consommateurs à prendre des décisions ayant des conséquences négatives pour eux ou qui les induisent en erreur à cette fin. L'utilisation de ces techniques de manipulation peut avoir pour but de persuader les utilisateurs, en particulier les consommateurs vulnérables, d'adopter un comportement non souhaité, de tromper les utilisateurs en les poussant à prendre des décisions relatives à des opérations de divulgation d'informations, ou d'influencer de manière excessive la prise de décision des utilisateurs du service, d'une manière qui sape ou altère leur autonomie, leur prise de décision et leur choix. Les pratiques commerciales communes et légitimes qui sont conformes au droit de l'Union ne devraient pas en soi être considérées comme étant des interfaces trompeuses. Les tiers et les détenteurs de données devraient respecter les obligations qui leur incombent au titre du droit de l'Union pertinent, en particulier les exigences prévues dans les directives 98/6/CE[24] et 2000/31/CE[25]du Parlement européen et du Conseil et dans les directives 2005/29/CE et 2011/83/UE.

Interdiction des interfaces trompeuses

Interdiction du profilage

(39) Les tiers devraient également s'abstenir d'utiliser des données relevant du champ d'application du présent règlement pour effectuer un profilage de personnes, à moins que de telles activités de traitement ne soient strictement nécessaires pour fournir le service demandé par l'utilisateur, y compris dans le contexte d’une prise de décision automatisée. L'obligation d'effacer les données lorsqu'elles ne sont plus nécessaires à la finalité convenue avec l'utilisateur, sauf accord différent en ce qui concerne les données à caractère non personnel, complète le droit à l'effacement conféré à la personne concernée en application de l'article 17 du règlement (UE) 2016/679. Lorsqu'un tiers est un fournisseur d'un service d'intermédiation de données, les garanties pour la personne concernée prévues par le règlement (UE) 2022/868 s'appliquent. Le tiers peut utiliser les données pour développer un produit connecté, ou un service connexe, nouveau et innovant, mais pas pour développer un produit connecté concurrent.

cf. RGPD

24. Directive 98/6/CE du Parlement européen et du Conseil du 16 février 1998 relative à la protection des consommateurs en matière d'indication des prix des produits offerts aux consommateurs (JO L 80 du 18.3.1998, p. 27).
25. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique") (JO L 178 du 17.7.2000, p. 1).

(40) Les start-up, les petites entreprises, les entreprises qui sont qualifiées d'entreprises moyennes au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE et les entreprises des secteurs traditionnels dont les capacités numériques sont moins poussées peinent à obtenir l'accès aux données pertinentes. Le présent règlement vise à faciliter l'accès de ces entités aux données, tout en veillant à ce que les obligations correspondantes soient aussi proportionnées que possible afin d'éviter tout excès. Dans le même temps, un petit nombre de très grandes entreprises ont vu le jour, lesquelles disposent d'une puissance économique considérable dans l'économie numérique grâce à l'accumulation et à l'agrégation de volumes importants de données ainsi qu'à l'infrastructure technologique nécessaire à leur monétisation. Parmi ces très grandes entreprises figurent des entreprises qui fournissent des services de plateforme essentiels contrôlant des écosystèmes de plateformes entiers au sein de l'économie numérique, que les opérateurs du marché existants ou nouveaux sont incapables de concurrencer ou de contester. Le règlement (UE) 2022/1925 du Parlement européen et du Conseil[26] vise à remédier à ces manques d'efficacité et déséquilibres en permettant à la Commission de désigner une entreprise en tant que "contrôleur d'accès", et impose à ces contrôleurs d'accès un certain nombre d'obligations, dont l'interdiction de combiner certaines données sans consentement, et l'obligation de garantir des droits effectifs à la portabilité des données en vertu de l'article 20 du règlement (UE) 2016/679. Conformément au règlement (UE) 2022/1925, et compte tenu de la capacité sans égale de ces entreprises en matière d'acquisition de données, il n'est pas nécessaire, pour atteindre l'objectif du présent règlement, et il serait donc disproportionné à l'égard des détenteurs de données soumis à de telles obligations, d'inclure ces contrôleurs d'accès parmi les bénéficiaires du droit d'accès aux données. Il est probable qu'une telle inclusion limiterait également les avantages du présent règlement pour les PME, liés à l'équité de la répartition de la valeur des données entre les acteurs du marché. Cela signifie qu'une entreprise fournissant des services de plateforme essentiels qui a été désignée comme contrôleur d'accès ne peut pas demander ou se voir accorder l'accès aux données des utilisateurs générées par l'utilisation d'un produit connecté ou d'un service connexe ou par un assistant virtuel en vertu du présent règlement. En outre, les tiers au profit desquels des données sont mises à disposition à la demande de l'utilisateur ne peuvent pas mettre celles-ci à la disposition d'un contrôleur d'accès. Par exemple, le tiers ne peut pas sous-traiter la fourniture d'un service à un contrôleur d'accès. Cela n'empêche toutefois pas que des tiers puissent recourir aux services de traitement de données offerts par un contrôleur d'accès. Cela n'empêche pas non plus ces entreprises d'obtenir et d'utiliser les mêmes données par d'autres moyens licites. Les droits d'accès prévus par le présent règlement contribuent à élargir le choix des services offerts aux consommateurs. Étant donné que les accords volontaires entre les contrôleurs d'accès et les détenteurs de données ne sont pas affectés, limiter le droit d'accès pour les contrôleurs d'accès ne les exclurait pas du marché ni ne les empêcherait de proposer leurs services.

(41) Compte tenu de l'état actuel de la technologie, il serait trop lourd d'imposer aux microentreprises et aux petites entreprises d'autres obligations en matière de conception pour les produits connectés fabriqués ou conçus ou les services connexes fournis par elles. Tel n'est toutefois pas le cas lorsqu'une microentreprise ou une petite entreprise a une entreprise partenaire ou une entreprise liée au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE qui n'est pas qualifiée de microentreprise ou de petite entreprise et lorsqu'elle travaille en sous-traitance pour la fabrication ou la conception d'un produit connecté ou pour fournir un service connexe. En pareils cas, l'entreprise qui a sous-traité la fabrication ou la conception à une microentreprise ou à une petite entreprise est en mesure d'accorder au sous-traitant une compensation appropriée. Une microentreprise ou une petite entreprise peut néanmoins être soumise aux exigences fixées par le présent règlement en tant que détenteur de données lorsqu'elle n'est pas le fabricant du produit connecté ou un fournisseur de services connexes. Une période transitoire devrait s'appliquer à une entreprise qui est qualifiée d'entreprise moyenne depuis moins d'un an et aux produits connectés pendant une période d'un an après la date à laquelle ils ont été mis sur le marché par une entreprise moyenne. Cette période d'un an permet à une telle entreprise moyenne de s'adapter et de se préparer avant d'affronter la concurrence sur le marché des services pour les produits connectés qu'elle fabrique sur la base des droits d'accès prévus par le présent

Équilibre du marché

cf. DMA

cf. RGPD

26. Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1).

règlement. Cette période transitoire ne s'applique pas lorsqu'une telle entreprise moyenne a une entreprise partenaire ou une entreprise liée qui n'est pas qualifiée de microentreprise ou de petite entreprise ou lorsqu'une telle entreprise moyenne a travaillé en sous-traitance pour la fabrication ou la conception du produit connecté ou pour fournir le service connexe.

Règles horizontales d’accès aux données

(42) Compte tenu de la diversité des produits connectés qui génèrent des données de nature, de volume et de fréquence différents, présentent des niveaux différents de risques en matière de données et de cybersécurité et offrent des possibilités économiques de valeur différente, et dans le but d'assurer la cohérence des pratiques de partage de données dans le marché intérieur, y compris entre les secteurs, et d'encourager et de promouvoir des pratiques équitables de partage de données, même dans les domaines où un tel droit d'accès aux données n'est pas prévu, le présent règlement prévoit des règles horizontales sur les modalités d'accès aux données, chaque fois qu'un détenteur de données est tenu, par le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union, de mettre des données à la disposition d'un destinataire de données. Un tel accès devrait être fondé sur des modalités et conditions équitables, raisonnables, non discriminatoires et transparentes. Ces règles générales d'accès ne s'appliquent pas aux obligations de mise à disposition de données prévues par le règlement (UE) 2016/679. Le partage volontaire de données n'est pas compromis par ces règles. Les clauses contractuelles types non contraignantes pour le partage de données entre entreprises qui doivent être élaborées et recommandées par la Commission peuvent aider les parties à conclure des contrats qui prévoient des modalités et conditions équitables, raisonnables et non discriminatoires et qui doivent être mis en œuvre de manière transparente. La conclusion de contrats, qui peuvent contenir les clauses contractuelles types non contraignantes, ne devrait pas signifier que le droit de partager des données avec des tiers est, de quelque manière que ce soit, subordonné à l'existence d'un tel accord. Si les parties ne sont pas en mesure de conclure un accord sur le partage des données, y compris avec l'aide d'organes de règlement des litiges, le droit de partager des données avec des tiers est opposable devant les juridictions nationales.

cf. RGPD

(43) Sur la base du principe de la liberté contractuelle, les parties devraient rester libres de négocier les conditions précises de mise à disposition de données dans leurs contrats, dans le cadre des règles générales d'accès pour la mise à disposition de données. Les clauses de ces contrats pourraient inclure des mesures techniques et organisationnelles, y compris en ce qui concerne la sécurité des données.

(44) Afin de garantir que les conditions d'accès obligatoire aux données soient équitables pour les deux parties à un contrat, les règles générales relatives aux droits d'accès aux données devraient faire référence à la règle visant à éviter les clauses contractuelles abusives.

Non discrimination entre destinataires de données

(45) Aucun accord conclu dans le cadre de relations entre entreprises au sujet d'une mise à disposition de données ne devrait créer de discrimination entre différentes catégories comparables de destinataires de données, que les parties soient de grandes entreprises ou des PME. Afin de compenser le manque d'informations sur les conditions figurant dans les différents contrats, qui complique la tâche du destinataire des données s'agissant de déterminer si les conditions de mise à disposition des données sont non discriminatoires, il devrait relever de la responsabilité des détenteurs de données de démontrer la nature non discriminatoire d'une clause contractuelle. N'est pas constitutif d'une discrimination illicite le fait qu'un détenteur de données ait recours à des clauses contractuelles différentes pour la mise à disposition des données si ces différences sont justifiées par des raisons objectives. Ces obligations sont sans préjudice du règlement (UE) 2016/679.

cf. RGPD

Compensation pour mise à disposition de données

(46) Afin de promouvoir la poursuite des investissements dans la production et la mise à disposition de données précieuses, y compris dans des outils techniques pertinents, tout en évitant d'alourdir de manière excessive l'accès aux données et l'utilisation de données, ce qui rendrait le partage de données non viable sur le plan commercial, le présent règlement consacre le principe selon lequel, dans les relations entre entreprises, les détenteurs de données peuvent demander une compensation raisonnable lorsqu'ils sont tenus, en vertu du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, de mettre des données à la disposition d'un destinataire de données. Une telle compensation ne devrait pas être comprise comme constituant un paiement en échange des données proprement dit. Il convient que la

Commission adopte des lignes directrices sur le calcul d'une compensation raisonnable dans le cadre de l'économie fondée sur les données.

Frais techniques

(47) Premièrement, une compensation raisonnable pour le respect de l'obligation en application du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union de donner suite à une demande de mise à disposition de données peut inclure une compensation pour les coûts occasionnés par la mise à disposition des données. Ces coûts peuvent correspondre à des frais techniques, tels que ceux nécessaires à la reproduction, la diffusion par voie électronique et le stockage des données, mais pas à la collecte ou la production des données. Ces frais techniques peuvent également inclure les frais de traitement nécessaires à la mise à disposition des données, y compris ceux liés au formatage des données. Les coûts associés à la mise à disposition des données peuvent également inclure les frais visant à faciliter les demandes concrètes de partage de données. Ils peuvent aussi varier en fonction du volume des données ainsi que des accords conclus pour la mise à disposition des données. Des accords à long terme entre les détenteurs de données et les destinataires de données, par exemple au moyen d'un modèle d'abonnement ou de l'utilisation de contrats intelligents, peuvent réduire les coûts lors de transactions régulières ou répétitives dans le cadre d'une relation commerciale. Les coûts liés à la mise à disposition des données peuvent être spécifiques à une demande particulière ou partagés avec d'autres demandes. Dans ce dernier cas, un destinataire de données unique ne devrait pas payer l'intégralité des frais relatifs à la mise à disposition des données. Deuxièmement, une compensation raisonnable peut également inclure une marge, sauf en ce qui concerne les PME et les organismes de recherche à but non lucratif. Une marge peut varier en fonction de facteurs liés aux données elles-mêmes, tels que le volume, le format ou la nature des données. Elle peut tenir compte des coûts associés à la collecte des données. Une marge peut donc diminuer lorsque le détenteur de données a collecté les données pour sa propre activité sans investissement important, ou augmenter s'il a beaucoup investi dans la collecte de données pour les besoins de son activité. Elle peut être limitée, voire exclue, dans les situations où l'utilisation des données par le destinataire de données n'a aucune incidence sur les activités propres du détenteur de données. Le fait que les données soient cogénérées par un produit connecté qui appartient à l'utilisateur, qu'il loue ou qu'il utilise en crédit-bail pourrait également réduire le montant de la compensation, comparativement à d'autres situations dans lesquelles les données sont générées par le détenteur de données, par exemple lors de la fourniture d'un service connexe.

Marge

(48) Il n'est pas nécessaire d'intervenir en cas de partage de données entre grandes entreprises, ou lorsque le détenteur de données est une petite entreprise ou une entreprise moyenne et que le destinataire de données est une grande entreprise. En pareils cas, les entreprises sont considérées comme capables de négocier la compensation dans les limites de ce qui est raisonnable et non discriminatoire.

(49) Afin de protéger les PME contre des charges économiques excessives qui les pénaliseraient trop sur le plan commercial pour élaborer et appliquer des modèles d'entreprise innovants, la compensation raisonnable à payer par celles-ci pour la mise à disposition de données ne devrait pas dépasser les coûts directement liés à cette mise à disposition. Les coûts directement liés sont ceux qui sont imputables à des demandes individuelles, compte tenu du fait que les interfaces techniques nécessaires ou les logiciels et la connectivité connexes doivent être installés de manière permanente par le détenteur des données. Le même régime devrait s'appliquer aux organismes de recherche à but non lucratif.

(50) Dans des cas dûment justifiés, y compris lorsqu'il faut préserver la participation des consommateurs et la concurrence ou promouvoir l'innovation sur certains marchés, une compensation réglementée pour la mise à disposition de types de données spécifiques peut être prévue par le droit de l'Union ou la législation nationale adoptée conformément au droit de l'Union.

Transparence de la compensation

(51) La transparence est un principe important pour garantir que la compensation demandée par un détenteur de données est raisonnable ou, si le destinataire de données est une PME ou un organisme de recherche à but non lucratif, que la compensation n'excède pas les coûts directement liés à la mise à la disposition du destinataire de données, des données et est imputable à la demande individuelle concernée. Afin de mettre les destinataires de données en mesure d'évaluer et de vérifier que la compensation satisfait aux exigences du présent règlement, le détenteur de données devrait four-

nir au destinataire de données des informations suffisamment détaillées pour le calcul de la compensation.

Règlement des litiges

(52) Garantir l'accès à des modes de règlement extrajudiciaire des litiges nationaux et transfrontières liés à la mise à disposition de données devrait profiter aux détenteurs de données et aux destinataires de données et, partant, renforcer la confiance dans le partage des données. Lorsque les parties ne parviennent pas à s'entendre sur des modalités et conditions équitables, raisonnables et non discriminatoires de mise à disposition des données, des organes de règlement des litiges devraient leur proposer une solution simple, rapide et peu coûteuse. Le présent règlement ne fixant que les conditions devant être remplies par les organes de règlement des litiges pour être certifiés, les États membres sont libres d'adopter toute règle spécifique concernant la procédure de certification, y compris l'expiration ou le retrait de la certification. Les dispositions du présent règlement relatives au règlement des litiges ne devraient pas imposer aux États membres de mettre en place des organes de règlement des litiges.

(53) La procédure de règlement des litiges prévue par le présent règlement est une procédure volontaire qui permet aux utilisateurs, aux détenteurs de données et aux destinataires de données de convenir de porter leurs différends devant des organes de règlement des litiges. Par conséquent, les parties devraient être libres de saisir l'organe de règlement des litiges de leur choix, que celui-ci se trouve à l'intérieur ou à l'extérieur des États membres dans lesquels elles sont établies.

(54) Afin d'éviter des situations dans lesquelles deux ou plusieurs organes de règlement des litiges seraient saisis du même litige, en particulier dans une situation transfrontière, tout organe de règlement des litiges devrait pouvoir refuser de traiter une demande de règlement d'un litige qui a déjà été porté devant un autre organe de règlement des litiges ou devant une juridiction d'un État membre.

(55) Afin d'assurer l'application uniforme du présent règlement, les organes de règlement des litiges devraient tenir compte des clauses contractuelles types non contraignantes qui doivent être élaborées et recommandées par la Commission, ainsi que des dispositions du droit de l'Union ou du droit national précisant les obligations en matière de partage des données ou des lignes directrices publiées par les autorités sectorielles pour l'application de telles dispositions.

(56) Les parties à une procédure de règlement des litiges ne devraient pas être empêchées d'exercer leurs droits fondamentaux à un recours effectif et à un procès équitable. Par conséquent, la décision de saisir un organe de règlement des litiges ne devrait pas priver ces parties de leur droit de demander réparation devant une juridiction d'un État membre. Les organes de règlement des litiges devraient rendre publics des rapports annuels d'activités.

Divulgation illicite de données

(57) Les détenteurs de données peuvent appliquer des mesures techniques de protection appropriées pour empêcher la divulgation illicite de données ou l'accès illicite à des données. Toutefois, ces mesures ne devraient pas donner lieu à une discrimination entre les destinataires de données ni entraver l'accès aux données ou l'utilisation de celles-ci pour les utilisateurs ou les destinataires de données. En cas de pratiques abusives de la part d'un destinataire de données, comme le fait de duper le détenteur de données en fournissant de fausses informations dans l'intention d'utiliser les données à des fins illicites, notamment la mise au point d'un produit connecté concurrent sur la base des données, le détenteur de données et, le cas échéant et s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires ou l'utilisateur peut demander au tiers ou au destinataire de données de mettre en œuvre, sans retard injustifié, des mesures correctives ou de remédiation. Toutes les demandes de ce type, et en particulier celles visant à mettre fin à la production, à l'offre ou à la mise sur le marché de biens, de données dérivées ou de services, ainsi que celles visant à mettre fin à l'importation, à l'exportation, au stockage de biens non conformes ou visant à ce que ceux-ci soient détruits, devraient être évaluées à la lumière de leur proportionnalité par rapport aux intérêts du détenteur de données, du détenteur de secrets d'affaires ou de l'utilisateur.

(58) Lorsqu'une partie se trouve dans une position de négociation plus forte, il existe un risque que cette partie puisse exploiter cette position au détriment de l'autre partie contractante lors de la négociation de l'accès aux données de sorte que l'accès aux données est commercialement moins viable, et parfois prohibitif, sur le plan économique.

Ces déséquilibres contractuels portent préjudice à toutes les entreprises qui ne disposent pas d'une capacité importante pour négocier les conditions d'accès aux données et qui n'ont peut-être pas d'autre choix que d'accepter des clauses contractuelles "à prendre ou à laisser". Par conséquent, les clauses contractuelles abusives régissant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction des obligations liées aux données, ne devraient pas être contraignantes pour les entreprises lorsque ces clauses ont été imposées unilatéralement à ces entreprises.

(59) Les règles relatives aux clauses contractuelles devraient tenir compte du principe de la liberté contractuelle en tant que concept essentiel dans les relations entre entreprises. Par conséquent, les clauses contractuelles ne devraient pas toutes être soumises à une appréciation du caractère abusif, mais uniquement celles qui sont imposées unilatéralement. Il s'agit des situations du type "à prendre ou à laisser" dans lesquelles une partie prévoit une certaine clause contractuelle et où l'autre entreprise ne peut pas influencer le contenu de cette clause malgré une tentative de négociation. Une clause contractuelle qui est simplement prévue par une partie et acceptée par l'autre entreprise, ou une clause négociée puis convenue sous une forme modifiée entre les parties contractantes, ne devrait pas être considérée comme ayant été imposée unilatéralement.

Clauses contractuelles abusives

(60) En outre, les règles relatives aux clauses contractuelles abusives ne devraient s'appliquer qu'aux éléments d'un contrat qui sont liés à la mise à disposition de données, à savoir les clauses contractuelles concernant l'accès aux données et l'utilisation des données, ainsi que la responsabilité ou les voies de recours en cas de violation et d'extinction des obligations relatives aux données. Les autres parties du même contrat, qui ne sont pas liées à la mise à disposition de données, ne devraient pas être soumises à l'appréciation du caractère abusif prévue par le présent règlement.

(61) Les critères permettant de déterminer les clauses contractuelles abusives ne devraient s'appliquer qu'aux clauses contractuelles excessives, en cas d'abus d'un pouvoir de négociation supérieur. La grande majorité des clauses contractuelles qui sont commercialement plus favorables à une partie qu'à l'autre, y compris celles qui sont normales dans les contrats entre entreprises, sont une expression normale du principe de la liberté contractuelle et continuent de s'appliquer. Aux fins du présent règlement, un écart flagrant par rapport aux bonnes pratiques commerciales inclurait, entre autres, une atteinte objective à la capacité de la partie à laquelle la clause a été imposée unilatéralement de protéger son intérêt commercial légitime dans les données en question.

(62) Afin de garantir la sécurité juridique, le présent règlement dresse une liste de clauses qui sont toujours considérées comme abusives et une liste de clauses qui sont présumées être abusives. Dans ce dernier cas, l'entreprise qui impose la clause contractuelle devrait pouvoir renverser la présomption de caractère abusif en démontrant que la clause contractuelle mentionnée dans la liste qui figure dans le présent règlement n'est pas abusive dans le cas particulier en question. Si une clause contractuelle n'est pas incluse dans la liste des clauses qui sont toujours considérées comme abusives ou présumées abusives, la disposition générale sur le caractère abusif s'applique. À cet égard, les clauses énumérées en tant que clauses contractuelles abusives dans le présent règlement devraient servir de critère d'interprétation de la disposition générale relative au caractère abusif. Enfin, des clauses contractuelles types non contraignantes pour les contrats de partage de données entre entreprises que la Commission doit élaborer et recommander peuvent également être utiles aux parties commerciales lorsqu'elles négocient des contrats. Si une clause contractuelle est déclarée abusive, le contrat concerné devrait continuer à s'appliquer sans cette clause, à moins que la clause contractuelle abusive ne soit pas dissociable des autres clauses du contrat.

Organismes publics et situations d’urgence ou exceptionnelles

(63) En cas de besoin exceptionnel, les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union peuvent être contraints d'utiliser, dans l'exercice de leurs fonctions statutaires à des fins d'intérêt public, des données existantes, y compris, le cas échéant, les métadonnées qui les accompagnent, pour réagir à des situations d'urgence ou dans d'autres cas exceptionnels. Les besoins exceptionnels correspondent à des circonstances imprévisibles et limitées dans le temps, contrairement à d'autres circonstances qui pourraient être planifiées, programmées, périodiques ou fréquentes. Alors que la notion de "détenteur de données" n'inclut pas, en règle générale, les organismes du secteur public, elle peut inclure des entreprises publiques. Les organismes exerçant une activité de recherche et les organi-

sations finançant une activité de recherche pourraient aussi être organisés comme des organismes du secteur public ou des organismes de droit public. Afin de limiter la charge pesant sur les entreprises, les microentreprises et les petites entreprises ne devraient être tenues de fournir des données aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union qu'en cas de besoin exceptionnel lorsque ces données sont requises pour réagir à une situation d'urgence et que l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir de telles données par d'autres moyens de manière rapide et efficace et dans des conditions équivalentes.

(64) En cas de situations d'urgence, telles que les urgences de santé publique, les urgences résultant de catastrophes naturelles, y compris celles aggravées par le changement climatique et la dégradation de l'environnement, ainsi que les catastrophes majeures d'origine humaine, telles que les incidents majeurs de cybersécurité, l'intérêt public résultant de l'utilisation des données l'emportera sur l'intérêt des détenteurs de données à disposer librement des données qu'ils détiennent. Dans ce cas, les détenteurs de données devraient être tenus de les mettre à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union à leur demande. L'existence d'une situation d'urgence devrait être déterminée ou déclarée conformément au droit de l'Union ou au droit national et fondée sur les procédures pertinentes, y compris celles des organisations internationales compétentes. Dans de tels cas, l'organisme du secteur public devrait démontrer que les données faisant l'objet de la demande ne pourraient pas, autrement, être obtenues de manière rapide et efficace et dans des conditions équivalentes, par exemple au moyen de la fourniture volontaire de données par une autre entreprise ou de la consultation d'une base de données publique.

(65) Un besoin exceptionnel peut également résulter de situations non urgentes. Dans de tels cas, un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union devrait être uniquement autorisé à demander des données à caractère non personnel. L'organisme du secteur public devrait démontrer que les données sont nécessaires à l'exécution d'une mission spécifique d'intérêt public explicitement prévue par la loi, telle que la production de statistiques officielles ou l'atténuation d'une situation d'urgence ou le rétablissement à la suite d'une situation d'urgence. En outre, une telle demande ne peut être effectuée que lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union a déterminé des données spécifiques qui ne pourraient pas, autrement, être obtenues de manière rapide et efficace et dans des conditions équivalentes, et uniquement s'il a épuisé tous les autres moyens à sa disposition pour se procurer ces données, tels que l'obtention des données au moyen d'accords volontaires, notamment en achetant des données à caractère non-personnel sur le marché aux prix du marché, ou le recours aux obligations existantes de mise à disposition des données ou l'adoption de nouvelles mesures législatives susceptibles de garantir la disponibilité des données en temps utile. Les conditions et principes régissant les demandes, tels que ceux liés à la limitation de la finalité, à la proportionnalité, à la transparence et à la limitation dans le temps, devraient également s'appliquer. En cas de demande de données nécessaires à la production de statistiques officielles, l'organisme du secteur public demandeur devrait également démontrer si le droit national l'autorise à acheter des données à caractère non-personnel sur le marché.

(66) Le présent règlement ne devrait pas s'appliquer aux accords volontaires d'échange de données entre entités privées et publiques, y compris la fourniture de données par les PME, ni s'y substituer, et est sans préjudice des actes juridiques de l'Union prévoyant des demandes d'informations obligatoires adressées par des entités publiques à des entités privées. Le présent règlement ne devrait pas avoir d'incidence sur les obligations imposées aux détenteurs de données de fournir des données qui sont motivées par des besoins de nature non exceptionnelle, en particulier lorsque l'éventail des données et des détenteurs de données est connu ou que l'utilisation des données peut avoir lieu régulièrement, comme dans le cas des obligations de déclaration et des obligations relatives au marché intérieur. Il ne devrait pas non plus avoir d'incidence sur les exigences relatives à l'accès aux données dans le but de vérifier le respect des règles applicables, y compris lorsque des organismes du secteur public confient la tâche de vérification du respect des règles à des entités autres que des organismes du secteur public.

(67) Le présent règlement complète, sans y porter atteinte, le droit de l'Union et le droit national prévoyant l'accès aux données et l'utilisation des données à des fins statistiques, en particulier le règlement (CE) no 223/2009 du Parlement européen et du Conseil[27], ainsi que les actes juridiques nationaux relatifs aux statistiques officielles.

(68) Pour l'exercice de leurs missions dans les domaines de la prévention ou de la détection des infractions pénales ou administratives, des enquêtes ou des poursuites en la matière, ou de l'exécution de sanctions pénales et administratives, ainsi que de la collecte de données à des fins fiscales ou douanières, les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union devraient faire valoir les pouvoirs qui leur sont conférés par le droit de l'Union ou le droit national. Le présent règlement ne porte donc pas atteinte aux actes législatifs relatifs au partage des données, à l'accès aux données et à l'utilisation des données dans ces domaines.

cf. RGPD

(69) Conformément à l'article 6, paragraphes 1 et 3, du règlement (UE) 2016/679, un cadre proportionné, limité et prévisible au niveau de l'Union est nécessaire lors de l'établissement de la base juridique permettant aux détenteurs de données, en cas de besoins exceptionnels, de mettre des données à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union, à la fois pour garantir la sécurité juridique et pour réduire au minimum les charges administratives pesant sur les entreprises. À cette fin, les demandes de données émanant d'organismes du secteur public, de la Commission, de la Banque centrale européenne ou d'organes de l'Union adressées aux détenteurs de données devraient être spécifiques, transparentes et proportionnées en ce qui concerne l'étendue de leur contenu et leur granularité. La finalité de la demande et l'utilisation prévue des données demandées devraient être spécifiques et clairement expliquées, tout en laissant à l'entité demandeuse une souplesse suffisante pour lui permettre d'exécuter ses missions spécifiques d'intérêt public. La demande devrait également respecter les intérêts légitimes des détenteurs de données auxquels elle est adressée. La charge pesant sur les détenteurs de données devrait être réduite au minimum en obligeant les entités demandeuses à respecter le principe "une fois pour toutes", qui empêche que les mêmes données soient demandées plus d'une fois par plus d'un organisme du secteur public ou par la Commission, la Banque centrale européenne ou des organes de l'Union. Dans un souci de transparence, les demandes de données formulées par la Commission, la Banque centrale européenne ou des organes de l'Union devraient être rendues publiques sans retard injustifié par l'entité qui demande les données. La Banque centrale européenne et les organes de l'Union devraient informer la Commission de leurs demandes. Si la demande de données a été formulée par un organisme du secteur public, cet organisme devrait également adresser une notification au coordinateur de données de l'État membre dans lequel l'organisme du secteur public est établi. Il convient de veiller à ce que toutes les demandes soient mises à la disposition du public en ligne. Dès réception de la notification d'une demande de données, l'autorité compétente peut décider d'évaluer la légalité de la demande et d'exercer ses fonctions en ce qui concerne l'exécution et l'application du présent règlement. La mise à la disposition du public en ligne de toutes les demandes formulées par des organismes du secteur public devrait être assurée par le coordinateur de données.

(70) L'objectif de l'obligation de fournir les données est de faire en sorte que les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union disposent des connaissances nécessaires pour réagir à une situation d'urgence, prévenir une situation d'urgence ou se rétablir à la suite d'une situation d'urgence, ou encore maintenir la capacité d'accomplir des missions spécifiques expressément prévues par la loi. Les données obtenues par ces entités peuvent être commercialement sensibles. Par conséquent, ni le règlement (UE) 2022/868 ni la directive (UE) 2019/1024 du Parlement européen et du Conseil[28] ne devraient s'appli-

27. Règlement (CE) no 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) no 1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) no 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).
28. Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (JO L 172 du 26.6.2019, p. 56).

quer aux données mises à disposition en vertu du présent règlement qui ne devraient pas être considérées comme des données ouvertes disponibles pour une réutilisation par des tiers. Cela ne devrait toutefois pas avoir d'incidence sur l'applicabilité de la directive (UE) 2019/1024 à la réutilisation de statistiques officielles pour la production desquelles les données obtenues en vertu du présent règlement ont été utilisées, à condition que la réutilisation ne comprenne pas les données sous-jacentes. En outre, et pour autant que les conditions énoncées dans le présent règlement soient satisfaites, la possibilité de partager les données à des fins de recherche ou pour le développement, la production et la diffusion de statistiques officielles ne devrait pas être affectée. Les organismes du secteur public devraient également être autorisés à échanger des données obtenues en vertu du présent règlement avec d'autres organismes du secteur public, la Commission, la Banque centrale européenne ou des organes de l'Union afin de répondre aux besoins exceptionnels pour lesquels les données ont été demandées.

(71) Les détenteurs de données devraient avoir la possibilité soit de rejeter une demande présentée par un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union, soit de demander sa modification sans retard injustifié et, en tout état de cause, au plus tard dans un délai de cinq ou trente jours ouvrables, en fonction de la nature du besoin exceptionnel invoqué dans la demande. Le cas échéant, le détenteur de données devrait avoir cette possibilité lorsqu'il n'a aucun contrôle sur les données demandées, c'est-à-dire lorsqu'il n'a pas immédiatement accès aux données et qu'il ne peut pas déterminer leur disponibilité. Un motif valable de ne pas mettre les données à disposition devrait exister s'il peut être démontré que la demande est similaire à une demande présentée précédemment pour la même finalité par un autre organisme du secteur public, ou la Commission, la Banque centrale européenne ou un organe de l'Union et le détenteur de données ne s'est pas vu notifier l'effacement des données en vertu du présent règlement. Un détenteur de données qui rejette la demande ou demande sa modification devrait communiquer à l'organisme du secteur public, à la Commission, à la Banque centrale européenne ou à l'organe de l'Union qui demande les données la justification sous-jacente. Lorsque les droits sui generis liés à la base de données prévus par la directive 96/9/CE du Parlement européen et du Conseil[29] s'appliquent aux ensembles de données demandés, les détenteurs de données devraient exercer leur droit d'une manière qui n'empêche pas l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union d'obtenir les données, ou de les partager, conformément au présent règlement.

(72) En cas de besoin exceptionnel lié à une réaction à une situation d'urgence, les organismes du secteur public devraient utiliser des données à caractère non personnel chaque fois que cela est possible. En cas de demande fondée sur un besoin exceptionnel non lié à une situation d'urgence, les données à caractère personnel ne peuvent pas être demandées. Chaque fois que des données à caractère personnel relèvent du champ de la demande, le détenteur de données devrait les anonymiser. Lorsqu'il est strictement nécessaire d'inclure des données à caractère personnel dans les données qui doivent être mises à la disposition d'un organisme du secteur public, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union ou lorsque l'anonymisation s'avère impossible, l'entité qui demande les données devrait démontrer la stricte nécessité et les finalités spécifiques et limitées du traitement. Les règles applicables en matière de protection des données à caractère personnel devraient être respectées. La mise à disposition des données et leur utilisation ultérieure devraient s'accompagner de garanties pour les droits et intérêts des personnes concernées par ces données.

(73) Les données mises à la disposition des organismes du secteur public, de la Commission, de la Banque centrale européenne ou des organes de l'Union sur le fondement d'un besoin exceptionnel ne devraient être utilisées que pour les finalités pour lesquelles elles ont été demandées, à moins que le détenteur de données qui a mis les données à disposition n'ait expressément consenti à ce que les données soient utilisées à d'autres fins. Les données devraient être effacées dès lors qu'elles ne sont plus nécessaires aux finalités indiquées dans la demande, sauf accord contraire, et le détenteur de données devrait en être informé. Le présent règlement s'appuie sur les règles d'accès en vigueur dans l'Union et dans les États membres et ne modifie pas les dispositions de

29. Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données (JO L 77 du 27.3.1996, p. 20).

droit national en matière d'accès du public aux documents dans le contexte des obligations de transparence. Les données devraient être effacées dès qu'elles ne sont plus nécessaires pour se conformer à ces obligations de transparence.

(74) Lors de la réutilisation des données fournies par les détenteurs de données, les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union devraient respecter à la fois le droit de l'Union ou le droit national applicables en vigueur et les obligations contractuelles auxquelles le détenteur de données est soumis. Ils devraient s'abstenir de mettre au point ou d'améliorer un produit connecté ou un service connexe concurrençant le produit connecté ou service connexe du détenteur de données, ainsi que de partager les données avec un tiers à ces fins. Ils devraient également accorder une reconnaissance publique aux détenteurs de données à la demande de ces derniers et devraient être responsables du maintien de la sécurité des données reçues. Lorsque la divulgation de secrets d'affaires du détenteur de données à des organismes du secteur public, à la Commission, à la Banque centrale européenne ou à des organes de l'Union est strictement nécessaire pour atteindre la finalité pour laquelle les données ont été demandées, la confidentialité de cette divulgation devrait être garantie avant la divulgation des données.

(75) Lorsque la sauvegarde d'un bien public important est en jeu, comme lorsqu'il s'agit de réagir à une situation d'urgence, l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union concerné ne devrait pas être tenu d'indemniser les entreprises pour les données obtenues. Les situations d'urgence sont des événements rares et ces urgences ne nécessitent pas toutes l'utilisation de données détenues par des entreprises. Dans le même temps, l'obligation de fournir des données pourrait représenter une charge considérable pour les microentreprises et les petites entreprises. Elles devraient donc être autorisées à réclamer une compensation même dans le cadre d'une réaction à une situation d'urgence. Le fait que les organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union fassent usage du présent règlement ne devrait donc pas avoir des répercussions négatives sur les activités commerciales des détenteurs de données. Toutefois, étant donné que les cas de besoins exceptionnels autres que les cas de réaction à des situations d'urgence pourraient être plus fréquents, les détenteurs de données devraient, dans de telles situations, avoir droit à une compensation raisonnable qui ne devrait pas dépasser les coûts techniques et organisationnels encourus pour se conformer à la demande et la marge raisonnable nécessaire pour mettre les données à la disposition de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union. La compensation ne devrait pas être comprise comme constituant le paiement des données proprement dites ou comme étant obligatoire. Les détenteurs de données ne devraient pas pouvoir prétendre à une compensation lorsque le droit national interdit aux instituts nationaux de statistique ou aux autres autorités nationales chargées de la production de statistiques d'indemniser les détenteurs de données pour la mise à disposition de données. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union concerné devrait pouvoir contester le niveau de compensation demandé par le détenteur de données en saisissant l'autorité compétente de l'État membre dans lequel le détenteur de données est établi.

(76) Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union devrait être habilité à partager les données qu'il a obtenues à la suite de la demande avec d'autres entités ou personnes lorsque cela est nécessaire pour mener des activités de recherche scientifique ou des activités d'analyse qu'il ne peut pas réaliser lui-même, à condition que ces activités soient compatibles avec la finalité pour laquelle les données ont été demandées. Il devrait informer le détenteur de données de ce partage en temps utile. Ces données peuvent également être partagées dans les mêmes conditions avec les instituts nationaux de statistique et Eurostat pour le développement, la production et la diffusion de statistiques officielles. Ces activités de recherche devraient toutefois être compatibles avec la finalité pour laquelle les données ont été demandées et le détenteur des données devrait être informé du partage ultérieur des données qu'il a fournies. Les personnes menant des activités de recherche ou les organismes de recherche avec lesquels ces données peuvent être partagées devraient agir soit dans un but non lucratif, soit dans le cadre d'une mission d'intérêt public reconnue par l'État. Les organismes sur lesquels des entreprises commerciales exercent une influence notable, permettant à ces entreprises d'exercer un contrôle en raison d'éléments structurels qui pourrait conduire à un accès préférentiel aux résultats

des recherches, ne devraient pas être considérés comme étant des organismes de recherche aux fins du présent règlement.

(77) Afin de traiter une situation d'urgence transfrontière ou un autre besoin exceptionnel, des demandes de données peuvent être adressées à des détenteurs de données dans des États membres autres que celui de l'organisme du secteur public demandeur. Dans ce cas, l'organisme du secteur public demandeur devrait adresser une notification à l'autorité compétente de l'État membre dans lequel le détenteur de données est établi afin de lui permettre d'examiner la demande au regard des critères établis dans le présent règlement. Il devrait en aller de même pour les demandes présentées par la Commission, la Banque centrale européenne ou un organe de l'Union. Lorsque des données à caractère personnel sont demandées, l'organisme du secteur public devrait adresser une notification à l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 dans l'État membre dans lequel l'organisme du secteur public est établi. L'autorité compétente concernée devrait être habilitée à conseiller l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union en vue de coopérer avec les organismes du secteur public de l'État membre dans lequel le détenteur de données est établi en ce qui concerne la nécessité de réduire au minimum la charge administrative pesant sur le détenteur de données. Lorsque l'autorité compétente soulève des objections dûment étayées en ce qui concerne la conformité de la demande avec le présent règlement, elle devrait rejeter la demande de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union, qui devrait tenir compte de ces objections avant de prendre toute nouvelle mesure, y compris soumettre à nouveau la demande.

cf. RGPD

Portabilité

(78) La capacité des clients de services de traitement de données, y compris de services en nuage et de services à la périphérie, de passer d'un service de traitement de données à un autre, tout en maintenant une fonctionnalité minimale du service et sans interruption des services, ou d'utiliser simultanément les services de plusieurs fournisseurs sans obstacles injustifiés ou frais excessifs de transfert de données, est une condition essentielle pour un marché plus concurrentiel, avec des barrières à l'entrée moins élevées pour les nouveaux fournisseurs de services de traitement de données, et pour garantir une plus grande résilience aux utilisateurs de ces services. Les clients bénéficiant d'offres gratuites devraient également bénéficier des dispositions relatives au changement de fournisseur prévues par le présent règlement, de sorte que ces offres n'entraînent pas un effet de verrouillage pour les clients.

(79) Le règlement (UE) 2018/1807 du Parlement européen et du Conseil[30] encourage les fournisseurs de services de traitement de données à élaborer et à mettre en œuvre de manière efficace des codes de conduite par autorégulation couvrant les bonnes pratiques pour, entre autres, faciliter le changement de fournisseur de services de traitement de données et le portage des données. Compte tenu de l'adoption limitée des cadres d'autorégulation mis au point à cette fin et de l'indisponibilité générale de normes et d'interfaces ouvertes, il est nécessaire d'adopter un ensemble d'obligations réglementaires minimales pour les fournisseurs de services de traitement de données afin d'éliminer les obstacles précommerciaux, commerciaux, techniques, contractuels et organisationnels, lesquels ne se limitent pas à la réduction de la vitesse de transfert des données lors du désengagement du client, qui freinent le changement effectif de services de traitement de données.

Services de traitement de données

(80) Les services de traitement de données devraient couvrir les services qui permettent un accès universel et à la demande par réseau à un ensemble partagé, configurable, modulable et variable de ressources informatiques distribuées. Ces ressources informatiques comprennent des ressources telles que les réseaux, serveurs ou autres infrastructures virtuelles ou physiques, les logiciels, y compris les outils de développement de logiciels, le stockage, les applications et les services. La capacité du client du service de traitement de données à s'équiper unilatéralement en ressources informatiques, comme en temps de serveur ou en stockage en réseau, sans aucune intervention humaine de la part du fournisseur de services de traitement de données pourrait être décrite comme exigeant un minimum d'efforts de gestion et d'interaction entre le fournisseur et le client. Le terme "universel" est utilisé pour décrire les capacités de calcul

30. Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (JO L 303 du 28.11.2018, p. 59).

fournies sur le réseau et auxquelles l'accès se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates (des navigateurs internet aux appareils mobiles et aux postes de travail). Le terme "modulable" renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services de traitement de données, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Le terme "variable" est utilisé pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes "ensemble partagé" sont utilisés pour décrire les ressources informatiques qui sont mises à la disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique. Le terme "distribué" est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages. Le terme "fortement distribué" est utilisé pour décrire les services de traitement de données qui impliquent un traitement de données plus proche du lieu où les données sont générées ou collectées, par exemple dans un dispositif de traitement de données connecté. Le traitement de données à la périphérie, qui est une forme de traitement de données fortement distribué, devrait générer de nouveaux modèles d'entreprise et de fourniture de services en nuage, qui devraient être ouverts et interopérables dès le départ.

(81) Le concept générique de "services de traitement de données" couvre un nombre important de services ayant un très large éventail de finalités, de fonctionnalités et de configurations techniques différentes. Comme généralement compris par les fournisseurs et les utilisateurs et conformément aux normes largement utilisées, les services de traitement de données relèvent d'un ou de plusieurs des trois modèles de fourniture de services de traitement de données suivants: l'infrastructure à la demande (IaaS), la plateforme à la demande (PaaS) et le logiciel à la demande (SaaS). Ces modèles de fourniture de services représentent une combinaison spécifique de ressources TIC proposées par un fournisseur de services de traitement de données. Ces trois modèles de base de fourniture de services de traitement de données sont complétés par de nouvelles variantes, chacune comprenant une combinaison distincte de ressources TIC, telles que le "stockage à la demande" et la "base de données à la demande". Les services de traitement de données peuvent être classés de manière plus fine et répartis dans une liste non exhaustive d'ensembles de services de traitement de données qui partagent le même objectif principal et les mêmes fonctionnalités principales ainsi que le même type de modèles de traitement de données, qui ne sont pas liés aux caractéristiques opérationnelles du service (même type de services). Les services relevant du même type de service peuvent partager le même modèle de service de traitement de données, toutefois, deux bases de données pourraient sembler partager le même objectif principal, mais après examen de leur modèle de fourniture de traitement de données, de leur modèle de distribution et des cas d'utilisation qu'ils ciblent, ces bases de données pourraient relever d'une sous-catégorie plus fine de services similaires. Des services du même type de service peuvent présenter des caractéristiques différentes et concurrentes, telles que la performance, la sécurité, la résilience et la qualité du service.

(82) Des problèmes d'extraction des données exportables appartenant au client chez le fournisseur d'origine de services de traitement de données peuvent entraver le rétablissement des fonctionnalités du service dans l'infrastructure du fournisseur de destination de services de traitement des données. Afin de faciliter la stratégie de sortie du client, d'éviter des tâches inutiles et lourdes et de veiller à ce que le client ne perde aucune de ses données à la suite de la procédure de changement de fournisseur, le fournisseur d'origine de services de traitement de données devrait informer le client à l'avance de l'étendue des données qui peuvent être exportées une fois que ce client décide de passer à un autre service fourni par un fournisseur de services de traitement de données différent ou à une infrastructure TIC sur site. Les données exportables devraient comprendre, au minimum, les données d'entrée et de sortie, y compris les métadonnées directement ou indirectement générées ou cogénérées par l'utilisation du service de traitement de données par le client, à l'exclusion de tous les actifs ou de toutes les données du fournisseur de services de traitement de données ou d'un tiers. Les données exportables devraient exclure les actifs ou les données du fournisseur de services de traitement de données ou des tiers qui sont protégés par des droits de propriété intellectuelle ou qui constituent des secrets d'affaires de ce fournisseur ou de ce

tiers, ou les données liées à l'intégrité et à la sécurité du service, dont l'exportation exposera les fournisseurs de services de traitement de données à des vulnérabilités en matière de cybersécurité. Ces exclusions ne devraient pas entraver ou retarder le processus de changement de fournisseur.

(83) Les actifs numériques désignent les éléments en format numérique pour lesquels le client possède un droit d'utilisation, y compris les applications et métadonnées liées à la configuration des paramètres, la sécurité et la gestion des droits d'accès et de contrôle, ainsi que d'autres éléments tels que les réalisations des technologies de virtualisation, y compris les machines virtuelles et la conteneurisation. Les actifs numériques peuvent être transférés lorsque le client est titulaire du droit d'utilisation, quelle que soit la relation contractuelle avec le service de traitement de données qu'il a l'intention de quitter. Ces autres éléments sont essentiels pour une utilisation efficace des données et applications du client dans l'environnement du fournisseur de destination de services de traitement de données.

Changement de services de traitement de données

(84) Le présent règlement vise à faciliter le changement de services de traitement de données, ce qui englobe les conditions et actions qui sont nécessaires pour qu'un client résilie un contrat relatif à un service de traitement de données, conclue un ou plusieurs nouveaux contrats avec différents fournisseurs de services de traitement de données, porte ses données exportables et actifs numériques, et le cas échéant, bénéficie de l'équivalence fonctionnelle.

(85) Le changement de fournisseur est une opération orientée vers le client, qui consiste en plusieurs étapes, notamment l'extraction de données, qui correspond au téléchargement de données à partir de l'écosystème du fournisseur d'origine de services de traitement de données; la transformation, lorsque les données sont structurées d'une manière qui ne correspond pas au schéma de l'emplacement cible; et le téléversement des données dans un nouvel emplacement de destination. Dans une situation particulière décrite dans le présent règlement, le découplage d'un service donné du contrat et son transfert vers un fournisseur différent devraient également être considérés comme un changement de fournisseur. Le processus de changement de fournisseur est parfois géré pour le compte du client par une entité tierce. Par conséquent, tous les droits et obligations du client établis par le présent règlement, y compris l'obligation de coopérer de bonne foi, devraient être compris comme s'appliquant à une telle entité tierce dans ces circonstances. Les fournisseurs de services de traitement de données et les clients ont différents niveaux de responsabilités, selon les étapes du processus visé. Par exemple, le fournisseur d'origine de services de traitement de données est responsable de l'extraction des données dans un format lisible par machine, mais ce sont le client et le fournisseur de destination de services de traitement de données qui doivent téléverser les données dans le nouvel environnement, sauf en cas de recours à un service professionnel spécifique de transition. Un client qui a l'intention d'exercer des droits liés au changement de fournisseur, prévus par le présent règlement, devrait informer le fournisseur d'origine de services de traitement de données de la décision de se tourner vers un fournisseur différent de services de traitement de données, de se tourner vers une infrastructure TIC sur site ou de supprimer les actifs de ce client et d'effacer ses données exportables.

(86) Par équivalence fonctionnelle, on entend le rétablissement, sur la base des données exportables et des actifs numériques du client, d'un niveau minimal de fonctionnalité dans l'environnement d'un nouveau service de traitement de données du même type de service après le changement de fournisseur, lorsque le service de traitement des données de destination donne un résultat sensiblement comparable en réponse au même intrant pour des fonctionnalités partagées fournies au client en vertu du contrat. On peut seulement attendre des fournisseurs de services de traitement de données qu'ils facilitent l'équivalence fonctionnelle pour les fonctionnalités que les services de traitement des données, tant d'origine que de destination, offrent de manière indépendante. Le présent règlement ne constitue pas une obligation de faciliter l'équivalence fonctionnelle pour les fournisseurs de services de traitement de données autres que ceux qui proposent des services du modèle de fourniture IaaS.

(87) Les services de traitement de données sont utilisés dans tous les secteurs et proposent des complexités et types de services différents. Il s'agit d'un élément important à prendre en considération en ce qui concerne le processus de portage et les délais. Néanmoins, une prolongation de la période transitoire en raison de l'impossibilité technique de finaliser le processus de changement de fournisseur dans le délai imparti

ne devrait être invoquée que dans des cas dûment justifiés. La charge de la preuve à cet égard devrait incomber entièrement au fournisseur du service de traitement de données concerné. Cela est sans préjudice du droit exclusif du client de prolonger la période transitoire une fois pour une période que le client juge plus adaptée pour ses propres finalités. Le client peut invoquer ce droit à une prolongation avant ou pendant la période transitoire, compte tenu du fait que le contrat reste applicable pendant la période transitoire.

(88) Les frais de changement de fournisseur sont les frais imposés par les fournisseurs de services de traitement de données aux clients pour le processus de changement de fournisseur. En général, ces frais sont destinés à répercuter les coûts que le fournisseur d'origine de services de traitement de données peut encourir en raison du processus de changement de fournisseur, sur le client qui souhaite changer de fournisseur. Les frais de changement de fournisseur courants sont, par exemple, les frais liés au transfert des données d'un fournisseur de services de traitement de données à un autre ou à une infrastructure TIC sur site (les frais de transfert des données) ou les frais encourus pour des actions de soutien spécifiques pendant le processus de changement de fournisseur. Les frais de transfert des données inutilement élevés ou les frais injustifiés non liés à des coûts réels de changement de fournisseur sont un frein au changement de fournisseur pour les clients, restreignent la libre circulation des données, peuvent restreindre la concurrence et provoquent des effets de verrouillage pour les clients en réduisant les incitations à choisir un fournisseur de services différent ou supplémentaire. Les frais de changement de fournisseur devraient dès lors être supprimés après trois ans à compter de la date d'entrée en vigueur du présent règlement. Les fournisseurs de services de traitement de données devraient pouvoir imposer des frais de changement de fournisseur réduits jusqu'à cette date.

(89) Un fournisseur d'origine de services de traitement de données devrait pouvoir externaliser certaines tâches et verser une compensation à des entités tierces afin de se conformer aux obligations prévues par le présent règlement. Un client ne devrait pas supporter les coûts découlant de l'externalisation de services décidée par le fournisseur d'origine de services de traitement de données au cours du processus de changement de fournisseur et ces coûts devraient être considérés comme étant injustifiés, à moins qu'ils ne couvrent des travaux entrepris par le fournisseur de services de traitement de données à la demande du client en vue d'un soutien supplémentaire dans le cadre du processus de changement de fournisseur qui dépassent les obligations en matière de changement de fournisseur expressément prévues par le présent règlement. Aucune disposition du présent règlement n'empêche un client de verser une compensation à des entités tierces pour un soutien dans le cadre du processus de migration, ni des parties de convenir de contrats de services de traitement de données d'une durée déterminée, y compris de pénalités de résiliation anticipée proportionnées pour couvrir la résiliation anticipée de tels contrats, conformément au droit de l'Union ou au droit national. Afin d'encourager la concurrence, la suppression progressive des frais de changement de fournisseur de services de traitement de données devrait porter en particulier sur les frais de transfert des données facturés par un fournisseur de services de traitement de données à un client. En soi, les frais de service standard afférents à la fourniture des services de traitement de données ne constituent pas des frais de changement de fournisseur. Ces frais de service standard ne sont pas susceptibles d'être supprimés et restent applicables jusqu'à ce que le contrat de fourniture des services concernés cesse de s'appliquer. Le présent règlement permet au client de demander la fourniture de services supplémentaires allant au-delà des obligations du fournisseur en matière de changement de fournisseur au titre du présent règlement. Ces services supplémentaires peuvent être fournis et facturés par le fournisseur lorsqu'ils sont fournis à la demande du client et que celui-ci marque à l'avance son accord sur le prix desdits services.

(90) Il est nécessaire d'adopter, en matière d'interopérabilité, une approche réglementaire ambitieuse et propice à l'innovation afin de remédier aux effets de verrouillage, qui nuisent à la concurrence et au développement de nouveaux services. L'interopérabilité des services de traitement de données requiert de multiples interfaces, couches d'infrastructures et couches de logiciels, et se limite rarement à un test binaire visant à en évaluer la faisabilité ou l'impossibilité. Par contre, la mise en œuvre d'une telle interopérabilité est soumise à une analyse coûts/avantages, nécessaire pour déterminer s'il est utile de chercher à obtenir des résultats raisonnablement prévisibles. La norme ISO/CEI 19941:2017 est une norme internationale importante qui constitue une réfé-

rence pour la réalisation des objectifs du présent règlement, car elle contient des considérations techniques clarifiant la complexité d'un tel processus.

(91) Lorsque les fournisseurs de services de traitement de données sont à leur tour clients de services de traitement de données fournis par un prestataire tiers, ils bénéficieront eux-mêmes d'un changement de fournisseur plus efficace, tout en restant liés par les obligations du présent règlement en ce qui concerne leurs propres offres de services.

(92) Les fournisseurs de services de traitement de données devraient être tenus, dans les limites de leurs capacités et proportionnellement à leurs obligations respectives, d'offrir toute l'assistance et le soutien nécessaires pour que le processus de changement de fournisseur de services de traitement de données soit fructueux, efficace et sûr. Le présent règlement n'impose pas aux fournisseurs de services de traitement de données de développer de nouvelles catégories de services de traitement de données, y compris au sein ou sur la base de l'infrastructure TIC de fournisseurs de services de traitement de données différents afin de garantir une équivalence fonctionnelle dans un environnement autre que leurs propres systèmes. Un fournisseur d'origine de services de traitement de données n'a pas accès à l'environnement du fournisseur de destination de services de traitement de données ou n'a pas d'informations sur celui-ci. L'équivalence fonctionnelle ne devrait pas être interprétée comme obligeant le fournisseur d'origine de services de traitement de données à reconstruire le service en question au sein de l'infrastructure du fournisseur de destination de services de traitement de données. Le fournisseur de services de traitement de données d'origine devrait, en revanche, prendre toutes les mesures raisonnables en son pouvoir pour faciliter le processus de réalisation de l'équivalence fonctionnelle en fournissant des capacités, des informations, une documentation, une assistance technique adéquates et, le cas échéant, les outils nécessaires.

(93) Les fournisseurs de services de traitement de données devraient également être tenus de supprimer les obstacles existants et de ne pas en imposer de nouveaux, y compris pour les clients souhaitant passer à une infrastructure TIC sur site. Les obstacles peuvent être notamment de nature précommerciale, commerciale, technique, contractuelle ou organisationnelle. Les fournisseurs de services de traitement de données devraient également être tenus de supprimer les obstacles empêchant de découpler un service individuel spécifique d'autres services de traitement de données fournis dans le cadre d'un contrat et de faire en sorte que le service concerné puisse faire l'objet d'un changement de fournisseur, en l'absence d'obstacles techniques majeurs et avérés empêchant un tel découplage.

(94) Tout au long du processus de changement de fournisseur, un niveau élevé de sécurité devrait être maintenu. Cela signifie que le fournisseur d'origine de services de traitement de données devrait étendre le niveau de sécurité auquel il s'est engagé pour le service à toutes les modalités techniques dont ce fournisseur est responsable au cours du processus de changement de fournisseur, telles que les connexions réseau ou les dispositifs matériels. Cela ne devrait pas porter atteinte aux droits existants en matière de résiliation des contrats, y compris ceux introduits par le règlement (UE) 2016/679 et la directive (UE) 2019/770 du Parlement européen et du Conseil[31]. Le présent règlement ne devrait pas être interprété comme empêchant un fournisseur de services de traitement de données de fournir aux clients des services nouveaux ou meilleurs ou des caractéristiques et des fonctionnalités nouvelles ou meilleures, ou de concurrencer d'autres fournisseurs de services de traitement de données sur cette base.

cf. RGPD

(95) Les informations que les fournisseurs de services de traitement de données doivent donner aux clients pourraient appuyer la stratégie de sortie des clients. Ces informations devraient comprendre les procédures à suivre pour entamer le changement de services de traitement de données; les formats de données lisibles par machine vers lesquels les données de l'utilisateur peuvent être exportées; les outils destinés à exporter les données, dont des interfaces ouvertes, ainsi que les informations sur la compatibilité avec les normes harmonisées ou les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes; des informations sur les restrictions

31. Directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques (JO L 136 du 22.5.2019, p. 1).

et les limites techniques connues qui pourraient influer sur le processus de changement de fournisseur; et le temps considéré comme nécessaire pour achever ledit processus de changement.

(96) Afin de faciliter l'interopérabilité et le changement de services de traitement de données, les utilisateurs et les fournisseurs de services de traitement de données devraient envisager l'utilisation d'outils de mise en œuvre et de contrôle de la conformité, en particulier ceux publiés par la Commission sous la forme d'un recueil de règles de l'Union européenne sur l'informatique en nuage et d'un guide sur les marchés publics pour les services de traitement des données. Les clauses contractuelles standard, en particulier, sont avantageuses car elles contribuent à accroître la confiance dans les services de traitement de données, à créer une relation plus équilibrée entre les utilisateurs et les fournisseurs de services de traitement de données et à améliorer la sécurité juridique quant aux conditions applicables au passage à d'autres services de traitement de données. Dans ce contexte, les utilisateurs et les fournisseurs de services de traitement de données devraient envisager l'utilisation de clauses contractuelles standard ou d'autres outils de contrôle de la conformité par autorégulation, à condition qu'ils soient en totale conformité avec le présent règlement, élaborés par des organes ou groupes d'experts compétents établis en vertu du droit de l'Union.

(97) Afin de faciliter le changement de services de traitement de données, toutes les parties concernées, y compris les fournisseurs d'origine et de destination de services de traitement de données, devraient coopérer de bonne foi en vue de rendre efficace le processus de changement de fournisseur, et de permettre un transfert sécurisé et en temps utile des données nécessaires dans un format couramment utilisé, lisible par machine, et au moyen d'interfaces ouvertes, tout en évitant les perturbations du service et en assurant la continuité des services.

(98) Les services de traitement de données qui portent sur des services dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux demandes spécifiques d'un client donné ou dont tous les composants ont été développés pour les besoins d'un client particulier devraient être exemptés de certaines des obligations applicables au changement de services de traitement de données. Ceci ne devrait pas concerner les services que le fournisseur de services de traitement de données propose sur une large échelle commerciale par l'intermédiaire de son catalogue de services. Le fournisseur de services de traitement de données a notamment l'obligation d'informer dûment les clients potentiels de ces services, avant la conclusion d'un éventuel contrat, des obligations prévues par le présent règlement qui ne s'appliquent pas aux services concernés. Rien n'empêche le fournisseur de services de traitement de données de déployer à terme ces services à grande échelle, auquel cas ce fournisseur devrait se conformer à toutes les obligations en matière de changement de fournisseur prévues par le présent règlement.

(99) Conformément à l'exigence minimale permettant le changement de fournisseur de services de traitement de données, le présent règlement vise également à améliorer l'interopérabilité pour l'utilisation simultanée de services de traitement de données multiples dotés de fonctionnalités complémentaires. Sont visées les situations dans lesquelles les clients ne résilient pas un contrat pour changer de fournisseur de services de traitement de données, mais utilisent simultanément plusieurs services de différents fournisseurs, de manière interopérable, afin de bénéficier des fonctionnalités complémentaires des différents services dans la mise en place du système du client. Toutefois, il est admis que le processus de sortie des données d'un fournisseur de services de traitement de données vers un autre dans le but de faciliter l'utilisation simultanée de services peut constituer une activité continue, contrairement à la sortie ponctuelle requise dans le cadre du processus de changement de fournisseur. Les fournisseurs de services de traitement de données devraient, par conséquent, continuer à pouvoir imposer des frais de transfert des données, ne dépassant pas les coûts encourus, aux fins de l'utilisation simultanée après trois ans à compter de la date d'entrée en vigueur du présent règlement. Cette possibilité est importante, entre autres, pour assurer le succès du déploiement de stratégies multinuages qui permettent aux clients de mettre en œuvre des stratégies TIC à l'épreuve du temps et réduisent la dépendance à l'égard de fournisseurs particuliers de services de traitement de données. Faciliter une approche multinuage pour les clients des services de traitement de données peut également contribuer à accroître leur résilience opérationnelle numérique, ainsi que le prévoit, pour les insti-

tutions de services financiers, le règlement (UE) 2022/2554 du Parlement européen et du Conseil[32].

(100) Les spécifications et les normes d'interopérabilité ouvertes élaborées conformément à l'annexe II du règlement (UE) no 1025/2012 du Parlement européen et du Conseil[33] dans le domaine de l'interopérabilité et de la portabilité devraient permettre un environnement en nuage multifournisseur, qui est une exigence essentielle pour l'innovation ouverte dans l'économie européenne fondée sur les données. Étant donné que l'adoption par le marché des normes recensées dans le cadre de l'initiative de coordination de la normalisation de l'informatique en nuage (CSC), décidée en 2016, a été limitée, il est également nécessaire que la Commission s'appuie sur les acteurs du marché pour élaborer des spécifications d'interopérabilité ouvertes pertinentes afin de suivre le rythme rapide de l'évolution technologique dans ce secteur. Ces spécifications d'interopérabilité ouvertes peuvent ensuite être adoptées par la Commission sous la forme de spécifications communes. En outre, lorsque les processus axés sur le marché n'ont pas démontré une capacité d'établir des spécifications ou des normes communes qui facilitent une interopérabilité effective en nuage au niveau des PaaS et des SaaS, la Commission devrait pouvoir, sur la base du présent règlement et conformément au règlement (UE) no 1025/2012, demander aux organismes européens de normalisation de définir de telles normes pour des types de services spécifiques pour lesquels ces normes n'existent pas encore. La Commission encouragera en outre les acteurs du marché à élaborer des spécifications d'interopérabilité ouvertes pertinentes. Après avoir consulté les parties prenantes, la Commission devrait pouvoir, par voie d'actes d'exécution, rendre obligatoire l'utilisation de normes harmonisées d'interopérabilité ou de spécifications communes pour des types de services spécifiques par une référence dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données. Les fournisseurs de services de traitement de données devraient garantir la compatibilité avec ces normes harmonisées et spécifications communes fondées sur des spécifications d'interopérabilité ouvertes, qui ne devraient pas porter atteinte à la sécurité ou à l'intégrité des données. Les normes harmonisées pour l'interopérabilité des services de traitement de données et les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes ne seront référencées que si elles respectent les critères spécifiés dans le présent règlement, qui ont la même signification que les exigences énoncées à l'annexe II du règlement (UE) no 1025/2012 et les facettes d'interopérabilité définies dans la norme internationale ISO/CEI 19941:2017. En outre, la normalisation devrait tenir compte des besoins des PME.

(101) Les pays tiers peuvent adopter des lois, des règlements et d'autres actes législatifs visant à obtenir un transfert direct de données à caractère non personnel situées à l'extérieur de leurs frontières, y compris dans l'Union, ou à donner à leurs pouvoirs publics un accès direct à ces données. Les décisions de juridictions ou d'autres autorités judiciaires ou administratives, y compris des autorités répressives, de pays tiers qui exigent un tel transfert ou accès concernant des données à caractère non personnel devraient être exécutoires lorsqu'elles sont fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. Dans d'autres cas, il peut arriver qu'une demande de transfert de données à caractère non personnel ou d'accès à de telles données fondée sur le droit d'un pays tiers soit incompatible avec l'obligation de protéger ces données au titre du droit de l'Union ou au titre du droit national de l'État membre concerné, en particulier en ce qui concerne la protection des droits fondamentaux de la personne, tels que le droit à la sécurité et le droit à un recours effectif, ou les intérêts fondamentaux d'un État membre en matière de sécurité nationale ou de défense, ainsi que des données commercialement sensibles, notamment des secrets d'affaires, ou des droits de propriété intellectuelle, y compris les engagements contractuels en matière de confidentialité conformément à ce droit. En l'absence d'accords internationaux régissant ces questions, il convient de n'autoriser le transfert de données à caractère non personnel ou

32. Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 (JO L 333 du 27.12.2022, p. 1).

33. Règlement (UE) no 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision no 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

l'accès aux données à caractère non personnel que s'il a été vérifié qu'en vertu du système juridique du pays tiers, les motifs et la proportionnalité de la décision doivent être exposés, la décision judiciaire ou administrative doit avoir un caractère spécifique, et l'objection motivée du destinataire doit faire l'objet d'un contrôle par une juridiction compétente du pays tiers habilitée à tenir dûment compte des intérêts juridiques pertinents du fournisseur des données. Chaque fois que cela est possible selon les termes de la demande d'accès aux données de l'autorité du pays tiers, le fournisseur de services de traitement de données devrait être en mesure d'informer le client dont les données sont demandées, avant d'accorder un accès à ces données, afin de vérifier l'existence d'un conflit potentiel entre cet accès et des dispositions du droit de l'Union ou du droit national, telles que celles relatives à la protection des données commercialement sensibles, y compris la protection des secrets d'affaires et des droits de propriété intellectuelle et les engagements contractuels en ce qui concerne la confidentialité.

(102) Afin de renforcer encore la confiance placée dans les données, il importe de mettre en œuvre, dans toute la mesure du possible, des garanties pour assurer le contrôle de données qui les concernent par les citoyens, le secteur public et les entreprises de l'Union. En outre, le droit, les valeurs et les normes de l'Union en ce qui concerne, entre autres, la sécurité, la protection des données et le respect de la vie privée, ainsi que la protection des consommateurs devraient être respectés. Afin de prévenir tout accès illicite des pouvoirs publics de pays tiers aux données à caractère non personnel, les fournisseurs de service de traitement de données soumis au présent règlement, tels que les services d'informatique en nuage et en périphérie, devraient prendre toute mesure raisonnable pour empêcher l'accès aux systèmes dans lesquels sont stockées des données à caractère non personnel, y compris, s'il y a lieu, par le chiffrement des données, la sujétion régulière à des audits, le respect vérifié de dispositifs de certification pertinents en matière de réassurance de sécurité et par une modification de leurs politiques d'entreprise.

(103) La normalisation et l'interopérabilité sémantique devraient jouer un rôle essentiel dans l'apport de solutions techniques permettant de garantir l'interopérabilité au sein d'espaces européens communs de données et entre ces espaces, qui sont des cadres interopérables de normes et de pratiques communes spécifiques à chaque finalité ou à chaque secteur ou transsectoriels visant à partager ou à traiter conjointement des données aux fins, entre autres, de la mise au point de nouveaux produits et services, de la recherche scientifique ou d'initiatives de la société civile. Le présent règlement fixe certaines exigences essentielles en matière d'interopérabilité. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants, qui sont des entités facilitant le partage de données au sein d'espaces européens communs de données, y compris les détenteurs de données, ou participant à ce partage, devraient respecter ces exigences pour ce qui est des éléments sous leur contrôle. Le respect de ces règles peut être assuré en adhérant aux exigences essentielles établies dans le présent règlement, ou peut être présumé en respectant des normes harmonisées ou des spécifications communes au moyen d'une présomption de conformité. Afin de faciliter la conformité avec les exigences en matière d'interopérabilité, il est nécessaire de prévoir une présomption de conformité des solutions d'interopérabilité qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) no 1025/2012, qui constitue le cadre par défaut pour l'élaboration de normes qui prévoient une telle présomption. La Commission devrait évaluer les obstacles à l'interopérabilité et donner la priorité aux besoins en matière de normalisation, sur la base desquels elle peut demander à une ou plusieurs organisations européennes de normalisation, en vertu du règlement (UE) no 1025/2012, d'élaborer des normes harmonisées qui satisfont aux exigences essentielles établies dans le présent règlement. Lorsque de telles demandes ne débouchent pas sur des normes harmonisées ou que ces normes harmonisées sont insuffisantes pour garantir le respect des exigences essentielles prévues par le présent règlement, la Commission devrait pouvoir adopter des spécifications communes dans ces domaines, à condition que, ce faisant, elle respecte dûment le rôle et les fonctions des organismes de normalisation. Des spécifications communes ne devraient être adoptées qu'à titre de solution de repli exceptionnelle en vue de faciliter le respect des exigences essentielles prévues par le présent règlement, ou lorsque le processus de normalisation est bloqué, ou lorsque l'établissement de normes harmonisées appropriées accuse du retard. Si un tel retard est dû à la complexité technique de la norme en question, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Des spécifications communes devraient être élaborées selon des modalités ouvertes et inclusives

et tenir compte, le cas échéant, des conseils formulés par le comité européen de l'innovation dans le domaine des données instauré par le règlement (UE) 2022/868. En outre, des spécifications communes dans différents secteurs pourraient être adoptées, conformément au droit de l'Union ou au droit national, en fonction des besoins spécifiques des secteurs concernés. La Commission devrait par ailleurs être habilitée à demander l'élaboration de normes harmonisées pour l'interopérabilité des services de traitement de données.

Contrats intelligents

(104) Afin de promouvoir l'interopérabilité des outils d'exécution automatique des accords de partage de données, il est nécessaire de définir les exigences essentielles des contrats intelligents que les professionnels créent pour d'autres ou intègrent dans des applications soutenant la mise en œuvre d'accords de partage de données. Afin de faciliter la conformité de ces contrats intelligents avec ces exigences essentielles, il est nécessaire de prévoir une présomption de conformité des contrats intelligents qui satisfont à des normes harmonisées ou à des parties de celles-ci conformément au règlement (UE) no 1025/2012. La notion de "contrat intelligent" figurant dans le présent règlement est technologiquement neutre. Les contrats intelligents peuvent, par exemple, être connectés à un registre électronique. Les exigences essentielles ne devraient s'appliquer qu'aux vendeurs de contrats intelligents, sauf lorsque ces derniers élaborent des contrats intelligents en interne à des fins exclusivement internes. L'exigence essentielle de faire en sorte que les contrats intelligents puissent être interrompus et résiliés implique le consentement mutuel des parties à l'accord de partage de données. L'utilisation de contrats intelligents pour l'exécution automatique de ces accords reste ou devrait rester sans incidence sur l'applicabilité des règles pertinentes du droit civil, du droit contractuel et du droit de la protection des consommateurs à de tels accords de partage de données.

(105) Afin de démontrer le respect des exigences essentielles du présent règlement, le vendeur d'un contrat intelligent ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie de celui-ci, pour mettre des données à disposition dans le cadre du présent règlement, devrait procéder à une évaluation de la conformité et délivrer une déclaration UE de conformité. Une telle évaluation de la conformité devrait être soumise aux principes généraux établis dans le règlement (CE) no 765/2008 du Parlement européen et du Conseil[34] et dans la décision (CE) no 768/2008 du Parlement européen et du Conseil[35].

(106) Outre l'obligation faite aux développeurs professionnels de contrats intelligents de respecter les exigences essentielles, il est également important d'encourager les participants aux espaces de données qui proposent des données ou des services fondés sur les données à d'autres participants au sein d'espaces européens communs des données et entre ces espaces à soutenir l'interopérabilité des outils de partage de données, y compris les contrats intelligents.

Autorités compétentes pour l'application du règlement sur les données

(107) Afin de garantir l'application et l'exécution efficace du présent règlement, les États membres devraient désigner une ou plusieurs autorités compétentes. Si un État membre désigne plusieurs autorités compétentes, il devrait également désigner parmi celles-ci un coordinateur de données. Les autorités compétentes devraient coopérer entre elles. Dans le cadre de l'exercice de leurs pouvoirs d'enquête conformément aux procédures nationales applicables, les autorités compétentes devraient pouvoir rechercher et obtenir des informations, en particulier en ce qui concerne les activités des entités relevant de leur compétence et, y compris dans le cadre d'enquêtes conjointes, en tenant dûment compte du fait que les mesures de surveillance et d'exécution concernant une entité relevant de la compétence d'un autre État membre devraient être adoptées par l'autorité compétente de cet autre État membre, le cas échéant, conformément aux procédures relatives à la coopération transfrontière. Les autorités compétentes devraient se prêter mutuellement assistance en temps utile, en particulier lorsqu'une autorité compétente d'un État membre détient des informations utiles aux fins d'une enquête menée par les autorités compétentes d'autres États membres, ou est en mesure

34. Règlement (CE) no 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) no 339/93 (JO L 218 du 13.8.2008, p. 30).

35. Décision no 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

de recueillir de telles informations auxquelles les autorités compétentes de l'État membre dans lequel l'entité est établie n'ont pas accès. Les autorités compétentes et les coordinateurs de données devraient être identifiés dans un registre public tenu par la Commission. Le coordinateur de données pourrait constituer un moyen supplémentaire de faciliter la coopération dans les situations transfrontières, notamment lorsqu'une autorité compétente d'un État membre donné ne sait pas à quelle autorité s'adresser dans l'État membre du coordinateur de données, par exemple lorsque le cas concerne plusieurs autorités compétentes ou secteurs. Le coordinateur de données devrait, entre autres, faire office de point de contact unique pour toutes les questions liées à l'application du présent règlement. Lorsqu'aucun coordinateur de données n'a été désigné, l'autorité compétente devrait assumer les tâches qui sont assignées à ce dernier en vertu du présent règlement. Les autorités chargées de contrôler le respect du droit en matière de protection des données et les autorités compétentes désignées en vertu du droit de l'Union ou du droit national devraient être responsables de l'application du présent règlement dans leurs domaines de compétence. Afin d'éviter des conflits d'intérêts, les autorités compétentes responsables de l'application et de l'exécution du présent règlement pour ce qui est de la mise à disposition de données à la suite d'une demande fondée sur un besoin exceptionnel ne devraient pas bénéficier du droit de présenter une telle demande.

Répartition des infractions

(108) Pour faire valoir leurs droits au titre du présent règlement, les personnes physiques et morales devraient pouvoir demander réparation pour des infractions à ces droits en introduisant une réclamation. Le coordinateur de données devrait, sur demande, fournir aux personnes physiques et morales toutes les informations nécessaires pour introduire leurs réclamations auprès de l'autorité compétente concernée. Les autorités compétentes devraient être tenues de coopérer afin de garantir que la réclamation est gérée et traitée de manière appropriée, efficace et rapide. Afin de recourir au mécanisme du réseau de coopération en matière de protection des consommateurs et de permettre des actions représentatives, le présent règlement modifie les annexes du règlement (UE) 2017/2394 du Parlement européen et du Conseil[36] et de la directive (UE) 2020/1828 du Parlement européen et du Conseil[37].

Sanctions

(109) Les autorités compétentes devraient veiller à ce que les infractions aux obligations prévues par le présent règlement fassent l'objet de sanctions. Ces sanctions pourraient revêtir la forme, entre autres, de sanctions pécuniaires, d'avertissements, de blâmes ou d'injonctions de mettre des pratiques commerciales en conformité avec les obligations instaurées par le présent règlement. Les sanctions définies par les États membres devraient être effectives, proportionnées et dissuasives et tenir compte des recommandations du comité européen de l'innovation dans le domaine des données, contribuant ainsi à atteindre le plus haut niveau possible de cohérence dans l'instauration et l'application des sanctions. Le cas échéant, les autorités compétentes devraient recourir à des mesures provisoires pour limiter les effets d'une infraction présumée tant que l'enquête sur cette infraction est en cours. Ce faisant, elles devraient tenir compte, entre autres, de la nature, de la gravité, de l'ampleur et de la durée de l'infraction au regard de l'intérêt public en jeu, de la portée et du type d'activités exercées, ainsi que de la capacité économique de l'auteur de l'infraction. Si l'auteur de l'infraction manque systématiquement ou de façon récurrente aux obligations qui lui incombent au titre du présent règlement, elles devraient également en tenir compte. Afin de garantir le respect du principe ne bis in idem, et d'éviter en particulier que la même infraction aux obligations prévues par le présent règlement ne soit sanctionnée plus d'une fois, un État membre qui entend exercer sa compétence à l'égard de l'auteur d'une infraction qui n'est pas établi dans l'Union et n'a pas désigné de représentant légal dans l'Union devrait, sans retard injustifié, en informer tous les coordinateurs de données ainsi que la Commission.

(110) Le comité européen de l'innovation dans le domaine des données devrait conseiller et assister la Commission dans la coordination des pratiques et politiques nationales sur les sujets couverts par le présent règlement ainsi que dans la réalisation

36. Règlement (UE) 2017/2394 du Parlement européen et du Conseil du 12 décembre 2017 sur la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et abrogeant le règlement (CE) no 2006/2004 (JO L 345 du 27.12.2017, p. 1).
37. Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

de ses objectifs en matière de normalisation technique en vue de renforcer l'interopérabilité. Le comité devrait également jouer un rôle essentiel pour faciliter des discussions approfondies entre autorités compétentes concernant l'application et l'exécution du présent règlement. Cet échange d'informations vise à améliorer l'accès effectif à la justice ainsi que la coopération en matière répressive et judiciaire dans l'ensemble de l'Union. Entre autres fonctions, les autorités compétentes devraient faire appel au comité européen de l'innovation dans le domaine des données en tant que plateforme pour évaluer, coordonner et adopter des recommandations sur la détermination de sanctions en cas d'infractions au présent règlement. Le comité devrait permettre aux autorités compétentes, avec l'aide de la Commission, de coordonner l'approche optimale pour déterminer et imposer de telles sanctions. Cette approche permet d'éviter la fragmentation tout en laissant une souplesse aux États membres et devrait déboucher sur des recommandations efficaces qui favorisent l'application cohérente du présent règlement. Le comité européen de l'innovation dans le domaine des données devrait également jouer un rôle consultatif dans les processus de normalisation et l'adoption des spécifications communes par voie d'actes d'exécution, dans l'adoption des actes délégués visant à établir un mécanisme de suivi des frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données et à préciser davantage les exigences essentielles pour l'interopérabilité des données, des mécanismes et des services de partage des données, ainsi que pour l'interopérabilité des espaces européens communs des données. Il devrait également conseiller et assister la Commission dans l'adoption des lignes directrices fixant des spécifications d'interopérabilité pour le fonctionnement des espaces européens communs des données.

Clauses contractuelles types

(111) Afin d'aider les entreprises à rédiger et à négocier des contrats, la Commission devrait élaborer et recommander des clauses contractuelles types non contraignantes pour les contrats de partage de données entre entreprises, en tenant compte, si nécessaire, des conditions prévalant dans certains secteurs et des pratiques existantes en matière de mécanismes de partage volontaire de données. Ces clauses contractuelles types devraient avant tout constituer un outil pratique aidant en particulier les PME à conclure un contrat. Lorsqu'elles seront largement et intégralement utilisées, ces clauses contractuelles types devraient également avoir pour effet bénéfique d'influencer la manière dont sont conçus les contrats en ce qui concerne l'accès aux données et à l'utilisation des données et conduire ainsi plus généralement à des relations contractuelles plus équitables en matière d'accès aux données et de partage des données.

(112) Afin d'éliminer le risque que les détenteurs de données contenues dans des bases de données obtenues ou générées au moyen de composants physiques, tels que des capteurs, d'un produit connecté ou d'un service connexe, ou d'autres types de données générées par des machines, invoquent le droit sui generis prévu par l'article 7 de la directive 96/9/CE, et puissent entraver ainsi, en particulier, l'exercice effectif du droit des utilisateurs d'avoir accès aux données et d' utiliser les données ainsi que du droit de partager des données avec des tiers prévus par le présent règlement, il y a lieu de préciser que le droit sui generis ne s'applique pas à ces bases de données. Cela ne porte pas atteinte à la potentielle application du droit sui generis prévu par l'article 7 de la directive 96/9/CE aux bases de données contenant des données ne relevant pas du champ d'application du présent règlement, à condition que les conditions de la protection en application du paragraphe 1 dudit article soient remplies.

Actes délégués

(113) Afin de tenir compte des aspects techniques des services de traitement de données, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en vue de compléter le présent règlement dans le but de créer un mécanisme de suivi des frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données sur le marché, et de préciser davantage les exigences essentielles en matière d'interopérabilité imposées aux participants aux espaces de données qui proposent des données ou des services de données aux autres participants. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016"Mieux légiférer"[38]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont

suivi des frais changement de fournisseur

exigences d’intéropérabilité

38. JO L 123 du 12.5.2016, p. 1.

systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(114) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne l'adoption de spécifications communes pour assurer l'interopérabilité des données, des mécanismes et des services de partage des données ainsi que des espaces européens communs de données, de spécifications communes concernant l'interopérabilité des services de traitement de données, et de spécifications communes concernant l'interopérabilité des contrats intelligents. Il convient aussi de conférer des compétences d'exécution à la Commission aux fins de publier les références des normes harmonisées et des spécifications communes pour l'interopérabilité des services de traitement de données dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données. Ces compétences devraient être exercées conformément au règlement (UE) no 182/2011 du Parlement européen et du Conseil[39].

(115) Le présent règlement devrait s'entendre sans préjudice des règles répondant à des besoins spécifiques à certains secteurs ou domaines d'intérêt public. Ces règles peuvent comprendre des exigences supplémentaires concernant les aspects techniques de l'accès aux données, tels que les interfaces d'accès aux données, ou la manière dont l'accès aux données pourrait être fourni, par exemple directement à partir du produit ou par l'intermédiaire de services d'intermédiation de données. Ces règles peuvent également inclure des limites aux droits des détenteurs de données d'accéder aux données des utilisateurs ou de les utiliser, ou d'autres aspects allant au-delà de l'accès aux données et de l'utilisation des données, tels que les aspects liés à la gouvernance ou des exigences en matière de sécurité, y compris de cybersécurité. Le présent règlement devrait également s'entendre sans préjudice de règles plus spécifiques dans le cadre du développement d'espaces européens communs de données ou, sous réserve des exceptions prévues par le présent règlement, sans préjudice du droit de l'Union et du droit national prévoyant l'accès aux données, et autorisant l'utilisation des données, à des fins de recherche scientifique.

(116) Le présent règlement ne devrait pas avoir d'incidence sur l'application des règles relatives à la concurrence, en particulier les articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Les mesures prévues par le présent règlement ne devraient pas être utilisées pour restreindre la concurrence d'une manière qui soit contraire au traité sur le fonctionnement de l'Union européenne.

(117) Afin de permettre aux acteurs relevant du champ d'application du présent règlement de s'adapter aux nouvelles règles prévues par celui-ci et de mettre en place les aménagements techniques nécessaires, ces règles devraient s'appliquer à partir du 12 septembre 2025.

(118) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis le 4 mai 2022.

Le CEPD/EDPS et le CEPD/EDPB ont été consultés

(119) Étant donné que les objectifs du présent règlement, à savoir garantir l'équité dans l'attribution de valeur issue de données parmi les acteurs de l'économie fondée sur les données et favoriser un accès équitable aux données et une utilisation équitable des données afin de contribuer à la création d'un véritable marché intérieur des données, ne peuvent être atteints de manière suffisante par les États membres mais peuvent, en raison des dimensions ou des effets de l'action et de l'utilisation transfrontière des données, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

39. Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

CHAPITRE I
DISPOSITIONS GENERALES

Article premier
Objet et champ d'application

Objectifs

1. Le présent règlement établit des règles harmonisées, entre autres, sur:

a) la mise à disposition de données relatives au produit et de données relatives au service connexe au profit de l'utilisateur du produit connecté ou du service connexe;

b) la mise à disposition de données par les détenteurs de données au profit des destinataires de données;

c) la mise à disposition de données par les détenteurs de données au profit d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union, lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public;

d) la facilitation du changement de de service de traitement de données;

e) l'introduction de garanties contre l'accès illicite de tiers à des données à caractère non personnel; et

f) le développement de normes d'interopérabilité pour les données auxquelles il doit être accédé, qui doivent être transférées et qui doivent être utilisées.

Périmètre concerné

2. Le présent règlement couvre les données à caractère personnel et non personnel, y compris les types de données ci-après, dans les contextes suivants:

Données

a) le chapitre II s'applique aux données, à l'exception du contenu, relatives à la performance, à l'utilisation et à l'environnement des produits connectés et des services connexes;

Secteur privé, obligation de partage

b) le chapitre III s'applique aux données du secteur privé qui sont soumises à des obligations légales de partage des données;

Accès aux données sur la base d’un contrat

c) le chapitre IV s'applique aux données du secteur privé auxquelles il est accédé et qui sont utilisées sur la base d'un contrat entre entreprises;

Données non personnelles

d) le chapitre V s'applique aux données du secteur privé, en particulier les données à caractère non personnel;

Fournisseurs de services de traitement de données

e) le chapitre VI s'applique aux données et aux services traités par des fournisseurs de services de traitement de données;

Données non personnelles détenues par des fournisseurs de services de traitement de données

f) le chapitre VII s'applique aux données à caractère non personnel détenues dans l'Union par des fournisseurs de services de traitement de données.

Entités concernées

3. Le présent règlement s'applique:

Fabricants

a) aux fabricants de produits connectés mis sur le marché de l'Union et aux fournisseurs de services connexes, quel que soit le lieu d'établissement de ces fabricants et fournisseurs;

Utilisateurs

b) aux utilisateurs dans l'Union de produits connectés ou de services connexes tels qu'ils sont visés au point a);

Détenteurs de données

c) aux détenteurs de données, quel que soit leur lieu d'établissement, qui mettent des données à la disposition de destinataires de données dans l'Union;

Destinataires de données

d) aux destinataires de données dans l'Union au profit desquels des données sont mises à disposition;

e) aux organismes du secteur public, à la Commission, à la Banque centrale européenne et aux organes de l'Union qui demandent aux détenteurs de données de mettre des données à disposition lorsqu'il existe un besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public, ainsi qu'aux détenteurs de données qui fournissent ces données en réponse à une telle demande;

Secteur public

f) aux fournisseurs de services de traitement de données, quel que soit leur lieu d'établissement, fournissant de tels services à des clients dans l'Union;

Fournisseurs de services de traitement

g) aux participants à des espaces de données et aux vendeurs d'applications utilisant des contrats intelligents et aux personnes dont l'activité commerciale, l'entreprise ou la profession implique le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord.

Partenaires de contrats intelligents

4. Lorsque le présent règlement fait référence à des produits connectés ou à des services connexes, ces références s'entendent également comme incluant également les assistants virtuels, dans la mesure où ceux-ci interagissent avec un produit connecté ou un service connexe.

5. Le présent règlement est sans préjudice du droit de l'Union et du droit national en matière de protection des données à caractère personnel, de la vie privée et de la confidentialité des communications et de l'intégrité des équipements terminaux, qui s'appliquent aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement, en particulier des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive 2002/58/CE, y compris des pouvoirs et des compétences des autorités de contrôle et des droits des personnes concernées. Dans la mesure où les utilisateurs sont les personnes concernées, les droits fixés au chapitre II du présent règlement complètent les droits d'accès par les personnes concernées et les droits à la portabilité des données prévus aux articles 15 et 20 du règlement (UE) 2016/679. En cas de conflit entre le présent règlement et le droit de l'Union en matière de protection des données à caractère personnel ou de vie privée, ou la législation nationale adoptée conformément audit droit de l'Union, les dispositions pertinentes du droit de l'Union ou du droit national en matière de protection des données à caractère personnel ou de vie privée prévalent.

cf. RGPD

6. Le présent règlement ne s'applique pas aux accords volontaires d'échange de données entre entités privées et publiques, en particulier aux accords volontaires de partage de données, ni ne les remplace.

cf. RGPD

Le présent règlement n'affecte pas les actes juridiques de l'Union ou nationaux prévoyant l'accès aux données, le partage et l'utilisation de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, ou à des fins douanières et fiscales, en particulier les règlements (UE) 2021/784, (UE) 2022/2065 et (UE) 2023/1543 et la directive (UE) 2023/1544, ou sur la coopération internationale dans ce domaine. Le présent règlement ne s'applique pas à la collecte ou au partage de données, ni à l'accès aux données ou à l'utilisation de données au titre du règlement (UE) 2015/847 et de la directive (UE) 2015/849. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en matière de sécurité publique, de défense ou de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches en rapport avec ces compétences, ou leur pouvoir de préserver d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public. Le présent règlement ne porte pas atteinte aux compétences des États membres en matière de douanes et d'administration fiscale, ou de santé et de sécurité des citoyens.

Respect des textes antérieurs

cf. DSA

7. Le présent règlement complète l'approche d'autorégulation suivie par le règlement (UE) 2018/1807 en ajoutant des obligations d'application générale en matière de changement de fournisseur de services d'informatique en nuage.

8. Le présent règlement est sans préjudice des actes juridiques de l'Union et nationaux prévoyant la protection des droits de propriété intellectuelle, notamment les directives 2001/29/CE, 2004/48/CE et (UE) 2019/790.

9. Le présent règlement complète le droit de l'Union qui vise à promouvoir les intérêts des consommateurs et à assurer un niveau élevé de protection des consommateurs, et à protéger leur santé, leur sécurité et leurs intérêts économiques, en particulier les directives 93/13/CEE, 2005/29/CE et 2011/83/UE, et il est sans préjudice dudit droit de l'Union.

10. Le présent règlement ne fait pas obstacle à la conclusion de contrats portant sur le partage volontaire et licite de données, y compris de contrats conclus sur une base réciproque, qui respectent les exigences fixées par le présent règlement.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

1) "données": toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels;

2) "métadonnées": une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données;

3) "données à caractère personnel": les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD

4) "données à caractère non personnel": les données autres que les données à caractère personnel;

5) "produit connecté": un objet qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données relatives au produit par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré et dont la fonction première n'est pas de stocker, de traiter ou de transmettre des données pour le compte de toute partie autre que l'utilisateur;

6) "service connexe": un service numérique, autre qu'un service de communications électroniques, y compris un logiciel, qui est connecté au produit au moment de l'achat, ou de la mise en location ou en crédit-bail, de telle sorte que son absence empêcherait le produit connecté d'exécuter une ou plusieurs de ses fonctions, ou qui est ensuite connecté au produit par le fabricant ou un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté;

7) "traitement": toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou d'autres moyens de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

La définition de « traitement » est la même que celle du RGPD à une différence près : elle s’applique à toutes les données et pas seulement aux données personnelles.

8) "service de traitement de données": un service numérique qui est fourni à un client et qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services;

9) "même type de service": un ensemble de services de traitement de données qui partagent le même objectif principal, le même modèle de service de traitement de données et les principales fonctionnalités;

10) "service d'intermédiation de données": le service d'intermédiation de données au sens de l'article 2, point 11), du règlement (UE) 2022/868;

11) "personne concernée": la personne concernée telle qu'elle est visée à l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD

12) "utilisateur": une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes;

Le règlement introduit une nouvelle typologie d'acteurs qui ne figuraient pas dans le RGPD :utilisateur, détenteur de données, destinataire de données...

13) "détenteur de données": une personne physique ou morale qui, conformément au présent règlement, aux dispositions applicables du droit de l'Union ou à la législation nationale adoptée conformément au droit de l'Union, a le droit ou l'obligation d'utiliser et de mettre à disposition des données, y compris, lorsqu'il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu'elle a extraites ou générées au cours de la fourniture d'un service connexe;

14) "destinataire de données": une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union;

A noter : la définition de « destinataire de données » est différente de celle de « destinataire » dans le RGPD.
Par contre, la notion de « tiers » n'est pas définie dans le présent règlement.

15) "données relatives au produit": les données générées par l'utilisation d'un produit connecté que le fabricant a conçu pour qu'elles puissent être extraites, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant;

16) "données relatives au service connexe": les données représentant la numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur lors de la fourniture d'un service connexe par le fournisseur;

17) "données facilement accessibles": les données relatives à un produit et les données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération;

18) "secret d'affaires": un secret d'affaires au sens de l'article 2, point 1), de la directive (UE) 2016/943;

19) "détenteur de secrets d'affaires": un détenteur de secrets d'affaires au sens de l'article 2, point 2), de la directive (UE) 2016/943;

20) "profilage": le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

cf. RGPD

21) "mise à disposition sur le marché": toute fourniture d'un produit connecté destiné à être distribué, consommé ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

22) "mise sur le marché": la première mise à disposition d'un produit connecté sur le marché de l'Union;

23) "consommateur": toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale;

24) "entreprise": une personne physique ou morale qui, en ce qui concerne les contrats et pratiques relevant du présent règlement, agit à des fins liées à son activité commerciale, industrielle, artisanale ou libérale;

25) "petite entreprise": une petite entreprise telle qu'elle est définie à l'article 2, paragraphe 2, de l'annexe de la recommandation 2003/361/CE;

Entreprise de moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros.

26) "microentreprise": une microentreprise telle qu'elle est définie à l'article 2, paragraphe 3, de l'annexe de la recommandation 2003/361/CE;

Entreprise de moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros.

27) "organes de l'Union": les organes et organismes de l'Union mis en place par ou en vertu des actes adoptés sur la base du traité sur l'Union européenne, du traité sur le

fonctionnement de l'Union européenne ou du traité instituant la Communauté européenne de l'énergie atomique;

28) "organismes du secteur public": les autorités nationales, régionales ou locales des États membres et les organismes de droit public des États membres ou les associations formées par une ou plusieurs de ces autorités ou un ou plusieurs de ces organismes;

29) "situation d'urgence": une situation exceptionnelle, d'une durée limitée, telle qu'une urgence de santé publique, une urgence résultant d'une catastrophe naturelle ou d'une catastrophe majeure d'origine humaine, y compris un incident majeur de cybersécurité, ayant une incidence négative sur la population de l'Union ou sur l'ensemble ou une partie d'un État membre, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, la stabilité financière, ou la détérioration substantielle et immédiate d'actifs économiques dans l'Union ou l'État membre concerné, et qui est déterminée ou officiellement déclarée conformément aux procédures pertinentes prévues par le droit de l'Union ou le droit national;

30) "client": une personne physique ou morale qui a noué une relation contractuelle avec un fournisseur de services de traitement de données dans le but d'utiliser un ou plusieurs services de traitement de données;

31) "assistants virtuels": des logiciels capables de traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores ou écrites, ou des gestes ou des mouvements, et qui, sur la base de ces demandes, tâches ou questions, donnent accès à d'autres services ou contrôlent les fonctions des produits connectés;

32) "actifs numériques": des éléments en format numérique, y compris des applications, pour lesquels le client est titulaire du droit d'utilisation, indépendamment de la relation contractuelle que le client a avec le service de traitement de données qu'il a l'intention de quitter;

33) "infrastructure TIC sur site": une infrastructure TIC et des ressources informatiques qui appartiennent au client, qu'il loue ou qu'il utilise en crédit-bail, situées dans le centre de données du client lui-même et exploitées par le client ou par un tiers;

34) "changement de fournisseur": le processus impliquant un fournisseur d'origine de services de traitement de données, un client d'un service de traitement de données et, le cas échéant, un fournisseur de destination de services de traitement de données, par lequel le client d'un service de traitement de données passe de l'utilisation d'un service de traitement de données à l'utilisation d'un autre service de traitement de données du même type de service, ou un autre service, proposé par un fournisseur de services de traitement de données différent, ou à une infrastructure TIC sur site, y compris par l'extraction, la transformation et le téléversement des données;

35) "frais de transfert des données": les frais de transfert de données facturés aux clients pour l'extraction de leurs données au moyen du réseau depuis l'infrastructure TIC d'un fournisseur de services de traitement de données vers le système d'un fournisseur différent ou vers une infrastructure TIC sur site;

36) "frais de changement de fournisseur": les frais, autres que les frais de service standard ou les pénalités de résiliation anticipée, imposés par un fournisseur de services de traitement de données à un client pour les actions requises par le présent règlement pour changer de fournisseur en passant au système d'un fournisseur différent ou à une infrastructure TIC sur site, y compris les frais de transfert des données;

37) "équivalence fonctionnelle": le rétablissement, sur la base des données exportables et des actifs numériques du client, d'un niveau minimal de fonctionnalité dans l'environnement d'un nouveau service de traitement de données du même type de service après le processus de changement de fournisseur, lorsque le service de traitement de données de destination donne un résultat sensiblement comparable en réponse à la même entrée pour les fonctionnalités partagées fournies au client en vertu du contrat;

38) "données exportables": aux fins des articles 23 à 31 et de l'article 35, les données d'entrée et de sortie, y compris les métadonnées, générées directement ou indirectement, ou cogénérées, par l'utilisation par le client du service de traitement de données,

à l'exclusion des actifs ou des données protégés par des droits de propriété intellectuelle, ou constituant un secret d'affaires, des fournisseurs de services de traitement de données ou des tiers;

39) "contrat intelligent": un programme informatique utilisé pour l'exécution automatique d'un accord ou d'une partie de celui-ci, utilisant une séquence d'enregistrements de données électroniques et garantissant leur intégrité et l'exactitude de leur ordre chronologique;

40) "interopérabilité": la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits connectés, applications, services de traitement de données ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions;

41) "spécification d'interopérabilité ouverte": une spécification technique dans le domaine des technologies de l'information et de la communication qui est orientée vers les performances et la réalisation de l'interopérabilité entre les services de traitement de données;

42) "spécifications communes": un document, autre qu'une norme, contenant des solutions techniques qui permettent de satisfaire à certaines exigences et obligations établies au titre du présent règlement;

43) "norme harmonisée": une norme harmonisée au sens de l'article 2, point 1), c), du règlement (UE) no 1025/2012.

CHAPITRE II
PARTAGE DE DONNEES ENTRE ENTREPRISES ET CONSOMMATEURS ET ENTRE ENTREPRISES

Article 3
Obligation de rendre les données relatives aux produits et les données relatives aux services connexes accessibles à l'utilisateur

Mise à disposition des données

1. Les produits connectés sont conçus et fabriqués, et les services connexes conçus et fournis, de telle sorte que les données relatives auxdits produits et les données relatives aux services connexes, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, sont, par défaut, accessibles à l'utilisateur, de manière aisée, sécurisée, sans frais, dans un format complet, structuré, couramment utilisé et lisible par machine, et sont, lorsque cela est pertinent et techniquement possible, directement accessibles à l'utilisateur.

Informations préalables à l’achat

2. Avant la conclusion d'un contrat d'achat, de location ou de crédit-bail relatif à un produit connecté, le vendeur, le loueur ou le bailleur, qui peut être le fabricant, communique à l'utilisateur, de manière claire et compréhensible, au moins les informations suivantes:

a) le type, le format et le volume estimé des données relatives au produit que le produit connecté est capable de générer;

b) si le produit connecté est capable de générer des données en continu et en temps réel;

c) si le produit connecté est capable de stocker des données sur un dispositif intégré ou sur un serveur distant, y compris, le cas échéant, la durée de conservation prévue;

d) la manière dont l'utilisateur peut accéder aux données, extraire les données ou, le cas échéant, les effacer, y compris les moyens techniques nécessaires pour ce faire, ainsi que leurs conditions d'utilisation et leur qualité de service.

Informations préalables à la conclusion d’un contrat

3. Avant la conclusion d'un contrat relatif à la fourniture d'un service connexe, le fournisseur d'un tel service connexe communique à l'utilisateur, de manière claire et compréhensible, au moins les informations suivantes:

a) la nature, le volume estimé et la fréquence de collecte des données relatives au produit que le détenteur de données potentiel devrait obtenir et, le cas échéant, les modalités selon lesquelles l'utilisateur peut accéder à ces données ou les extraire, y compris les modalités de stockage des données du détenteur de données potentiel et la durée de conservation;

b) la nature et le volume estimé des données relatives aux services connexes à générer, ainsi que les modalités selon lesquelles l'utilisateur peut avoir accès à ces données ou les extraire, y compris les modalités de stockage des données du détenteur de données potentiel et la durée de conservation;

c) si le détenteur de données potentiel a l'intention d'utiliser lui-même des données facilement accessibles et les finalités pour lesquelles ces données sont utilisées, et s'il a l'intention d'autoriser un ou plusieurs tiers à utiliser les données pour des finalités convenues avec l'utilisateur;

d) l'identité du détenteur de données potentiel, telle que sa raison sociale et l'adresse géographique à laquelle il est établi et, le cas échéant, des autres parties au traitement de données;

e) les moyens de communication qui permettent de contacter rapidement le détenteur de données potentiel et de communiquer efficacement avec lui;

f) la manière dont l'utilisateur peut demander à ce que les données soient partagées avec un tiers et, le cas échéant, mettre un terme au partage des données;

g) le droit de l'utilisateur d'introduire une réclamation pour infraction aux dispositions du présent chapitre auprès de l'autorité compétente désignée en vertu de l'article 37;

h) si un détenteur de données potentiel est le détenteur de secrets d'affaires contenus dans les données qui sont accessibles à partir du produit connecté ou générées au cours de la fourniture d'un service connexe, et, lorsque le détenteur de données potentiel n'est pas le détenteur de secrets d'affaires, l'identité du détenteur de secrets d'affaires;

i) la durée du contrat entre l'utilisateur et le détenteur de données potentiel, ainsi que les modalités de résiliation de ce contrat.

Article 4
Droits et obligations des utilisateurs et des détenteurs de données concernant l'accès aux données relatives au produit et aux données relatives au service connexe, leur utilisation et leur mise à disposition

Accès aux données : droits et obligations des utilisateurs et des détenteurs

Données facilement accessibles

1. Lorsque l'utilisateur ne peut pas accéder directement à des données à partir du produit connecté ou du service connexe, les détenteurs de données rendent les données facilement accessibles, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, accessibles à l'utilisateur sans retard injustifié, à un niveau de qualité identique à celui dont bénéficie le détenteur de données, de manière aisée, sécurisée, sans frais, dans un format complet, structuré, couramment utilisé et lisible par machine et, lorsque cela est pertinent et techniquement possible, en continu et en temps réel. À cet effet, une simple demande est envoyée par voie électronique lorsque cela est techniquement possible.

Exigences de sécurité

2. Les utilisateurs et les détenteurs de données peuvent contractuellement restreindre ou interdire l'accès aux données, leur utilisation ou leur partage ultérieur, si un tel traitement est susceptible de porter atteinte aux exigences de sécurité du produit connecté, telles qu'elles sont prévues par le droit de l'Union ou le droit national, entraînant de graves effets indésirables pour la santé, la sûreté ou la sécurité des personnes physiques. Les autorités sectorielles peuvent fournir aux utilisateurs et aux détenteurs de données une expertise technique dans ce contexte. Lorsque le détenteur de données refuse de partager des données en vertu du présent article, il adresse une notification à l'autorité compétente désignée conformément à l'article 37.

Résolutions des litiges

3. Sans préjudice du droit de l'utilisateur de demander réparation à tout moment devant une juridiction d'un État membre, l'utilisateur, dans le cadre de tout litige avec le détenteur de données concernant les restrictions ou interdictions contractuelles visées au paragraphe 2, peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b); ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

Interdiction des interfaces trompeuses

4. Les détenteurs de données ne rendent pas indûment difficile pour les utilisateurs le fait d'effectuer des choix ou d'exercer des droits prévus au présent article, y compris en offrant des choix à l'utilisateur d'une manière qui n'est pas neutre ou en réduisant ou en compromettant l'autonomie, la prise de décision ou le choix des utilisateurs au moyen de la structure, de la conception, de la fonction ou du mode de fonctionnement d'une interface numérique utilisateur ou d'une partie de celle-ci.

Vérification du statut d'utilisateur

5. Afin de vérifier si une personne physique ou morale peut être considérée comme un utilisateur aux fins du paragraphe 1, un détenteur de données n'exige pas de ladite personne qu'elle fournisse d'autres informations que celles qui sont nécessaires. Les détenteurs de données ne conservent aucune autre information, en particulier aucune donnée de connexion, sur l'accès de l'utilisateur aux données demandées que celles qui sont nécessaires à la bonne exécution de la demande d'accès de l'utilisateur et à la sécurité et à la maintenance de l'infrastructure de données.

Préservation des sécrets d'affaires

6. Les secrets d'affaires sont préservés et ne sont divulgués que lorsque le détenteur de données et l'utilisateur prennent toutes les mesures nécessaires avant la divulgation pour préserver leur confidentialité, en particulier en ce qui concerne les tiers. Le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires recense les données protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes, et convient avec l'utilisateur de mesures techniques et organisationnelles proportionnées nécessaires afin de préserver la confidentialité des données partagées, en particulier en ce qui concerne les tiers, telles que des clauses contractuelles types, des accords de confidentialité, des protocoles d'accès stricts, des normes techniques et l'application de codes de conduite.

7. En l'absence d'accord sur les mesures nécessaires visées au paragraphe 6, ou si l'utilisateur ne met pas en œuvre les mesures convenues en vertu du paragraphe 6 ou compromet la confidentialité des secrets d'affaires, le détenteur de données peut bloquer ou, selon le cas, suspendre le partage des données définies comme secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit à l'utilisateur sans retard injustifié. Dans de tels cas, le détenteur de données notifie à l'autorité compétente désignée en vertu de l'article 37 qu'il a retenu ou suspendu le partage de données et indique les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise.

8. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d'affaires peut démontrer qu'il est très probable qu'il subisse un préjudice économique grave du fait de la divulgation de secrets d'affaires, malgré les mesures techniques et organisationnelles prises par l'utilisateur en vertu du paragraphe 6 du présent article, ce détenteur de données peut refuser au cas par cas une demande d'accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d'éléments objectifs, en particulier l'opposabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté, et est fournie par écrit à l'utilisateur sans retard injustifié. Lorsque le détenteur de données refuse de partager des données en vertu du présent paragraphe, il adresse une notification à l'autorité compétente désignée en vertu de l'article 37.

9. Sans préjudice du droit d'un utilisateur de demander réparation à tout moment devant une juridiction d'un État membre, un utilisateur souhaitant contester la décision d'un détenteur de données de refuser ou de bloquer ou suspendre le partage de données en vertu des paragraphes 7 et 8 peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b), qui décide, sans retard injustifié, si et dans quelles conditions le partage des données doit commencer ou reprendre; ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

Usage légal des données

10. L'utilisateur ne se sert pas des données obtenues en réponse à une demande visée au paragraphe 1 pour mettre au point un produit connecté concurrençant le produit connecté dont proviennent les données, ni ne partage les données avec un tiers dans cette intention, et il n'utilise pas ces données pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du fabricant ou, le cas échéant, du détenteur de données.

11. L'utilisateur s'abstient d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes dans l'infrastructure technique du détenteur de données qui est destinée à protéger les données pour obtenir l'accès aux données.

Fondement juridique

12. Lorsque l'utilisateur n'est pas la personne concernée dont les données à caractère personnel font l'objet de la demande, les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe ne sont mises à la disposition de l'utilisateur par le détenteur de données que s'il existe un fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies.

cf. RGPD

13. Un détenteur de données n'utilise les données facilement accessibles qui sont des données à caractère non personnel que sur la base d'un contrat avec l'utilisateur. Un détenteur de données n'utilise pas ces données pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation qu'en fait ce dernier, d'une quelconque autre manière susceptible de porter atteinte à la position commerciale dudit utilisateur sur les marchés où celui-ci est actif.

14. Les détenteurs de données ne mettent pas à la disposition de tiers les données à caractère non personnel relatives aux produits à des fins commerciales ou non commerciales autres que l'exécution de leur contrat avec l'utilisateur. Le cas échéant, les détenteurs de données obligent contractuellement les tiers à ne pas partager les données reçues de leur part.

Article 5
Droit de l'utilisateur de partager des données avec des tiers

Partage de données avec des tiers

1. Lorsqu'un utilisateur ou une partie agissant pour le compte d'un utilisateur en fait la demande, le détenteur de données met les données facilement accessibles, ainsi que les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, à la disposition d'un tiers sans retard injustifié, à un niveau de qualité identique à celui dont bénéficie le détenteur de données, de manière aisée, sécurisée, sans frais pour l'utilisateur, dans un format complet, structuré, couramment utilisé et lisible par machine et, lorsque cela est pertinent et techniquement possible, en continu et en temps réel. Les données sont mises à la disposition du tiers par le détenteur de données conformément aux articles 8 et 9.

2. Le paragraphe 1 ne s'applique pas aux données facilement accessibles dans le cadre de l'essai de nouveaux produits connectés, substances ou procédés qui ne sont pas encore mis sur le marché, à moins que leur utilisation par un tiers ne soit contractuellement autorisée.

3. Toute entreprise désignée comme contrôleur d'accès, conformément à l'article 3 du règlement (UE) 2022/1925, n'est pas un tiers éligible au titre du présent article et ne peut par conséquent pas:

Les contrôleurs d’accès ne sont pas des tiers éligibles.

a) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, quelles qu'elles soient, y compris en fournissant une compensation pécuniaire ou de toute autre nature, à mettre à la disposition de l'un de ses services des données que l'utilisateur a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1;

b) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, à demander au détenteur de données de mettre des données à la disposition de l'un de ses services conformément au paragraphe 1 du présent article;

c) recevoir d'un utilisateur des données que ce dernier a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1.

4. Afin de vérifier si une personne physique ou morale peut être considérée comme un utilisateur ou un tiers aux fins du paragraphe 1, l'utilisateur ou le tiers n'est pas tenu de fournir d'autres informations que celles qui sont nécessaires. Les détenteurs de données ne conservent aucune autre information sur l'accès du tiers aux données demandées que celles qui sont nécessaires à la bonne exécution de la demande d'accès du tiers et à la sécurité et à la maintenance de l'infrastructure de données.

Usage loyal des données par les tiers

5. Le tiers s'abstient d'avoir recours à des moyens coercitifs ou de tirer avantage de lacunes dans l'infrastructure technique d'un détenteur de données qui est destinée à protéger les données pour obtenir l'accès aux données.

6. Un détenteur de données n'utilise aucune donnée facilement accessible pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du tiers, ou sur l'utilisation qu'en fait ce dernier, d'une quelconque autre manière susceptible de porter atteinte à la position commerciale du tiers sur les marchés sur lesquels il exerce ses activités, à moins que le tiers n'ait autorisé cette utilisation et ne dispose de la possibilité technique de retirer facilement cette autorisation à tout moment.

Fondement juridique

7. Lorsque l'utilisateur n'est pas la personne concernée dont les données à caractère personnel font l'objet de la demande, les données à caractère personnel générées par l'utilisation d'un produit connecté ou d'un service connexe, ne sont mises à la disposition du tiers par le détenteur de données que s'il existe un fondement juridique valable pour le traitement au titre de l'article 6 du règlement (UE) 2016/679 et, le cas échéant, si les conditions énoncées à l'article 9 dudit règlement et à l'article 5, paragraphe 3, de la directive 2002/58/CE sont remplies.

cf. RGPD

8. L'absence d'accord entre le détenteur de données et le tiers concernant les modalités de transmission des données ne doit pas entraver, empêcher ou interférer avec l'exercice des droits de la personne concernée au titre du règlement (UE) 2016/679 et, en particulier, du droit à la portabilité des données prévu à l'article 20 dudit règlement.

cf. RGPD

9. Les secrets d'affaires sont préservés et ne sont divulgués à des tiers que dans la mesure où cette divulgation est strictement nécessaire pour atteindre la finalité convenue entre l'utilisateur et le tiers. Le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, recense les données protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes, et convient avec le tiers de toutes les mesures techniques et organisationnelles proportionnées nécessaires afin de préserver la confidentialité des données partagées, telles que des clauses contractuelles types, des accords de confidentialité, des protocoles d'accès stricts, des normes techniques et l'application de codes de conduite.

10. En l'absence d'accord sur les mesures nécessaires visées au paragraphe 9 du présent article, ou si le tiers ne met pas en œuvre les mesures convenues en vertu du paragraphe 9 du présent article ou compromet la confidentialité des secrets d'affaires, le détenteur de données peut bloquer ou, selon le cas, suspendre le partage des données définies comme constituant des secrets d'affaires. La décision du détenteur de données est dûment motivée et communiquée par écrit au tiers, sans retard injustifié. Dans de tels cas, le détenteur de données notifie à l'autorité compétente désignée en vertu de l'article 37 qu'il a retenu ou suspendu le partage de données et indique les mesures qui n'ont pas été convenues ou mises en œuvre et, le cas échéant, les secrets d'affaires dont la confidentialité a été compromise.

11. Dans des circonstances exceptionnelles, lorsque le détenteur de données qui est un détenteur de secret d'affaires peut démontrer qu'il est très probable qu'il subisse un préjudice économique grave du fait de la divulgation de secrets d'affaires, malgré les mesures techniques et organisationnelles prises par le tiers en vertu du paragraphe 9 du présent article, ce détenteur de données peut refuser au cas par cas une demande d'accès aux données spécifiques en question. Cette démonstration est dûment étayée sur la base d'éléments objectifs, en particulier l'opposabilité de la protection des secrets d'affaires dans les pays tiers, la nature et le niveau de confidentialité des données demandées, ainsi que le caractère unique et neuf du produit connecté, et est fournie par écrit au tiers sans retard injustifié. Lorsque le détenteur de données refuse de

partager des données en vertu du présent paragraphe, il adresse une notification à l'autorité compétente désignée en vertu de l'article 37.

12. Sans préjudice du droit du tiers de demander réparation à tout moment devant une juridiction d'un État membre, un tiers souhaitant contester la décision du détenteur de données de refuser ou de bloquer ou suspendre le partage de données en vertu des paragraphes 10 et 11 peut:

a) introduire une réclamation auprès de l'autorité compétente conformément à l'article 37, paragraphe 5, point b), qui décide, sans retard injustifié, si et dans quelles conditions le partage des données doit commencer ou reprendre; ou

b) convenir avec le détenteur de données de porter la question devant un organe de règlement des litiges conformément à l'article 10, paragraphe 1.

13. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits des personnes concernées conformément au droit de l'Union et au droit national applicables en matière de protection des données à caractère personnel.

Article 6
Obligations des tiers recevant des données à la demande de l'utilisateur

Obligations des tiers

1. Un tiers traite les données mises à sa disposition en application de l'article 5 uniquement aux fins et dans les conditions convenues avec l'utilisateur et sous réserve du droit de l'Union et du droit national en matière de protection des données à caractère personnel, y compris les droits de la personne concernée dans la mesure où les données à caractère personnel sont concernées. Le tiers efface les données lorsqu'elles ne sont plus nécessaires à la finalité convenue, sauf accord contraire avec l'utilisateur en ce qui concerne les données à caractère non personnel.

2. Le tiers ne peut pas:

a) rendre l'exercice des choix ou des droits de l'utilisateur, au titre de l'article 5 et du présent article, indûment difficile, y compris en proposant des choix à l'utilisateur d'une manière qui n'est pas neutre, ou en contraignant, en trompant ou en manipulant l'utilisateur, ou en réduisant ou en compromettant l'autonomie, la prise de décision ou les choix de l'utilisateur, y compris au moyen d'une interface numérique utilisateur ou d'une partie de celle-ci;

b) nonobstant l'article 22, paragraphe 2, points a) et c), du règlement (UE) 2016/679, utiliser les données qu'il reçoit à des fins de profilage, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur;

cf. RGPD

c) mettre les données qu'il reçoit à la disposition d'un autre tiers, à moins que les données ne soient mises à disposition sur le fondement d'un contrat avec l'utilisateur, et à condition que l'autre tiers prenne toutes les mesures nécessaires convenues entre le détenteur de données et le tiers pour préserver la confidentialité des secrets d'affaires;

d) mettre les données qu'il reçoit à la disposition d'une entreprise désignée comme contrôleur d'accès, conformément à l'article 3 du règlement (UE) 2022/1925;

e) utiliser les données qu'il reçoit pour développer un produit concurrençant le produit connecté dont proviennent les données auxquelles il a accès ou de partager les données avec un autre tiers à cette fin; les tiers n'utilisent pas non plus de données à caractère non personnel relatives au produit ou relatives au service connexe mises à leur disposition pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production du détenteur de données ou sur l'utilisation que ce dernier en fait;

f) utiliser les données qu'il reçoit d'une manière qui nuit à la sécurité du produit connecté ou du service connexe;

g) méconnaître les mesures spécifiques convenues avec le détenteur de données ou le détenteur de secrets d'affaires conformément à l'article 5, paragraphe 9, et compromettre la confidentialité des secrets d'affaires;

h) empêcher l'utilisateur qui est un consommateur, y compris sur le fondement 'd'un contrat, de mettre à la disposition d'autres parties les données qu'il reçoit.

Article 7
Champ d'application des obligations en matière de partage de données entre consommateurs et entreprises et entre entreprises

Exemption pour les petites et micro-entreprises

1. Les obligations définies dans le présent chapitre ne s'appliquent pas aux données générées par l'utilisation de produits connectés fabriqués ou conçus ou de services connexes fournis par une microentreprise ou une petite entreprise, à condition que cette entreprise n'ait pas une entreprise partenaire ou une entreprise liée au sens de l'article 3 de l'annexe de la recommandation 2003/361/CE qui n'est pas qualifiée de microentreprise ou de petite entreprise et lorsque la microentreprise et petite entreprise ne travaille pas en sous-traitance pour fabriquer ou concevoir un produit connecté ou pour fournir un service connexe.

Il en va de même pour les données générées par l'utilisation de produits connectés fabriqués ou de services connexes fournis par une entreprise qui est qualifiée d'entreprise moyenne au titre de l'article 2 de l'annexe de la recommandation 2003/361/CE depuis moins d'un an et pour les produits connectés pendant une période d'un an après la date à laquelle ils ont été mis sur le marché par une entreprise moyenne.

2. Toute clause contractuelle qui, au détriment de l'utilisateur, exclut l'application des droits de l'utilisateur au titre du présent chapitre, y déroge ou en modifie les effets, n'est pas contraignante pour l'utilisateur.

CHAPITRE III
OBLIGATIONS APPLICABLES AUX DETENTEURS DE DONNEES TENUS DE METTRE DES DONNEES A DISPOSITION EN VERTU DU DROIT DE L'UNION

Obligations des détenteurs de données

Article 8
Conditions dans lesquelles les détenteurs de données mettent des données à la disposition des destinataires de données

Conditions de mise à disposition

1. Lorsque, dans le cadre de relations entre entreprises, un détenteur de données est tenu de mettre des données à la disposition d'un destinataire de données au titre de l'article 5 ou au titre d'autres dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, il convient des modalités de cette mise à disposition des données avec un destinataire de données, et ce selon des modalités et conditions équitables, raisonnables et non discriminatoires et de manière transparente, conformément au présent chapitre et au chapitre IV.

2. Une clause contractuelle concernant l'accès aux données et l'utilisation des données, ou la responsabilité et les voies de recours en cas de violation ou d'extinction des obligations relatives aux données, n'est pas contraignante si elle constitue une clause contractuelle abusive au sens de l'article 13 ou si, au détriment de l'utilisateur, elle exclut l'application des droits de l'utilisateur au titre du chapitre II, y déroge ou en modifie les effets.

3. Lorsqu'il met des données à disposition, un détenteur de données s'abstient de toute discrimination en ce qui concerne les modalités de mise à disposition des données entre des catégories comparables de destinataires de données, y compris les entreprises partenaires ou les entreprises liées du destinataire de données. Lorsqu'un destinataire de données considère que les conditions dans lesquelles des données ont été mises à sa disposition sont discriminatoires, le détenteur de données fournit, sans retard injustifié, au destinataire de données, sur demande motivée de celui-ci, des informations attestant l'absence de discrimination.

4. Un détenteur de données ne met pas de données à la disposition d'un destinataire de données, y compris sur une base d'exclusivité, sauf si l'utilisateur le demande au titre du chapitre II.

5. Les détenteurs de données et les destinataires de données ne sont pas tenus de fournir des informations autres que celles qui sont nécessaires pour vérifier le respect des

clauses contractuelles convenues pour la mise à disposition des données ou des obligations qui leur incombent au titre du présent règlement ou d'autres dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union.

6. Sauf disposition contraire du droit de l'Union, y compris l'article 4, paragraphe 6, et l'article 5, paragraphe 9, du présent règlement, ou de la législation nationale adoptée conformément au droit de l'Union, l'obligation de mettre des données à la disposition d'un destinataire de données n'impose pas la divulgation de secrets d'affaires.

Article 9
Compensation pour la mise à disposition de données

Compensation

1. Toute compensation convenue, dans le cadre de relations entre entreprises, entre un détenteur de données et un destinataire de données pour la mise à disposition des données est non discriminatoire et raisonnable et peut inclure une marge.

2. Lorsqu'ils s'accordent sur une compensation, le détenteur de données et le destinataire de données tiennent compte en particulier:

a) des coûts occasionnés par la mise à disposition des données, dont, notamment, les coûts encourus pour le formatage des données, leur diffusion par voie électronique et leur stockage;

b) des investissements dans la collecte et la production de données, le cas échéant, en prenant en compte le fait que d'autres parties ont contribué ou non à l'obtention, à la production ou à la collecte des données en question.

3. La compensation visée au paragraphe 1 peut également dépendre du volume, du format et de la nature des données.

4. Lorsque le destinataire de données est une PME ou un organisme de recherche à but non lucratif et que ce destinataire de données n'a pas d'entreprises partenaires ou d'entreprises liées qui ne sont pas considérées comme des PME, toute compensation convenue n'excède pas les coûts visés au paragraphe 2, point a).

5. La Commission adopte des lignes directrices sur le calcul de la compensation raisonnable, en tenant compte de l'avis du comité européen de l'innovation dans le domaine des données visé à l'article 42.

6. Le présent article ne fait pas obstacle à ce que d'autres dispositions du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union excluent une éventuelle compensation pour la mise à disposition de données ou prévoient une compensation moins élevée.

7. Le détenteur de données fournit au destinataire de données des informations exposant la base de calcul de la compensation de manière suffisamment détaillée pour lui permettre d'évaluer si les exigences des paragraphes 1 à 4 sont respectées.

Article 10
Règlement des litiges

Litiges

1. Les utilisateurs, les détenteurs de données et les destinataires de données ont accès à un organe de règlement des litiges, certifié conformément au paragraphe 5 du présent article, pour régler les litiges en vertu de l'article 4, paragraphes 3 et 9, et de l'article 5, paragraphe 12, ainsi que les litiges portant sur les modalités et conditions équitables, raisonnables et non discriminatoires applicables à la mise à disposition de données et à la façon de mettre ces données à disposition en toute transparence conformément au présent chapitre et au chapitre IV.

2. Les organes de règlement des litiges informent les parties concernées des frais, ou des mécanismes utilisés pour les déterminer, avant que ces parties ne demandent une décision.

3. Pour les litiges portés devant un organe de règlement des litiges en vertu de l'article 4, paragraphes 3 et 9, et de l'article 5, paragraphe 12, lorsque l'organe de règlement des

litiges se prononce sur un litige en faveur de l'utilisateur ou du destinataire de données, le détenteur de données supporte tous les frais facturés par l'organe de règlement des litiges et rembourse à cet utilisateur ou à ce destinataire de données toute autre dépense raisonnable qu'il a supportée en lien avec le règlement du litige. Lorsque l'organe de règlement des litiges se prononce sur un litige en faveur du détenteur de données, l'utilisateur ou le destinataire de données n'est pas tenu de rembourser les frais ou autres dépenses que le détenteur de données a engagés ou dont il est redevable en lien avec le règlement du litige, à moins que l'organe de règlement des litiges ne constate que l'utilisateur ou le destinataire de données a manifestement agi de mauvaise foi.

4. Les clients et les fournisseurs de services de traitement de données ont accès à un organe de règlement des litiges, certifié conformément au paragraphe 5 du présent article, pour régler les litiges relatifs aux violations des droits des clients et aux obligations des fournisseurs de services de traitement de données conformément aux articles 23 à 31.

5. L'État membre dans lequel l'organe de règlement des litiges est établi certifie cet organe à sa demande, lorsqu'il a démontré qu'il remplit toutes les conditions suivantes:

a) il est impartial et indépendant et doit rendre ses décisions conformément à des règles de procédure claires, non discriminatoires et équitables;

b) il dispose de l'expertise nécessaire, en particulier en ce qui concerne les modalités et conditions équitables, raisonnables et non discriminatoires, y compris en matière de compensation, et en ce qui concerne la mise à disposition de données en toute transparence, ce qui permet à l'organisme de déterminer efficacement ces modalités et conditions;

c) il est facilement accessible au moyen de technologies de communication électronique;

d) il est en mesure d'adopter ses décisions de manière rapide, efficace et économiquement avantageuse, dans au moins une langue officielle de l'Union.

6. Les États membres notifient à la Commission la liste des organes de règlement des litiges certifiés conformément au paragraphe 5. La Commission publie une liste de ces organes sur un site internet spécifique et la tient à jour.

7. Un organe de règlement des litiges refuse de traiter une demande de règlement d'un litige qui a déjà été porté devant un autre organe de règlement des litiges ou devant une juridiction d'un État membre.

8. Un organe de règlement des litiges donne aux parties la possibilité, dans un délai raisonnable, d'exprimer leur point de vue sur les questions qu'elles ont soumises à cet organe. Dans ce contexte, chaque partie à un litige se voit communiquer les observations de l'autre partie au litige et toute déclaration faite par des experts. Les parties ont la possibilité de formuler des observations sur ces observations et déclarations.

9. Un organe de règlement des litiges prend sa décision sur toute question qui lui est soumise dans un délai de 90 jours à compter de la réception d'une demande présentée en vertu des paragraphes 1 et 4. Cette décision est formulée par écrit ou sur un support durable et est étayée par un exposé des motifs.

10. Les organes de règlement des litiges rédigent et rendent publics des rapports annuels d'activité. Ces rapports annuels incluent en particulier les informations générales suivantes:

a) une agrégation des résultats des litiges;

b) le laps de temps moyen nécessaire à la résolution des litiges;

c) les causes les plus courantes de litiges.

11. Afin de faciliter l'échange d'informations et de bonnes pratiques, un organe de règlement des litiges peut décider d'inclure des recommandations dans le rapport visé au paragraphe 10 sur la manière dont les problèmes peuvent être évités ou résolus.

12. La décision d'un organe de règlement des litiges n'est contraignante pour les parties que si celles-ci ont expressément consenti à son caractère contraignant avant le début de la procédure de règlement du litige.

13. Le présent article ne porte pas atteinte au droit des parties de former un recours effectif devant une juridiction d'un État membre.

Article 11
Mesures techniques de protection relatives à l'utilisation ou à la divulgation non autorisées de données

Mesures de protection des données

1. Un détenteur de données peut appliquer des mesures techniques appropriées de protection, y compris des contrats intelligents et le chiffrement, afin d'empêcher l'accès non autorisé aux données, y compris les métadonnées, et de garantir le respect des articles 4, 5, 6, 8 et 9, ainsi que des clauses contractuelles convenues pour la mise à disposition des données. Ces mesures techniques de protection ne doivent pas donner lieu à une discrimination entre les destinataires de données ni porter atteinte au droit de l'utilisateur d'obtenir une copie des données, de les récupérer, de les utiliser ou d'y accéder, de fournir des données à des tiers conformément à l'article 5 ou aux droits des tiers au titre du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union. Les utilisateurs, les tiers et les destinataires de données ne modifient pas ni ne suppriment de telles mesures techniques de protection, sauf accord du détenteur de données.

2. Dans les circonstances visées au paragraphe 3, le tiers ou le destinataire de données donne suite, sans retard injustifié, aux demandes du détenteur de données et, le cas échéant et s'il ne s'agit pas de la même personne, du détenteur de secrets d'affaires ou de l'utilisateur:

a) d'effacer les données mises à disposition par le détenteur de données et les éventuelles copies de celles-ci;

b) de mettre fin à la production, à l'offre ou à la mise sur le marché ou à l'utilisation de biens, de données dérivées ou de services produits sur la base des connaissances obtenues au moyen de ces données, ou à l'importation, à l'exportation ou au stockage de biens non conformes destinés aux fins précitées, et de détruire tout bien non conforme, lorsqu'il existe un risque grave que l'utilisation illicite de ces données cause un préjudice important au détenteur de données, au détenteur de secrets d'affaires ou à l'utilisateur ou lorsqu'une telle mesure ne serait pas disproportionnée au regard des intérêts du détenteur de données, du détenteur de secrets d'affaires ou de l'utilisateur;

c) d'informer l'utilisateur de l'utilisation ou de la divulgation non autorisées des données et des mesures prises pour mettre fin à l'utilisation ou à la divulgation non autorisée des données;

d) d'indemniser la partie lésée par l'utilisation abusive ou la divulgation de ces données auxquelles il a été accédé illégalement ou qui ont été utilisées illégalement.

3. Le paragraphe 2 s'applique lorsqu'un tiers ou un destinataire de données:

a) aux fins de l'obtention de données, a fourni de fausses informations à un détenteur de données, a eu recours à des moyens trompeurs ou coercitifs ou a tiré avantage de lacunes dans l'infrastructure technique du détenteur de données destinée à protéger les données;

b) a utilisé les données mises à disposition à des fins non autorisées, y compris le développement d'un produit connecté concurrent au sens de l'article 6, paragraphe 2, point e);

c) a divulgué illégalement des données à une autre partie;

d) n'a pas maintenu les mesures techniques et organisationnelles convenues en vertu de l'article 5, paragraphe 9; ou

e) a modifié ou supprimé des mesures techniques de protection appliquées par le détenteur de données en vertu du paragraphe 1 du présent article sans l'accord du détenteur de données.

4. Le paragraphe 2 s'applique également lorsqu'un utilisateur ou un destinataire de données modifie ou retire des mesures techniques de protection appliquées par le détenteur de données ou ne maintient pas des mesures techniques et organisationnelles prises par l'utilisateur en accord avec le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires, afin de préserver les secrets d'affaires, ainsi qu'à l'égard de toute autre partie qui reçoit les données de l'utilisateur à la suite d'une infraction au présent règlement.

5. Lorsque le destinataire de données enfreint l'article 6, paragraphe 2, point a) ou b), les utilisateurs disposent des mêmes droits que les détenteurs de données au titre du paragraphe 2 du présent article.

Article 12
Champ d'application des obligations applicables aux détenteurs de données tenus au titre du droit de l'Union de mettre des données à disposition

1. Le présent chapitre s'applique lorsque, dans le cadre de relations entre entreprises, un détenteur de données est tenu, au titre de l'article 5 ou des dispositions applicables du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, de mettre des données à la disposition d'un destinataire de données.

2. Toute clause contractuelle figurant dans un accord de partage de données qui, au détriment d'une partie ou, le cas échéant, au détriment de l'utilisateur, exclut l'application du présent chapitre, y déroge ou en modifie les effets, n'est pas contraignante pour cette partie.

CHAPITRE IV
CLAUSES CONTRACTUELLES ABUSIVES RELATIVES A L'ACCES AUX DONNEES ET A L'UTILISATION DES DONNEES ENTRE ENTREPRISES

Clauses contractuelles abusives

Article 13
Clauses contractuelles abusives imposées unilatéralement à une autre entreprise

1. Une clause contractuelle concernant l'accès aux données et l'utilisation des données ou la responsabilité et les voies de recours en cas de violation ou d'extinction d'obligations liées aux données qu'une entreprise a imposée unilatéralement à une autre entreprise ne lie pas cette dernière entreprise si elle est abusive.

2. Une clause contractuelle qui reflète des dispositions impératives du droit de l'Union ou des dispositions du droit de l'Union qui s'appliqueraient si les clauses contractuelles ne réglaient pas la question n'est pas considérée comme étant abusive.

3. Une clause contractuelle est abusive si elle est d'une nature telle que son utilisation s'écarte manifestement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation des données, contrairement à la bonne foi et à un usage loyal.

4. En particulier, aux fins du paragraphe 3, une clause contractuelle est abusive si elle a pour objet ou pour effet:

a) d'exclure ou de limiter la responsabilité de la partie qui a unilatéralement imposé la clause en cas d'actes intentionnels ou de négligence grave;

b) d'exclure les voies de recours dont dispose la partie à laquelle la clause a été unilatéralement imposée en cas d'inexécution d'obligations contractuelles ou la responsabilité

de la partie qui a unilatéralement imposé la clause en cas de manquement à ces obligations;

c) de donner à la partie qui a unilatéralement imposé la clause le droit exclusif de déterminer si les données fournies sont conformes au contrat ou d'interpréter toute clause contractuelle.

5. Aux fins du paragraphe 3, une clause contractuelle est présumée être abusive si elle a pour objet ou pour effet:

a) de limiter de manière inappropriée les voies de recours en cas d'inexécution des obligations contractuelles ou la responsabilité en cas de manquement à ces obligations, ou d'étendre la responsabilité de l'entreprise à laquelle la clause a été imposée unilatéralement;

b) de permettre à la partie qui a imposé unilatéralement la clause d'avoir accès aux données de l'autre partie contractante et de les utiliser d'une manière qui porte gravement atteinte aux intérêts légitimes de l'autre partie contractante, en particulier lorsque ces données contiennent des données commercialement sensibles ou sont protégées par des secrets d'affaires ou des droits de propriété intellectuelle;

c) d'empêcher la partie à laquelle la clause a été imposée unilatéralement d'utiliser les données qu'elle a fournies ou générées pendant la durée du contrat, ou de limiter l'utilisation de ces données dans la mesure où cette partie n'est pas autorisée à utiliser ou à enregistrer ces données, à y accéder ou à les contrôler ou à en exploiter la valeur de manière adéquate;

d) d'empêcher la partie à laquelle la clause a été imposée unilatéralement de résilier l'accord dans un délai raisonnable;

e) d'empêcher la partie à laquelle la clause a été imposée unilatéralement d'obtenir une copie des données qu'elle a fournies ou générées pendant la durée du contrat ou dans un délai raisonnable après la résiliation de celui-ci;

f) de permettre à la partie qui a imposé unilatéralement la clause de résilier le contrat dans un délai excessivement court, compte tenu des possibilités dont l'autre partie contractante dispose raisonnablement pour se tourner vers un service alternatif et comparable et du préjudice financier causé par cette résiliation, sauf s'il existe des motifs sérieux de le faire;

g) de permettre à la partie qui a imposé unilatéralement la clause de modifier substantiellement le prix indiqué dans le contrat ou toute autre condition de fond liée à la nature, au format, à la qualité ou à la quantité des données à partager, lorsqu'aucun motif valable ou aucun droit pour l'autre partie de résilier le contrat dans le cas d'une telle modification n’est stipulé dans le contrat.

Le premier alinéa, point g), n'affecte pas les clauses par lesquelles la partie qui a imposé unilatéralement la clause en question se réserve le droit de modifier unilatéralement les clauses d'un contrat à durée indéterminée, pour autant que le contrat ait prévu une raison valable pour effectuer de telles modifications unilatéralement, que la partie qui a imposé unilatéralement la clause soit tenue d'informer l'autre partie contractante moyennant un préavis raisonnable de son intention d'effectuer une telle modification, et que l'autre partie contractante soit libre de résilier le contrat sans frais dans le cas d'une telle modification.

6. Une clause contractuelle est considérée comme étant imposée unilatéralement au sens du présent article si elle a été fournie par une partie contractante et si l'autre partie contractante n'a pas été en mesure d'influencer son contenu malgré une tentative de négociation. Il appartient à la partie contractante qui a fourni la clause contractuelle de prouver que cette clause n'a pas été imposée unilatéralement. La partie contractante qui a fourni la clause contractuelle faisant l'objet d'une contestation ne peut pas invoquer le caractère abusif de la clause contractuelle.

7. Lorsque la clause abusive est dissociable des autres clauses du contrat, ces dernières sont contraignantes.

8. Le présent article ne s'applique pas aux clauses contractuelles définissant l'objet principal du contrat ni à l'adéquation entre le prix et les données fournies en contrepartie.

9. Les parties à un contrat relevant du paragraphe 1 n'excluent pas l'application du présent article, n'y dérogent pas ou n'en modifient pas les effets.

CHAPITRE V
MISE A LA DISPOSITION D'ORGANISMES DU SECTEUR PUBLIC, DE LA COMMISSION, DE LA BANQUE CENTRALE EUROPEENNE ET D'ORGANES DE L'UNION DE DONNEES SUR LE FONDEMENT D'UN BESOIN EXCEPTIONNEL

Organismes publics

Article 14
Obligation de mettre des données à disposition sur le fondement d'un besoin exceptionnel

Besoins exceptionnels

Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union démontre l'existence d'un besoin exceptionnel, tel qu'il est décrit à l'article 15, d'utiliser certaines données, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, pour exercer ses fonctions statutaires à des fins d'intérêt public, les détenteurs de données qui sont des personnes morales, autres que des organismes du secteur public, qui détiennent ces données les mettent à disposition sur demande dûment motivée.

Article 15
Besoin exceptionnel d'utiliser des données

1. Un besoin exceptionnel d'utiliser certaines données au sens du présent chapitre a une durée et une portée limitées et est réputé exister uniquement dans les cas suivants:

a) lorsque les données demandées sont nécessaires pour réagir à une situation d'urgence et que l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union n'est pas en mesure d'obtenir ces données par d'autres moyens en temps utile et de manière efficace et dans des conditions équivalentes;

b) dans des circonstances non couvertes par le point a) et uniquement en ce qui concerne les données à caractère non personnel, lorsque:

i) un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union agit sur la base du droit de l'Union ou du droit national et a déterminé des données spécifiques, dont l'absence l'empêche d’exécuter une mission spécifique d'intérêt public, qui a été explicitement prévue par la loi, telle que la production de statistiques officielles, l'atténuation d'une situation d'urgence ou le rétablissement à la suite d'une situation d'urgence; et

ii) l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union a épuisé tous les autres moyens à sa disposition pour obtenir ces données, y compris l'achat de données à caractère non personnel sur le marché aux prix du marché ou le recours aux obligations existantes de mise à disposition des données ou l'adoption de nouvelles mesures législatives pouvant garantir la disponibilité des données en temps utile.

2. Le paragraphe 1, point b), ne s'applique pas aux microentreprises ni aux petites entreprises.

3. L'obligation de démontrer que l'organisme du secteur public n'a pas été en mesure d'obtenir des données à caractère non personnel en les achetant sur le marché ne s'applique pas lorsque la mission spécifique exécutée dans l'intérêt public consiste en la production de statistiques officielles et que l'achat de ces données n'est pas autorisé par le droit national.

Article 16
Relation avec d'autres obligations de mettre des données à la disposition d'organismes du secteur public, de la Commission, de la Banque centrale européenne et d'organes de l'Union

1. Le présent chapitre n'affecte pas les obligations prévues par le droit de l'Union ou par le droit national aux fins de l'établissement de rapports, du respect des demandes d'accès aux informations ou de la démonstration ou de la vérification du respect des obligations légales.

2. Le présent chapitre ne s'applique pas aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union lorsqu'ils exercent des activités de prévention et de détection des infractions pénales ou administratives, d'enquêtes ou de poursuites en la matière, ou d'exécution de sanctions pénales, ni à l'administration douanière ou fiscale. Le présent chapitre n'affecte pas les dispositions applicables du droit de l'Union et du droit national relatives à la prévention et à la détection des infractions pénales ou administratives, aux enquêtes et aux poursuites en la matière, à l'exécution de sanctions pénales ou administratives, ou relatives à l'administration douanière ou fiscale.

Article 17
Demandes de mise à disposition de données

Demandes de données

1. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union demande des données en vertu de l'article 14, il ou elle:

a) précise les données qui sont demandées, y compris les métadonnées nécessaires à l'interprétation et à l'utilisation de ces données;

b) démontre que les conditions nécessaires à l'existence d'un besoin exceptionnel conformément à l'article 15 pour lequel les données sont demandées sont remplies;

c) explique la finalité de la demande, l'utilisation qu'il est prévu de faire des données demandées, y compris, le cas échéant, par un tiers conformément au paragraphe 4 du présent article, la durée de cette utilisation et, le cas échéant, la manière dont le traitement de données à caractère personnel doit répondre au besoin exceptionnel;

d) précise, si possible, la date à laquelle les données sont censées être effacées par toutes les parties qui y ont accès;

e) justifie le choix du détenteur de données auquel la demande est adressée;

f) précise avec qui, parmi les autres organismes du secteur public, la Commission, la Banque centrale européenne ou les organes de l'Union ou les tiers, il est prévu de partager les données demandées;

g) lorsque des données à caractère personnel sont demandées, précise les éventuelles mesures techniques et organisationnelles proportionnées et nécessaires pour mettre en œuvre les principes de protection des données et les garanties nécessaires, telles que la pseudonymisation, et si l'anonymisation peut être appliquée par le détenteur de données avant de mettre les données à disposition;

h) indique la disposition juridique confiant à l'organisme du secteur public demandeur, à la Commission, à la Banque centrale européenne ou à l'organe de l'Union la mission spécifique exécutée dans l'intérêt public qui justifie la demande de données;

i) précise le délai dans lequel les données doivent être mises à disposition et le délai visé à l'article 18, paragraphe 2, dans lequel le détenteur de données peut rejeter la demande ou demander sa modification;

j) met tout en œuvre pour éviter qu'en donnant suite à la demande de données, les détenteurs de données n'engagent leur responsabilité pour infraction au droit de l'Union ou au droit national.

2. Une demande de données présentée en vertu du paragraphe 1 du présent article:

a) est formulée par écrit et exprimée en termes clairs, concis et simples, compréhensibles pour le détenteur de données;

b) est spécifique quant au type de données demandées et correspond aux données sur lesquelles le détenteur de données exerce un contrôle au moment de la demande;

c) est proportionnée au besoin exceptionnel et dûment motivée, en ce qui concerne la granularité et le volume des données demandées, ainsi que la fréquence d'accès aux données demandées;

d) respecte les objectifs légitimes du détenteur de données, en s'engageant à garantir la protection des secrets d'affaires conformément à l'article 19, paragraphe 3, ainsi qu'en tenant compte des coûts et des efforts nécessaires pour mettre les données à disposition;

e) concerne des données à caractère non personnel et, uniquement s'il est démontré que cela est insuffisant pour répondre au besoin exceptionnel d'utiliser des données, conformément à l'article 15, paragraphe 1, point a), des données à caractère personnel sous une forme pseudonymisée et établit les mesures techniques et organisationnelles qui doivent être prises pour protéger les données;

f) informe le détenteur de données des sanctions qui doivent être imposées au titre de l'article 40 par l'autorité compétente désignée en vertu de l'article 37 s'il n'est pas donné suite à la demande;

g) lorsqu'elle est présentée par un organisme du secteur public, est transmise au coordinateur de données visé à l'article 37 de l'État membre dans lequel est établi l'organisme du secteur public demandeur, qui publie la demande en ligne sans retard injustifié, à moins que le coordinateur de données ne considère qu'une telle publication présenterait un risque pour la sécurité publique;

h) lorsqu'elle est présentée par la Commission, la Banque centrale européenne ou un organe de l'Union, est mise à disposition en ligne sans retard injustifié;

i) lorsque des données à caractère personnel sont demandées, est notifiée sans retard injustifié à l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 dans l'État membre dans lequel l'organisme du secteur public est établi.

cf. RGPD

La Banque centrale européenne et les organes de l'Union informent la Commission de leurs demandes.

3. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union ne met pas les données obtenues au titre du présent chapitre à disposition en vue de leur réutilisation au sens de l'article 2, point 2), du règlement (UE) 2022/868 ou de l'article 2, point 11), de la directive (UE) 2019/1024. Le règlement (UE) 2022/868 et la directive (UE) 2019/1024 ne s'appliquent pas aux données détenues par des organismes du secteur public obtenues au titre du présent chapitre.

4. Le paragraphe 3 du présent article n'empêche pas un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union d'échanger des données obtenues en vertu du présent chapitre avec un autre organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union en vue de l'accomplissement des tâches prévues à l'article 15, comme indiqué dans la demande conformément au paragraphe 1, point f), du présent article, ni de mettre les données à la disposition d'un tiers lorsqu'il ou elle a délégué, au moyen d'un accord accessible au public, des inspections techniques ou d'autres fonctions auprès de ce tiers. Les obligations incombant aux organismes du secteur public conformément à l'article 19, en particulier les garanties visant à préserver la confidentialité des secrets d'affaires, s'appliquent également à ces tiers. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union transmet ou met des données à disposition en vertu du présent paragraphe, il ou elle adresse une notification, sans retard injustifié, au détenteur de données auprès duquel les données ont été obtenues.

5. Lorsque le détenteur de données estime que ses droits au titre du présent chapitre ont été enfreints par la transmission ou la mise à disposition de données, il peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

6. La Commission élabore un modèle de demande conformément au présent article.

Article 18
Suivi des demandes de données

Suivi des demandes

1. Le détenteur de données qui reçoit une demande de mise à disposition de données au titre du présent chapitre met ces données à la disposition de l'organisme du secteur public demandeur, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union sans retard injustifié, en tenant compte des mesures techniques, organisationnelles et juridiques nécessaires.

2. Sans préjudice des besoins spécifiques concernant la disponibilité des données définis dans le droit de l'Union ou le droit national, un détenteur de données peut rejeter la demande de mise à disposition de données ou demander sa modification dans le cadre du présent chapitre, sans retard injustifié et, en tout état de cause, dans un délai maximal de cinq jours ouvrables suivant la réception d'une demande de données nécessaires pour réagir à une situation d'urgence, sans retard injustifié et, en tout état de cause, dans un délai maximal de trente jours ouvrables suivant la réception d'une telle demande dans les autres cas de besoin exceptionnel, pour l'un quelconque des motifs suivants:

a) le détenteur de données n'exerce pas de contrôle sur les données demandées;

b) une demande similaire a été présentée précédemment pour la même finalité par un autre organisme du secteur public ou la Commission, la Banque centrale européenne ou un organe de l'Union, et le détenteur de données ne s'est pas vu notifier l'effacement des données conformément à l'article 19, paragraphe 1, point c);

c) la demande ne satisfait pas aux conditions énoncées à l'article 17, paragraphes 1 et 2.

3. Si le détenteur de données décide de rejeter la demande ou de demander sa modification conformément au paragraphe 2, point b), il indique l'identité de l'organisme du secteur public ou de la Commission, de la Banque centrale européenne ou de l'organe de l'Union qui a présenté précédemment une demande pour la même finalité.

4. Lorsque les données demandées comprennent des données à caractère personnel, le détenteur de données anonymise correctement les données, à moins que le suivi de la demande de mettre des données à la disposition d'un organisme du secteur public, de la Commission, de la Banque centrale européenne ou d'un organe de l'Union n'exige la divulgation de données à caractère personnel. En pareils cas, le détenteur de données pseudonymise les données.

5. Lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union souhaite contester le refus d'un détenteur de données de fournir les données demandées, ou lorsque le détenteur de données souhaite contester la demande et que la question ne peut pas être résolue par une modification appropriée de la demande, la question est portée devant l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 19
Obligations des organismes du secteur public, de la Commission, de la Banque centrale européenne et des organes de l'Union

Obligations des organismes publics

1. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union qui reçoit des données à la suite d'une demande présentée en vertu de l'article 14:

a) n'utilise pas les données d'une manière incompatible avec la finalité pour laquelle elles ont été demandées;

b) a mis en œuvre des mesures techniques et organisationnelles qui préservent la confidentialité et l'intégrité des données demandées et la sécurité des transferts de données, en particulier en ce qui concerne les données à caractère personnel, et garantissent les droits et libertés des personnes concernées;

c) efface les données dès qu'elles ne sont plus nécessaires à la finalité indiquée et informe, sans retard injustifié, le détenteur de données ainsi que les personnes ou organisations qui ont reçu les données conformément à l'article 21, paragraphe 1, que les données ont été effacées, à moins que l'archivage des données ne soit requis conformément au droit de l'Union ou au droit national en matière d'accès du public aux documents dans le cadre des obligations de transparence.

2. Un organisme du secteur public, la Commission, la Banque centrale européenne, un organe de l'Union ou un tiers qui reçoit des données en vertu du présent chapitre ne peut pas:

a) utiliser les données ou les informations sur la situation économique, les actifs et les méthodes de production ou d'exploitation du détenteur de données pour développer ou améliorer un produit connecté ou un service connexe concurrençant le produit connecté ou le service connexe du détenteur de données;

b) partager les données avec un autre tiers pour l'une quelconque des finalités visées au point a).

3. La divulgation de secrets d'affaires à un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union n'est exigée que dans la mesure où elle est strictement nécessaire pour atteindre la finalité d'une demande présentée au titre de l'article 15. Dans ce cas, le détenteur de données ou, s'il ne s'agit pas de la même personne, le détenteur de secrets d'affaires détermine les données qui sont protégées en tant que secrets d'affaires, y compris dans les métadonnées pertinentes. L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union prend, avant la divulgation de secrets d'affaires, toutes les mesures techniques et organisationnelles nécessaires et appropriées pour préserver la confidentialité des secrets d'affaires, y compris, le cas échéant, l'utilisation de clauses contractuelles types et de normes techniques et l'application de codes de conduite.

4. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union est responsable de la sécurité des données qu'il ou elle reçoit.

Article 20
Compensation en cas de besoin exceptionnel

Compensation

1. Les détenteurs de données autres que les microentreprises et les petites entreprises mettent gratuitement à disposition les données nécessaires pour réagir à une situation d'urgence conformément à l'article 15, paragraphe 1, point a). L'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union qui a reçu des données accorde une reconnaissance publique au détenteur de données si celui-ci lui en fait la demande.

2. Le détenteur de données dispose d'un droit à une juste compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15, paragraphe 1, point b). Une telle compensation couvre les coûts techniques et organisationnels encourus pour donner suite à la demande, y compris, le cas échéant, les coûts d'anonymisation, de pseudonymisation, d'agrégation et d'adaptation technique, et une marge raisonnable. À la demande de l'organisme du secteur public, de la Commission, de la Banque centrale européenne ou de l'organe de l'Union, le détenteur de données fournit des informations sur la base du calcul des coûts et de la marge raisonnable.

3. Le paragraphe 2 s'applique également lorsqu'une microentreprise ou une petite entreprise demande une compensation pour la mise à disposition de données.

4. Les détenteurs de données ne sont pas habilités à recevoir une compensation pour la mise à disposition de données à la suite d'une demande présentée au titre de l'article 15, paragraphe 1, point b), lorsque la mission spécifique effectuée dans l'intérêt public consiste en la production de statistiques officielles et que l'achat de données n'est pas autorisé par le droit national. Les États membres adressent une notification à la Com-

mission lorsque le droit national n'autorise pas l'achat de données en vue de la production de statistiques officielles.

5. Lorsque l'organisme du secteur public, la Commission, la Banque centrale européenne ou l'organe de l'Union conteste le niveau de compensation demandé par le détenteur de données, il ou elle peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 21
Partage de données obtenues dans le cadre d'un besoin exceptionnel avec des organismes de recherche ou des organismes statistiques

Partage des données

1. Un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union a le droit de partager les données reçues au titre du présent chapitre:

a) avec des particuliers ou des organismes en vue de mener des travaux de recherche scientifique ou des analyses compatibles avec la finalité pour laquelle les données ont été demandées; ou

b) avec des instituts nationaux de statistique et Eurostat en vue de la production de statistiques officielles.

2. Les particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 agissent dans un but non lucratif ou dans le cadre d'une mission d'intérêt public reconnue par le droit de l'Union ou le droit national. Sont exclus les organismes sur lesquels des entreprises commerciales ont une influence significative, ce qui est susceptible de conduire à un accès préférentiel aux résultats des recherches.

3. Les particuliers ou les organismes qui reçoivent les données en vertu du paragraphe 1 du présent article se conforment aux mêmes obligations que celles qui sont applicables aux organismes du secteur public, à la Commission, à la Banque centrale européenne ou aux organes de l'Union au titre de l'article 17, paragraphe 3, et de l'article 19.

4. Nonobstant l'article 19, paragraphe 1, point c), les personnes ou organismes qui reçoivent les données en vertu du paragraphe 1 du présent article peuvent conserver les données reçues pour la finalité pour laquelle elles ont été demandées pendant une période maximale de six mois après leur effacement par les organismes du secteur public, la Commission, la Banque centrale européenne et les organes de l'Union.

5. Lorsqu'un organisme du secteur public, la Commission, la Banque centrale européenne ou un organe de l'Union a l'intention de transmettre ou de mettre à disposition des données au titre du paragraphe 1 du présent article, il ou elle adresse une notification sans retard injustifié au détenteur de données dont émanent les données reçues, en précisant l'identité et les coordonnées de l'organisme ou du particulier destinataire des données, la finalité de la transmission ou de la mise à disposition des données, la période pendant laquelle les données doivent être utilisées et les mesures de protection techniques et organisationnelles prises, y compris lorsque des données à caractère personnel ou des secrets d'affaires sont concernés. Lorsque le détenteur de données conteste la transmission ou la mise à disposition de données, il peut introduire une réclamation auprès de l'autorité compétente désignée en vertu de l'article 37 de l'État membre dans lequel le détenteur de données est établi.

Article 22
Assistance mutuelle et coopération transfrontière

Coopération transfrontière

1. Les organismes du secteur public, la Commission, la Banque centrale européenne et les organes de l'Union coopèrent et se prêtent mutuellement assistance afin de mettre en œuvre le présent chapitre de manière cohérente.

2. Les données échangées dans le cadre de la demande d'assistance et fournies en vertu du paragraphe 1 ne sont pas utilisées d'une manière incompatible avec la finalité pour laquelle elles ont été demandées.

3. Lorsqu'un organisme du secteur public a l'intention de demander des données à un détenteur de données établi dans un autre État membre, il notifie d'abord cette intention à l'autorité compétente désignée en vertu de l'article 37 dans ledit État membre. Cette exigence s'applique également aux demandes adressées par la Commission, la Banque centrale européenne et les organes de l'Union. La demande est examinée par l'autorité compétente de l'État membre dans lequel le détenteur de données est établi.

4. Après avoir examiné la demande à la lumière des exigences prévues à l'article 17, l'autorité compétente concernée prend, sans retard injustifié, l'une des mesures suivantes:

a) transmettre la demande au détenteur de données et, le cas échéant, informer l'organisme du secteur public demandeur, la Commission, la Banque centrale européenne ou l'organe de l'Union de la nécessité, le cas échéant, de coopérer avec les organismes du secteur public de l'État membre dans lequel le détenteur de données est établi, dans le but de réduire la charge administrative pesant sur le détenteur de données qui donne suite à la demande;

b) rejeter la demande pour des motifs dûment étayés, conformément au présent chapitre.

L'organisme du secteur public demandeur, la Commission, la Banque centrale européenne et l'organe de l'Union tiennent compte de l'avis de l'autorité compétente concernée et des motifs avancés par l'autorité compétente concernée en vertu du premier alinéa avant de prendre une quelconque mesure, comme soumettre à nouveau la demande, le cas échéant.

CHAPITRE VI
CHANGEMENT DE SERVICES DE TRAITEMENT DE DONNEES

Changement de services de traitement de données

Article 23
Suppression des obstacles à un changement de fournisseur effectif

Suppression des obstacles

Les fournisseurs de services de traitement de données prennent les mesures prévues aux articles 25, 26, 27, 29 et 30 afin de permettre aux clients de changer de fournisseur pour passer à un service de traitement de données, couvrant le même type de service, qui est fourni par un fournisseur de services de traitement de données différent, ou passer à une infrastructure TIC sur site, ou, le cas échéant, recourir simultanément à plusieurs fournisseurs de services de traitement de données. En particulier, les fournisseurs de services de traitement de données n'imposent pas d'obstacles et suppriment les obstacles précommerciaux, commerciaux, techniques, contractuels et organisationnels, qui freinent les clients dans les démarches suivantes:

a) la résiliation, après le préavis maximal et l'achèvement avec succès du processus de changement de fournisseur, conformément à l'article 25, du contrat portant sur le service de traitement de données;

b) la conclusion de nouveaux contrats avec un fournisseur de services de traitement de données différent couvrant le même type de service;

c) le portage des données exportables et des actifs numériques du client vers un fournisseur de services de traitement de données différent ou vers une infrastructure TIC sur site, y compris après avoir bénéficié d'une offre gratuite;

d) conformément à l'article 24, la réalisation de l'équivalence fonctionnelle lors de l'utilisation du nouveau service de traitement de données dans l'environnement TIC d'un fournisseur de services de traitement de données différent couvrant le même type de service;

e) le découplage, lorsqu'il est techniquement possible, des services de traitement de données visés à l'article 30, paragraphe 1, des autres services de traitement de données fournis par le fournisseur de services de traitement de données.

Article 24
Champ d'application des obligations techniques

Les responsabilités des fournisseurs de services de traitement de données définies aux articles 23, 25, 29, 30 et 34 ne s'appliquent qu'aux services, contrats ou pratiques commerciales du fournisseur d'origine de services de traitement de données.

Article 25
Clauses contractuelles concernant le changement de fournisseur

Clauses contractuelles

1. Les droits du client et les obligations du fournisseur de services de traitement de données dans le cadre d'un changement de fournisseur entre des fournisseurs de ces services ou, le cas échéant, le passage à une infrastructure TIC sur site sont clairement énoncés dans un contrat écrit. Le fournisseur de services de traitement de données met le contrat à la disposition du client avant la signature du contrat d'une manière qui permet à ce dernier de le stocker et de le reproduire.

2. Sans préjudice de la directive (UE) 2019/770, le contrat visé au paragraphe 1 du présent article comporte au moins les éléments suivants:

a) des clauses permettant au client, sur demande, de passer à un service de traitement de données proposé par un fournisseur de services de traitement de données différent ou de porter toutes les données exportables et tous les actifs numériques vers une infrastructure TIC sur site, sans retard injustifié et, en tout état de cause, pas après la période transitoire maximale obligatoire de trente jours calendaires prenant effet au terme du délai de préavis maximal visé au point d), période pendant laquelle le contrat de fourniture de service reste applicable et durant laquelle le fournisseur de services de traitement de données:

i) fournit une assistance raisonnable au client et aux tiers autorisés par le client dans le cadre du processus de changement de fournisseur;

ii) agit avec la diligence requise pour maintenir la continuité des activités et poursuivre la fourniture des fonctions ou services au titre du contrat;

iii) fournit des informations claires sur les risques connus, qui relèvent du fournisseur d'origine de services de traitement de données, pour la continuité de la fourniture des fonctions ou services;

iv) veille à ce qu'un niveau élevé de sécurité soit maintenu tout au long du processus de changement de fournisseur, en particulier en ce qui concerne la sécurité des données pendant leur transfert et le maintien de la sécurité des données pendant la période de récupération indiquée au point g), conformément au droit de l'Union ou au droit national applicables;

b) une obligation pour le fournisseur de services de traitement de données de concourir à la stratégie de sortie du client concernant les services couverts par le contrat, y compris en communiquant toutes les informations pertinentes;

c) une clause précisant que le contrat est considéré comme étant résilié et que la résiliation est notifiée au client dans l'un des cas suivants:

i) le cas échéant, lorsque le processus de changement de fournisseur est achevé avec succès;

ii) au terme du délai de préavis maximal visé au point d), lorsque le client ne souhaite pas changer de fournisseur mais souhaite effacer ses données exportables et actifs numériques lors de la résiliation du service;

d) un délai de préavis maximal pour le lancement du processus de changement de fournisseur, qui ne dépasse pas deux mois;

e) une spécification exhaustive de toutes les catégories de données et d'actifs numériques qui peuvent être portées pendant le processus de changement de fournisseur, y compris, au minimum, toutes les données exportables;

f) une spécification exhaustive des catégories de données spécifiques au fonctionnement interne du service de traitement de données du fournisseur qui doivent être exclues des données exportables au titre du point e) du présent paragraphe lorsqu'il existe un risque de violation des secrets d'affaires du fournisseur, à condition que ces exclusions n'entravent ni ne retardent le processus de changement de fournisseur prévu à l'article 23;

g) une période minimale d'au moins trente jours calendaires pour la récupération des données, débutant après la fin de la période transitoire convenue entre le client et le fournisseur de services de traitement de données, conformément au point a) du présent paragraphe et au paragraphe 4;

h) une clause garantissant l'effacement intégral de toutes les données exportables et de tous les actifs numériques générés directement par le client, ou se rapportant directement au client, après l'expiration de la période de récupération visée au point g) ou après l'expiration d'une autre période convenue à une date postérieure à la date d'expiration de la période de récupération visée au point g), à condition que le processus de changement de fournisseur soit achevé avec succès;

i) les frais de changement de fournisseur pouvant être facturés par les fournisseurs de services de traitement de données conformément à l'article 29.

3. Le contrat visé au paragraphe 1 comprend notamment des clauses prévoyant que le client peut notifier au fournisseur de services de traitement de données sa décision de prendre une ou plusieurs des mesures suivantes à la fin du délai de préavis maximal visé au paragraphe 2, point d):

a) passer à un fournisseur de services de traitement de données différent, auquel cas le client fournit les renseignements nécessaires concernant ce fournisseur;

b) passer à une infrastructure TIC sur site;

c) effacer ses données exportables et ses actifs numériques.

4. Lorsqu'il est techniquement impossible de respecter la période transitoire maximale obligatoire prévue au paragraphe 2, point a), le fournisseur de services de traitement de données en informe le client dans un délai de quatorze jours ouvrables à compter de la présentation de la demande de changement de fournisseur, motive dûment l'impossibilité technique et indique une autre période transitoire, qui ne peut excéder sept mois. Conformément au paragraphe 1, la continuité du service est assurée tout au long de l'autre période transitoire.

5. Sans préjudice du paragraphe 4, le contrat visé au paragraphe 1 contient des clauses accordant au client le droit de prolonger la période transitoire une fois pour une durée que le client juge plus appropriée à ses propres fins.

Article 26
Obligation d'information incombant aux fournisseurs de services de traitement de données

Obligation d’information des fournisseurs

Le fournisseur de services de traitement de données fournit au client:

a) des informations sur les procédures disponibles pour le changement de fournisseur et le portage vers le service de traitement de données, y compris des informations sur les méthodes et formats de changement de fournisseur et de portage disponibles, ainsi que sur les restrictions et les limitations techniques connues du fournisseur de services de traitement de données;

b) une référence à un registre en ligne à jour et hébergé par le fournisseur de services de traitement de données, avec des informations détaillées sur toutes les structures de données et tous les formats de données ainsi que les normes pertinentes et les spécifications d'interopérabilité ouvertes, dans lequel les données exportables visées à l'article 25, paragraphe 2, point e), sont disponibles.

Article 27
Obligation de bonne foi

Toutes les parties impliquées, y compris les fournisseurs de destination de services de traitement de données, coopèrent de bonne foi pour rendre le processus de changement de fournisseur effectif, permettre le transfert en temps utile des données et maintenir la continuité du service de traitement de données.

Article 28
Obligations contractuelles en matière de transparence concernant l'accès et le transfert internationaux

1. Les fournisseurs de services de traitement de données mettent à disposition et tiennent à jour sur leur site internet les informations suivantes:

a) les juridictions dont dépend l'infrastructure TIC déployée pour le traitement des données de leurs différents services;

b) une description générale des mesures techniques, organisationnelles et contractuelles adoptées par le fournisseur de services de traitement de données afin d'empêcher l'accès international des autorités publiques aux données à caractère non personnel détenues dans l'Union ou le transfert international de ces données lorsque cet accès ou ce transfert risque d'être en conflit avec le droit de l'Union ou le droit de l'État membre concerné.

2. Les sites internet visés au paragraphe 1 sont énumérés dans les contrats concernant tous les services de traitement de données proposés par les fournisseurs de services de traitement de données.

Article 29
Suppression progressive des frais de changement de fournisseur

Suppression des frais de changement de fournisseur

1. À compter du 12 janvier 2027, les fournisseurs de services de traitement de données ne peuvent imposer aucun frais de changement de fournisseur au client pour le processus de changement de fournisseur.

2. À compter du 11 janvier 2024 et jusqu'au 12 janvier 2027, les fournisseurs de services de traitement de données peuvent imposer des frais de changement de fournisseur réduits au client, pour le processus de changement de fournisseur.

3. Les frais de changement de fournisseur réduits visés au paragraphe 2 ne dépassent pas les coûts supportés par le fournisseur de services de traitement de données qui sont directement liés au processus de changement de fournisseur concerné.

4. Avant de conclure un contrat avec un client, les fournisseurs de services de traitement de données fournissent au client potentiel des informations claires sur les frais de service standard et les pénalités liées à la résiliation anticipée qui pourraient lui être facturés, ainsi que sur les frais de changement de fournisseur réduits qui pourraient lui être facturés pendant le délai visé au paragraphe 2.

5. Le cas échéant, les fournisseurs de services de traitement de données communiquent à un client des informations sur les services de traitement de données pour lesquels un changement de fournisseur est très complexe ou coûteux ou pour lesquels il est impossible de changer de fournisseur sans qu'il y ait une interférence significative portant sur les données, les actifs numériques ou l'architecture des services.

6. Le cas échéant, les fournisseurs de services de traitement de données mettent les informations visées aux paragraphes 4 et 5 à la disposition des clients publiquement au travers d'une section spécifique de leur site internet ou par tout autre moyen facilement accessible.

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 45 pour compléter le présent règlement en mettant en place un mécanisme de suivi permettant à la Commission de suivre les frais de changement de fournisseur imposés par les fournisseurs de services de traitement de données sur le marché afin de garantir que la suppression et la réduction des frais de changement de fournisseur en vertu des

paragraphes 1 et 2 du présent article sont réalisées dans les délais prévus aux mêmes paragraphes.

Article 30
Aspects techniques du changement de fournisseur

Aspects techniques

1. Les fournisseurs de services de traitement de données qui concernent des ressources informatiques modulables et variables limitées à des éléments d'infrastructure tels que les serveurs, les réseaux et les ressources virtuelles nécessaires à l'exploitation de l'infrastructure, sans donner accès aux services, logiciels et applications d'exploitation qui sont stockés, autrement traités ou déployés sur ces éléments d'infrastructure, prennent, conformément à l'article 27, toutes les mesures raisonnables en leur pouvoir afin de faciliter une équivalence fonctionnelle pour le client dans l'utilisation du service de traitement de données de destination, après qu'il soit passé à un service couvrant le même type de service. Le fournisseur d'origine de services de traitement de données facilite le processus de changement de fournisseur en fournissant des capacités, les informations adéquates, de la documentation, une assistance technique et, le cas échéant, les outils nécessaires.

2. Les fournisseurs de services de traitement de données, autres que ceux visés au paragraphe 1, mettent gratuitement et dans la même mesure à la disposition de tous leurs clients et des fournisseurs de destination de services de traitement de données concernés des interfaces ouvertes afin de faciliter le processus de changement de fournisseur. Ces interfaces contiennent des informations suffisantes sur le service concerné pour permettre le développement de logiciels capables de communiquer avec les services, aux fins de la portabilité et de l'interopérabilité des données.

3. Pour les services de traitement de données autres que ceux visés au paragraphe 1 du présent article, les fournisseurs de services de traitement de données assurent la compatibilité avec les spécifications communes fondées sur des spécifications d'interopérabilité ouvertes ou les normes harmonisées d'interopérabilité au moins douze mois après que les références à ces spécifications communes ou à ces normes harmonisées pour l'interopérabilité des services de traitement des données ont été publiées dans le répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données à la suite de la publication des actes d'exécution sous-jacents au Journal officiel de l'Union européenne conformément à l'article 35, paragraphe 8.

4. Les fournisseurs de services de traitement de données autres que ceux visés au paragraphe 1 du présent article mettent à jour le registre en ligne visé à l'article 26, point b), conformément aux obligations qui leur incombent au titre du paragraphe 3 du présent article.

5. En cas de changement de services du même type de service, pour lequel des spécifications communes ou des normes harmonisées pour l'interopérabilité visées au paragraphe 3 du présent article n'ont pas été publiées dans le répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données conformément à l'article 35, paragraphe 8, le fournisseur des services de traitement de données exporte, à la demande du client, toutes les données exportables, dans un format structuré, couramment utilisé et lisible par machine.

6. Les fournisseurs de services de traitement de données ne sont pas tenus de développer de nouvelles technologies ou de nouveaux services, ou de divulguer ou transférer des actifs numériques qui sont protégés par des droits de propriété intellectuelle ou qui constituent un secret d'affaires, à un client ou à un fournisseur de services de traitement de données différent ou de compromettre la sécurité et l'intégrité du service du client ou du fournisseur.

Article 31
Régime spécifique applicable à certains services de traitement de données

Cas particuliers

1. Les obligations prévues à l'article 23, point d), à l'article 29 et à l'article 30, paragraphes 1 et 3, ne s'appliquent pas aux services de traitement de données dont la majorité des caractéristiques principales ont été conçues sur mesure pour répondre aux besoins spécifiques d'un client particulier ou dont tous les composants ont été développés pour les besoins d'un client particulier, et lorsque ces services de traitement de

données ne sont pas proposés à grande échelle sur le plan commercial par l'intermédiaire du catalogue de services du fournisseur de services de traitement de données.

2. Les obligations prévues dans le présent chapitre ne s'appliquent pas aux services de traitement de données fournis en tant que version non destinée à la production à des fins d'essai et d'évaluation et pour une durée limitée.

3. Avant la conclusion d'un contrat pour la fourniture de services de traitement de données visés au présent article, le fournisseur de services de traitement de données informe le client potentiel des obligations énoncées au présent chapitre qui ne s'appliquent pas.

CHAPITRE VII
ACCES INTERNATIONAL ILLICITE AUX DONNEES A CARACTERE NON PERSONNEL ET TRANSFERT INTERNATIONAL ILLICITE DE CES DONNEES PAR LES AUTORITES PUBLIQUES

Accès international illicite

Article 32
Accès et transfert internationaux par les autorités publiques

1. Les fournisseurs de services de traitement de données prennent toutes les mesures techniques, organisationnelles et juridiques adéquates, y compris des contrats, afin d'empêcher l'accès international des autorités publiques et l'accès des autorités publiques des pays tiers aux données à caractère non personnel détenues dans l'Union et le transfert de ces données lorsque ce transfert ou cet accès risque d'être en conflit avec le droit de l'Union ou le droit national de l'État membre concerné, sans préjudice du paragraphe 2 ou 3.

2. Toute décision ou tout jugement d'une juridiction d'un pays tiers et toute décision d'une autorité administrative d'un pays tiers exigeant d'un fournisseur de services de traitement de données qu'il transfère des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou qu'il donne accès à ces données ne sont reconnus ou rendus exécutoires de quelque manière que ce soit que s’ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union, ou tout accord de ce type entre le pays tiers demandeur et un État membre.

3. En l'absence d'un accord international tel qu'il est visé au paragraphe 2, lorsqu'un fournisseur de services de traitement de données est destinataire d'une décision ou d'un jugement d'une juridiction d'un pays tiers ou d'une décision d'une autorité administrative d'un pays tiers imposant de transférer des données à caractère non personnel relevant du champ d'application du présent règlement et détenues dans l'Union ou d'y donner accès, et lorsque le respect d'une telle décision risquerait de mettre le destinataire en conflit avec le droit de l'Union ou avec le droit national de l'État membre concerné, le transfert de ces données vers cette autorité d'un pays tiers ou l'accès à ces données par cette même autorité n'a lieu que s'il est satisfait aux conditions suivantes:

a) le système du pays tiers exige que les motifs et la proportionnalité d'une telle décision ou d'un tel jugement soient exposés et que cette décision ou ce jugement revête un caractère spécifique, par exemple en établissant un lien suffisant avec certains suspects ou avec des infractions;

b) l'objection motivée du destinataire fait l'objet d'un examen par une juridiction compétente du pays tiers; et

c) la juridiction compétente d'un pays tiers qui rend la décision ou le jugement ou qui contrôle la décision d'une autorité administrative est habilitée, en vertu du droit de ce pays tiers, à prendre dûment en compte les intérêts juridiques concernés du fournisseur des données protégées par le droit de l'Union ou par le droit national de l'État membre concerné.

Le destinataire de la décision ou du jugement peut solliciter l'avis de l'autorité nationale ou de l'organisme national concernés compétents pour la coopération internatio-

nale en matière juridique, afin de déterminer si les conditions prévues au premier alinéa sont remplies, notamment lorsqu'il estime que la décision peut concerner des secrets d'affaires et d'autres données commercialement sensibles ainsi que du contenu protégé par des droits de propriété intellectuelle, ou que le transfert peut donner lieu à une réidentification. L'autorité nationale ou l'organisme national concernés peut consulter la Commission. Si le destinataire estime que la décision ou le jugement est susceptible de porter atteinte aux intérêts de l'Union ou de ses États membres en matière de sécurité nationale ou de défense, il demande l'avis de l'autorité nationale ou de l'organisme national concernés afin de déterminer si les données demandées concernent les intérêts de l'Union ou de ses États membres en matière de sécurité nationale ou de défense. Si le destinataire n'a pas reçu de réponse dans un délai d'un mois, ou si cette autorité ou cet organisme conclut dans son avis que les conditions prévues au premier alinéa ne sont pas remplies, le destinataire peut, pour ces motifs, rejeter la demande de transfert de données à caractère non personnel ou d'accès à de telles données.

Le comité européen de l'innovation dans le domaine des données visé à l'article 42 conseille et assiste la Commission dans l'élaboration de lignes directrices relatives à l'évaluation du respect des conditions prévues au premier alinéa du présent paragraphe.

4. Si les conditions énoncées au paragraphe 2 ou 3 sont remplies, le fournisseur de services de traitement de données fournit le volume minimal de données admissible en réponse à une demande, sur la base de l'interprétation que peut raisonnablement donner de cette demande le fournisseur ou l'autorité nationale ou l'organisme national concernés visés au paragraphe 3, deuxième alinéa.

5. Le fournisseur de services de traitement de données informe le client de l'existence d'une demande d'accès à des données le concernant qui émane d'une autorité d'un pays tiers avant de donner suite à cette demande, sauf lorsque cette demande sert des fins répressives et aussi longtemps que cela est nécessaire pour préserver l'efficacité de l'action répressive.

CHAPITRE VIII
INTEROPERABILITE

Interopérabilité

Article 33
Exigences essentielles concernant l'interopérabilité des données, des mécanismes et des services de partage des données ainsi que des espaces européens communs de données

1. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants respectent les exigences essentielles suivantes en vue de faciliter l'interopérabilité des données, des mécanismes et des services de partage de données, ainsi que des espaces européens communs des données qui sont des cadres interopérables de normes et de pratiques communes transsectoriels ou spécifiques à chaque finalité ou à chaque secteur visant à partager ou à traiter conjointement des données pour, entre autres, la mise au point de nouveaux produits et services, la recherche scientifique ou des initiatives de la société civile:

a) le contenu de l'ensemble de données, les restrictions d'utilisation, les licences, la méthode de collecte des données, la qualité des données et l'incertitude sur les données sont suffisamment décrits, le cas échéant, dans un format lisible par machine, pour permettre au destinataire de trouver les données, d'y accéder et de les utiliser;

b) les structures de données, les formats de données, les vocabulaires, les systèmes de classification, les taxinomies et les listes de codes, le cas échéant, sont décrits de manière publiquement accessible et cohérente;

c) les moyens techniques d'accès aux données, tels que les interfaces de programmation d'applications, ainsi que leurs conditions d'utilisation et leur qualité de service sont suffisamment décrits pour permettre l'accès automatique aux données et leur transmission automatique entre les parties, y compris en continu, en téléchargement de masse ou en temps réel dans un format lisible par machine, lorsque cela est techniquement possible et n'entrave pas le bon fonctionnement du produit connecté;

d) le cas échéant, les moyens permettant l'interopérabilité des outils d'exécution automatique des accords de partage de données, tels que les contrats intelligents, sont prévus.

Ces exigences peuvent être de nature générique ou concerner des secteurs spécifiques, tout en tenant pleinement compte de l'interdépendance avec les exigences découlant d'autres dispositions du droit de l'Union ou du droit national.

2. La Commission est habilitée à adopter des actes délégués conformément à l'article 45 du présent règlement afin de compléter le présent règlement en précisant davantage les exigences essentielles prévues au paragraphe 1 du présent article, en ce qui concerne les exigences qui, par leur nature, ne peuvent produire l'effet escompté que si elles sont précisées davantage dans des actes juridiques contraignants de l'Union, et afin de refléter correctement l'évolution des technologies et du marché.

Lorsqu'elle adopte des actes délégués, la Commission tient compte des avis du comité européen de l'innovation dans le domaine des données conformément à l'article 42, point c), iii).

3. Les participants aux espaces de données qui proposent des données ou des services de données à d'autres participants aux espaces de données qui satisfont aux normes harmonisées ou à des parties de normes harmonisées, dont les références sont publiées au Journal officiel de l'Union européenne, sont présumés être en conformité avec les exigences essentielles prévues au paragraphe 1, dans la mesure où ces exigences sont couvertes par de telles normes harmonisées ou des parties de ces normes.

4. En application de l'article 10 du règlement (UE) no 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles prévues au paragraphe 1 du présent article.

5. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes couvrant l'une ou l'ensemble des exigences essentielles prévues au paragraphe 1 lorsque les conditions suivantes sont remplies:

a) la Commission a demandé, conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012, à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée qui satisfait aux exigences essentielles prévues au paragraphe 1 du présent article et:

i) la demande n'a pas été acceptée;

ii) les normes harmonisées répondant à cette demande ne sont pas fournies dans le délai déterminé conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012; ou

iii) les normes harmonisées ne répondent pas à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences essentielles pertinentes prévues au paragraphe 1 du présent article n'est publiée au Journal officiel de l'Union européenne conformément au règlement (UE) no 1025/2012 et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

6. Avant de préparer un projet d'acte d'exécution visé au paragraphe 5 du présent article, la Commission informe le comité visé à l'article 22 du règlement (UE) no 1025/2012 qu'elle estime que les conditions énoncées au paragraphe 5 du présent article ont été remplies.

7. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 5, la Commission tient compte de l'avis du comité européen de l'innovation dans le domaine des données et du point de vue d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

8. Les participants aux espaces de données qui proposent des données ou des services de données aux autres participants aux espaces de données qui satisfont aux spécifications communes établies par des actes d'exécution visés au paragraphe 5 ou à des parties de celles-ci sont présumés être en conformité avec les exigences essentielles prévues au paragraphe 1 dans la mesure où ces exigences sont couvertes par de telles spécifications communes ou des parties de celles-ci.

9. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au Journal officiel de l'Union européenne, la Commission évalue la norme harmonisée conformément au règlement (UE) no 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au Journal officiel de l'Union européenne, la Commission abroge les actes d'exécution visés au paragraphe 5 du présent article, ou les parties de ces actes qui couvrent les mêmes exigences essentielles que celles couvertes par ladite norme harmonisée.

10. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues au paragraphe 1, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue cette explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

11. La Commission peut adopter des lignes directrices en tenant compte de la proposition du comité européen de l'innovation dans le domaine des données conformément à l'article 30, point h), du règlement (UE) 2022/868 établissant des cadres interopérables pour les normes et pratiques communes pour le fonctionnement des espaces européens communs des données.

Article 34
Interopérabilité aux fins de l'utilisation simultanée de services de traitement de données

1. Les exigences prévues à l'article 23, à l'article 24, à l'article 25, paragraphe 2, points a) ii), a) iv), e) et f), et à l'article 30, paragraphes 2 à 5, s'appliquent également mutatis mutandis aux fournisseurs de services de traitement de données pour faciliter l'interopérabilité aux fins de l'utilisation simultanée de services de traitement de données.

2. Lorsqu'un service de traitement de données et un autre service de traitement de données sont utilisés simultanément, les fournisseurs de services de traitement de données peuvent imposer des frais de transfert des données, mais seulement aux fins de répercuter les coûts de sortie occasionnés, sans dépasser de tels coûts.

Article 35
Interopérabilité des services de traitement de données

1. Les spécifications d'interopérabilité ouvertes et les normes harmonisées pour l'interopérabilité des services de traitement de données:

a) réalisent, lorsque cela est techniquement possible, l'interopérabilité entre différents services de traitement de données couvrant le même type de service;

b) améliorent la portabilité des actifs numériques entre différents services de traitement de données couvrant le même type de service;

c) facilitent, lorsque cela est techniquement possible, l'équivalence fonctionnelle entre différents services de traitement de données visés à l'article 30, paragraphe 1, couvrant le même type de service;

d) ne portent pas atteinte à la sécurité et à l'intégrité des services de traitement des données et des données;

e) sont conçues de manière à permettre des avancées techniques et l'inclusion de nouvelles fonctions et innovations dans les services de traitement de données.

2. Les spécifications d'interopérabilité ouvertes et les normes harmonisées pour l'interopérabilité des services de traitement de données couvrent de manière appropriée:

a) les aspects de l'interopérabilité de l'informatique en nuage qui concernent l'interopérabilité du transport, l'interopérabilité syntactique, l'interopérabilité sémantique des données, l'interopérabilité comportementale et l'interopérabilité du cadre normatif;

b) les aspects de la portabilité des données en nuage pour la portabilité syntactique des données, la portabilité sémantique des données et la portabilité stratégique des données;

c) les aspects applicatifs de l'informatique en nuage qui concernent la portabilité syntactique des applications, la portabilité des instructions des applications, la portabilité des métadonnées des applications, la portabilité comportementale des applications et la portabilité stratégique des applications.

3. Les spécifications d'interopérabilité ouvertes sont conformes à l'annexe II du règlement (UE) no 1025/2012.

4. Après avoir tenu compte des normes internationales et européennes pertinentes ainsi que des initiatives d'autorégulation, la Commission peut, conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012, demander à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles prévues aux paragraphes 1 et 2 du présent article.

5. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes fondées sur des spécifications d'interopérabilité ouvertes couvrant toutes les exigences essentielles prévues aux paragraphes 1 et 2.

6. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 5 du présent article, la Commission tient compte du point de vue des autorités compétentes visées à l'article 37, paragraphe 5, point h), et d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

7. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues aux paragraphes 1 et 2, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue cette explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

8. Aux fins de l'article 30, paragraphe 3, la Commission publie, par voie d'actes d'exécution, les références des normes harmonisées et des spécifications communes pour l'interopérabilité des services de traitement de données dans un répertoire central des normes de l'Union pour l'interopérabilité des services de traitement de données.

9. Les actes d'exécution visés au présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

Article 36
Exigences essentielles concernant les contrats intelligents pour l'exécution des accords de partage de données

Contrats intelligents pour le partage de données

1. Le vendeur d'une application utilisant des contrats intelligents ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données, veille à ce que ces contrats intelligents respectent les exigences essentielles suivantes:

a) robustesse et contrôle de l'accès, pour veiller à ce que le contrat intelligent ait été conçu de manière à offrir des mécanismes de contrôle d'accès et un degré très élevé de robustesse afin d'éviter des erreurs fonctionnelles et de résister aux tentatives de manipulation par des tiers;

b) résiliation et interruption en toute sécurité, pour veiller à ce qu'il existe un mécanisme permettant de mettre fin à l'exécution continue des transactions et à ce que le

contrat intelligent intègre des fonctions internes qui peuvent réinitialiser le contrat ou lui donner instruction de cesser ou d'interrompre l'opération, en particulier pour éviter de futures exécutions accidentelles;

c) archivage et continuité des données, pour garantir, dans les circonstances dans lesquelles un contrat intelligent doit être résilié ou désactivé, qu'il y a la possibilité d'archiver les données relatives aux transactions, la logique et le code du contrat intelligent afin de conserver l'enregistrement des opérations effectuées sur les données dans le passé (vérifiabilité);

d) contrôle de l'accès, pour garantir qu'un contrat intelligent est protégé par des mécanismes rigoureux de contrôle d'accès au niveau de la gouvernance et des contrats intelligents; et

e) cohérence, pour assurer la cohérence avec les dispositions de l'accord de partage de données que le contrat intelligent exécute.

2. Le vendeur d'un contrat intelligent ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données, procède à une évaluation de la conformité en vue de satisfaire aux exigences essentielles prévues au paragraphe 1 et, en ce qui concerne le respect de ces exigences, délivre une déclaration UE de conformité.

3. Lorsqu'il établit la déclaration UE de conformité, le vendeur d'une application utilisant des contrats intelligents ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données est responsable du respect des exigences essentielles prévues au paragraphe 1.

4. Un contrat intelligent qui satisfait aux normes harmonisées ou aux parties concernées de celles-ci et dont les références sont publiées au Journal officiel de l'Union européenne est présumé être en conformité avec les exigences essentielles prévues au paragraphe 1, dans la mesure où ces exigences sont couvertes par de telles normes harmonisées ou des parties de celles-ci.

5. Conformément à l'article 10 du règlement (UE) no 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont aux exigences essentielles prévues au paragraphe 1 du présent article.

6. La Commission peut, par voie d'actes d'exécution, adopter des spécifications communes couvrant l'une ou l'ensemble des exigences essentielles prévues au paragraphe 1 lorsque les conditions suivantes sont remplies:

a) la Commission a demandé, conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012, à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée qui satisfait aux exigences essentielles prévues au paragraphe 1 du présent article et:

i) la demande n'a pas été acceptée;

ii) les normes harmonisées répondant à cette demande n'ont pas été fournies dans le délai déterminé conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012; ou

iii) les normes harmonisées ne répondent pas à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences essentielles pertinentes prévues au paragraphe 1 du présent article n'est publiée au Journal officiel de l'Union européenne conformément au règlement (UE) no 1025/2012 et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 46, paragraphe 2.

7. Avant de préparer un projet d'acte d'exécution visé au paragraphe 6 du présent article, la Commission informe le comité visé à l'article 22 du règlement (UE) no 1025/2012 qu'elle estime que les conditions prévues au paragraphe 6 du présent article ont été remplies.

8. Lorsqu'elle prépare le projet d'acte d'exécution visé au paragraphe 6, la Commission tient compte de l'avis du comité européen de l'innovation dans le domaine des données et du point de vue d'autres organismes ou groupes d'experts compétents et consulte dûment toutes les parties prenantes concernées.

9. Le vendeur d'un contrat intelligent ou, à défaut, la personne dont l'activité commerciale, l'entreprise ou la profession nécessite le déploiement de contrats intelligents pour des tiers dans le cadre de l'exécution d'un accord ou d'une partie d'un accord de mise à disposition des données qui sont conformes aux spécifications communes établies par des actes d'exécution visés au paragraphe 6, ou à des parties de celles-ci, est présumé respecter les exigences essentielles prévues au paragraphe 1 dans la mesure où ces exigences sont couvertes par de telles spécifications communes ou par des parties de celles-ci.

10. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au Journal officiel de l'Union européenne, la Commission évalue la norme harmonisée conformément au règlement (UE) no 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au Journal officiel de l'Union européenne, la Commission abroge les actes d'exécution visés au paragraphe 6 du présent article, ou des parties de ces actes qui couvrent les mêmes exigences essentielles que celles qui sont couvertes par ladite norme harmonisée.

11. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences essentielles prévues au paragraphe 1, il en informe la Commission en lui fournissant une explication détaillée. La Commission évalue ladite explication détaillée et peut, le cas échéant, modifier l'acte d'exécution établissant la spécification commune en question.

CHAPITRE IX
MISE EN ŒUVRE ET EXECUTION

Mise en œuvre

Article 37
Autorités compétentes et coordinateurs de données

1. Chaque État membre désigne une ou plusieurs autorités compétentes chargées de l'application et de l'exécution du présent règlement (ci-après dénommées "autorités compétentes"). Les États membres peuvent mettre en place une ou plusieurs nouvelles autorités ou s'appuyer sur des autorités existantes.

2. Lorsqu'un État membre désigne plus d'une autorité compétente, il désigne un coordinateur de données parmi celles-ci afin de faciliter la coopération entre les autorités compétentes et afin d'aider les entités relevant du champ d'application du présent règlement sur toutes les questions liées à son application et à son exécution. Les autorités compétentes coopèrent entre elles dans l'exercice des missions et pouvoirs qui leur sont conférés au titre du paragraphe 5.

cf. RGPD

3. Les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 sont chargées de surveiller l'application du présent règlement en ce qui concerne la protection des données à caractère personnel. Les chapitres VI et VII du règlement (UE) 2016/679 s'appliquent mutatis mutandis.

Rôle des autorités de contrôle et du CEPD/ EDPS

Le Contrôleur européen de la protection des données est chargé de surveiller l'application du présent règlement dans la mesure où il concerne la Commission, la Banque centrale européenne ou des organes de l'Union. Le cas échéant, l'article 62 du règlement (UE) 2018/1725 s'applique mutatis mutandis.

Les autorités de contrôle visées au présent paragraphe exercent leurs missions et leurs pouvoirs à l'égard du traitement des données à caractère personnel.

4. Sans préjudice du paragraphe 1 du présent article:

a) pour les questions spécifiques sur l'accès aux données sectorielles et leur utilisation en lien avec l'application du présent règlement, la compétence des autorités sectorielles est respectée;

b) l'autorité compétente chargée de l'application et de l'exécution des articles 23 à 31 et des articles 34 et 35 dispose d'une expérience dans le domaine des données et des services de communications électroniques.

5. Les États membres veillent à ce que les missions et pouvoirs des autorités compétentes soient clairement définis et incluent:

Missions et pouvoirs des autorités compétentes

a) la promotion de l'éducation aux données et la sensibilisation des utilisateurs et des entités relevant du champ d'application du présent règlement aux droits et obligations découlant du présent règlement;

b) le traitement des réclamations découlant des infractions alléguées au présent règlement, y compris en lien avec des secrets d'affaires, l'examen de l'objet de la réclamation, dans la mesure nécessaire, et l'information à intervalles réguliers de l'auteur de la réclamation, le cas échéant conformément au droit national, sur l'état d'avancement et l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité compétente est nécessaire;

c) la réalisation d'enquêtes sur des questions concernant l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité compétente ou d'une autre autorité publique;

d) l'imposition de sanctions financières effectives, proportionnées et dissuasives, pouvant comporter des astreintes et des sanctions avec effet rétroactif, ou l'engagement de procédures judiciaires en vue d'infliger des amendes;

e) le suivi des évolutions technologiques et commerciales pertinentes pour la mise à disposition et l'utilisation des données;

f) la coopération avec les autorités compétentes d'autres États membres, et, le cas échéant, avec la Commission ou le comité européen de l'innovation dans le domaine des données, pour garantir l'application cohérente et efficace du présent règlement, y compris l'échange de toutes les informations pertinentes par voie électronique, sans retard injustifié, y compris en ce qui concerne le paragraphe 10 du présent article;

g) la coopération avec les autorités compétentes concernées chargées de la mise en œuvre d'autres actes juridiques de l'Union ou nationaux, y compris avec les autorités compétentes dans le domaine des données et des services de communications électroniques, avec l'autorité de contrôle chargée de surveiller l'application du règlement (UE) 2016/679 ou avec les autorités sectorielles afin de veiller à ce que le présent règlement soit appliqué de manière cohérente par rapport aux autres dispositions du droit de l'Union et du droit national;

cf. RGPD

h) la coopération avec les autorités compétentes concernées afin de veiller à ce que les articles 23 à 31 et les articles 34 et 35 soient exécutées de manière cohérente par rapport au droit de l'Union et aux mesures d'autoréglementation applicables aux fournisseurs de services de traitement de données;

i) l'assurance que les frais de changement de fournisseur sont supprimés conformément à l'article 29;

j) l'examen des demandes de données introduites en application du chapitre V.

Lorsqu'un coordinateur de données a été désigné, il facilite la coopération visée aux points f), g) et h) du premier alinéa et assiste les autorités compétentes à leur demande.

6. Lorsqu'une telle autorité compétente a été désignée, le coordinateur de données:

a) fait office de point de contact unique pour toutes les questions liées à l'application du présent règlement;

b) veille à ce que soient mises à la disposition du public en ligne les demandes de mise à disposition des données présentées par des organismes du secteur public en cas de besoin exceptionnel au titre du chapitre V et encourage les accords de partage volontaire de données entre les organismes du secteur public et les détenteurs de données;

c) informe annuellement la Commission des refus notifiés au titre de l'article 4, paragraphes 2 et 8, et de l'article 5, paragraphe 11.

7. Les États membres communiquent à la Commission le nom des autorités compétentes ainsi que leurs missions et pouvoirs et, le cas échéant, le nom du coordinateur de données. La Commission tient un registre public de ces autorités.

8. Lorsqu'elles accomplissent leurs missions et exercent leurs pouvoirs conformément au présent règlement, les autorités compétentes restent impartiales et libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent, pour des cas individuels, d'instructions d'aucune autre autorité publique ni d'aucune entité privée.

9. Les États membres veillent à ce que les autorités compétentes disposent de ressources humaines et techniques suffisantes et de l'expertise adéquate pour s'acquitter efficacement de leurs missions conformément au présent règlement.

10. Les entités relevant du champ d'application du présent règlement sont soumises à la compétence de l'État membre dans lequel elles sont établies. Lorsque l'entité est établie dans plus d'un État membre, elle est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son établissement principal, c'est-à-dire là où l'entité a son siège social ou son siège statutaire d'où sont exercés les principales fonctions financières et le contrôle opérationnel.

11. Toute entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union et qui n'est pas établie dans l'Union désigne un représentant légal dans l'un des États membres.

12. Aux fins de garantir le respect du présent règlement, un représentant légal est mandaté par une entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union pour être contacté, en plus de ladite entité ou à sa place, par les autorités compétentes en ce qui concerne toutes les questions liées à cette entité. Ce représentant légal coopère avec les autorités compétentes et leur démontre de manière exhaustive, sur demande, les mesures prises et les dispositions mises en place par l'entité relevant du champ d'application du présent règlement qui met des produits connectés à disposition ou propose des services connexes dans l'Union pour garantir le respect du présent règlement.

13. Une entité relevant du champ d'application du présent règlement qui met à disposition des produits connectés ou propose des services dans l'Union est considérée comme relevant de la compétence de l'État membre dans lequel se trouve son représentant légal. La désignation d'un représentant légal par une telle entité est sans préjudice de la responsabilité de cette entité et des actions en justice qui pourraient être intentées contre elle. Jusqu'à ce qu'une entité désigne un représentant légal conformément au présent article, elle relève de la compétence de tous les États membres, le cas échéant, aux fins de garantir l'application et l'exécution du présent règlement. Toute autorité compétente peut exercer sa compétence, y compris en imposant des sanctions effectives, proportionnées et dissuasives, pour autant que l'entité ne fasse pas l'objet d'une procédure d'exécution au titre du présent règlement portant sur les mêmes faits par une autre autorité compétente.

14. Les autorités compétentes sont habilitées à demander aux utilisateurs, aux détenteurs de données ou aux destinataires de données, ou à leurs représentants légaux, qui relèvent de la compétence de leur État membre toutes les informations nécessaires pour vérifier le respect du présent règlement. Toute demande d'information est proportionnée à l'accomplissement de la mission sous-jacente et est motivée.

15. Lorsqu'une autorité compétente dans un État membre sollicite l'assistance d'une autorité compétente d'un autre État membre ou l'application de mesures d'exécution par celle-ci, elle présente une demande motivée. Lorsqu'elle reçoit une telle demande, une autorité compétente fournit, sans retard injustifié, une réponse détaillant les mesures qui ont été prises ou qu'il est prévu de prendre.

16. Les autorités compétentes respectent les principes de confidentialité et de secret professionnel et commercial et protègent les données à caractère personnel conformément au droit de l'Union ou au droit national. Toutes les informations échangées dans le cadre d'une demande d'assistance et fournies en vertu du présent article ne sont utilisées qu'aux fins pour lesquelles elles ont été demandées.

Article 38
Droit d'introduire une réclamation

Droit à réclamation

1. Sans préjudice de tout autre recours administratif ou juridictionnel, les personnes physiques et morales ont le droit d'introduire une réclamation, individuellement ou, le cas échéant, collectivement, auprès de l'autorité compétente concernée dans l'État membre dans lequel se trouve leur résidence habituelle, leur lieu de travail ou leur lieu d'établissement, si elles considèrent qu'il a été porté atteinte aux droits que leur confère le présent règlement. Le coordinateur de données fournit, sur demande, aux personnes physiques et morales toutes les informations nécessaires à l'introduction de leur réclamation auprès de l'autorité compétente concernée.

2. L'autorité compétente auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation, conformément au droit national, de l'état d'avancement de la procédure et de la décision prise.

3. Les autorités compétentes coopèrent pour gérer et traiter les réclamations de manière efficace et rapide, y compris en échangeant toutes les informations pertinentes par voie électronique, sans retard injustifié. Cette coopération n'affecte pas les mécanismes de coopération prévus aux chapitres VI et VII du règlement (UE) 2016/679 et ceux prévus par le règlement (UE) 2017/2394.

cf. RGPD

Article 39
Droit à un recours juridictionnel effectif

Droit au recours juridictionnel

1. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, toute personne physique ou morale lésée dispose du droit à un recours juridictionnel effectif en ce qui concerne les décisions juridiquement contraignantes prises par les autorités compétentes.

2. Lorsqu'une autorité compétente ne donne pas suite à une réclamation, toute personne physique ou morale lésée a, conformément au droit national, soit droit à un recours juridictionnel effectif, soit accès à un réexamen réalisé par un organe impartial doté des compétences appropriées.

3. Les actions intentées en vertu du présent article sont portées devant les juridictions de l'État membre de l'autorité compétente contre laquelle le recours juridictionnel a été formé individuellement ou, le cas échéant, collectivement par les représentants d'une ou de plusieurs personnes physiques ou morales.

Article 40
Sanctions

Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives.

2. Les États membres informent la Commission, au plus tard le 12 septembre 2025, du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures. La Commission tient et met à jour régulièrement un registre public facilement accessible de ces mesures.

3. Les États membres tiennent compte des recommandations du comité européen de l'innovation dans le domaine des données et des critères non exhaustifs suivants pour l'imposition de sanctions en cas de violation du présent règlement:

a) la nature, la gravité, l'ampleur et la durée de l'infraction;

b) toute mesure prise par l'auteur de l'infraction pour atténuer ou réparer le préjudice causé par l'infraction;

c) toute infraction antérieure commise par l'auteur de l'infraction;

d) les avantages financiers obtenus ou les pertes évitées par l'auteur de l'infraction en raison de l'infraction, si ces avantages ou pertes peuvent être établis de manière fiable;

e) toute autre circonstance aggravante ou atténuante applicable au cas concerné;

f) le chiffre d'affaires annuel réalisé par l'auteur de l'infraction au cours de l'exercice précédent dans l'Union.

4. En ce qui concerne les infractions aux obligations prévues aux chapitres II, III et V du présent règlement, les autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 peuvent, dans les limites de leur compétence, imposer des amendes administratives conformément à l'article 83 du règlement (UE) 2016/679, jusqu'à concurrence du montant visé à l'article 83, paragraphe 5, dudit règlement.

cf. RGPD

5. En ce qui concerne les infractions aux obligations prévues au chapitre V du présent règlement, le Contrôleur européen de la protection des données peut, dans les limites de sa compétence, imposer des amendes administratives conformément à l'article 66 du règlement (UE) 2018/1725, à concurrence du montant visé à l'article 66, paragraphe 3, dudit règlement.

Article 41
Clauses contractuelles types et clauses contractuelles standard

Clauses contractuelles types et standard

Avant le 12 septembre 2025, la Commission élabore et recommande des clauses contractuelles types non contraignantes concernant l'accès aux données et l'utilisation des données, y compris des clauses relatives à une compensation raisonnable et à la protection des secrets d'affaires, ainsi que des clauses contractuelles standard non contraignantes pour les contrats d'informatique en nuage, afin d'aider les parties à rédiger et à négocier des contrats garantissant des droits et obligations contractuels équitables, raisonnables et non discriminatoires.

Article 42
Rôle du comité européen de l'innovation dans le domaine des données

Comité européen de l’innovation dans le domaine des données

Le comité européen de l'innovation dans le domaine des données, institué par la Commission en tant que groupe d'experts en vertu de l'article 29 du règlement (UE) 2022/868, au sein duquel les autorités compétentes sont représentées, favorise l'application cohérente du présent règlement:

a) en conseillant et en assistant la Commission en ce qui concerne l'élaboration d'une pratique cohérente des autorités compétentes pour l'exécution des chapitres II, III, V et VII;

b) en facilitant la coopération entre les autorités compétentes par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes pour l'échange efficace d'informations relatives à l'application des droits et obligations prévus aux chapitres II, III et V dans les affaires transfrontières, y compris la coordination en ce qui concerne l’instauration de sanctions;

c) en conseillant et en assistant la Commission en ce qui concerne:

i) l'opportunité de demander l'élaboration de normes harmonisées visées à l'article 33, paragraphe 4, à l'article 35, paragraphe 4, et à l'article 36, paragraphe 5;

ii) la préparation des actes d'exécution visés à l'article 33, paragraphe 5, à l'article 35, paragraphes 5 et 8, et à l'article 36, paragraphe 6;

iii) la préparation des actes délégués visés à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2; et

iv) l'adoption de lignes directrices établissant des cadres interopérables de normes et de pratiques communes pour le fonctionnement d'espaces européens communs des données visées à l'article 33, paragraphe 11.

CHAPITRE X
DROIT SUI GENERIS PREVU PAR LA DIRECTIVE 96/9/CE

Article 43
Bases de données contenant certaines données

Le droit sui generis prévu par l'article 7 de la directive 96/9/CE ne s'applique pas lorsque des données sont obtenues à partir d'un produit connecté ou d'un service connexe relevant du champ d'application du présent règlement ou générées par un tel produit ou service, en particulier en ce qui concerne ses articles 4 et 5.

CHAPITRE XI
DISPOSITIONS FINALES

Dispositions finales

Article 44
Autres actes juridiques de l'Union régissant les droits et obligations relatifs à l'accès aux données et à leur utilisation

1. Les obligations spécifiques relatives à la mise à disposition de données entre entreprises, entre entreprises et consommateurs, et, à titre exceptionnel, entre entreprises et organismes du secteur public, définies dans les actes juridiques de l'Union en vigueur au 11 janvier 2024 ou avant cette date et dans les actes délégués ou d'exécution adoptés en vertu de ces actes, restent inchangées.

2. Le présent règlement est sans préjudice du droit de l'Union précisant, à la lumière des besoins d'un secteur, d'un espace européen commun des données ou d'un domaine d'intérêt public, d'autres exigences, en particulier en ce qui concerne:

a) les aspects techniques de l'accès aux données;

b) les limitations des droits des détenteurs de données d'avoir accès à certaines données fournies par les utilisateurs ou de les utiliser;

c) les aspects allant au-delà de l'accès aux données et de l'utilisation de données.

3. Le présent règlement, à l'exception du chapitre V, est sans préjudice du droit de l'Union et du droit national prévoyant l'accès aux données et autorisant l'utilisation de données à des fins de recherche scientifique.

Article 45
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2, est conféré à la Commission pour une durée indéterminée à compter du 11 janvier 2024.

3. La délégation de pouvoir visée à l'article 29, paragraphe 7, et à l'article 33, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Jour-

nal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016"Mieux légiférer".

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 29, paragraphe 7, ou de l'article 33, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 46
Comité

1. La Commission est assistée par le comité institué par le règlement (UE) 2022/868. Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

Article 47
Modification du règlement (UE) 2017/2394

Dans l'annexe du règlement (UE) 2017/2394, le point suivant est ajouté:

"29. Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).".

Article 48
Modification de la directive (UE) 2020/1828

Dans l'annexe I de la directive (UE) 2020/1828, le point suivant est ajouté:

"68. Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).".

Article 49
Évaluation et réexamen

1. Au plus tard le 12 septembre 2028, la Commission procède à une évaluation du présent règlement et présente ses principales conclusions dans un rapport au Parlement européen et au Conseil, ainsi qu'au Comité économique et social européen. Cette évaluation porte, en particulier, sur les aspects suivants:

a) les situations qui doivent être considérées comme des situations de besoin exceptionnel aux fins de l'article 15 du présent règlement et de l'application du chapitre V du présent règlement, en particulier l'expérience acquise dans l'application du chapitre V du présent règlement par les organismes du secteur public, la Commission, la Banque centrale européenne et les organes de l'Union; le nombre de procédures engagées auprès de l'autorité compétente au titre de l'article 18, paragraphe 5, concernant l'application du chapitre V du présent règlement et leur issue, telles que déclarées par les autorités compétentes; l'incidence d'autres obligations prévues par le droit de l'Union ou le droit national aux fins de donner suite aux demandes d'accès aux informations; l'incidence des mécanismes de partage volontaire des données, tels que ceux mis en

place par des organisations altruistes en matière de données reconnues en vertu du règlement (UE) 2022/868, sur la réalisation des objectifs du chapitre V du présent règlement, et le rôle des données à caractère personnel dans le contexte de l'article 15 du présent règlement, y compris l'évolution des technologies renforçant la protection de la vie privée;

b) l'incidence du présent règlement sur l'utilisation des données dans l'économie, y compris sur l'innovation dans le domaine des données, les pratiques de monétisation des données et les services d'intermédiation de données, ainsi que sur le partage de données au sein des espaces européens communs des données;

c) l'accessibilité et l'utilisation des différentes catégories et des différents types de données;

d) l'exclusion de certaines catégories d'entreprises en tant que bénéficiaires au titre de l'article 5;

e) l'absence de toute incidence sur les droits de propriété intellectuelle;

f) l'incidence sur les secrets d'affaires, y compris sur la protection contre leur obtention, leur utilisation et leur divulgation illicites, ainsi que l'incidence du mécanisme permettant au détenteur de données de refuser la demande de l'utilisateur au titre de l'article 4, paragraphe 8, et de l'article 5, paragraphe 11, en tenant compte, dans la mesure du possible, de toute révision de la directive (UE) 2016/943;

g) la question de savoir si la liste des clauses contractuelles abusives visée à l'article 13 est à jour à la lumière des nouvelles pratiques commerciales et du rythme rapide de l'innovation sur le marché;

h) les changements dans les pratiques contractuelles des fournisseurs de services de traitement de données et la question de savoir si cela se traduit par un respect suffisant de l'article 25;

i) la réduction des frais imposés par les fournisseurs de services de traitement de données pour le processus de changement de fournisseur, en conformité avec la suppression progressive des frais de changement de fournisseur en vertu de l'article 29;

j) l'interaction du présent règlement avec d'autres actes juridiques de l'Union présentant un intérêt pour l'économie fondée sur les données;

k) la prévention de tout accès illicite des pouvoirs publics aux données à caractère non personnel;

l) l'efficacité du système de contrôle d'application requis au titre de l'article 37;

m) les effets du présent règlement sur les PME en ce qui concerne leur capacité d'innovation, la disponibilité des services de traitement des données pour les utilisateurs dans l'Union et la charge que représente le respect de nouvelles obligations.

2. Au plus tard le 12 septembre 2028, la Commission procède à une évaluation du présent règlement et présente au Parlement européen et au Conseil, ainsi qu'au Comité économique et social européen, un rapport reprenant ses principales conclusions. Cette évaluation porte sur les effets des articles 23 à 31 et des articles 34 et 35, en particulier en ce qui concerne la tarification et la diversité des services de traitement de données offerts au sein de l'Union, en accordant une attention particulière aux PME en tant que fournisseurs.

3. Les États membres fournissent à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 1 et 2.

4. Sur la base des rapports visés aux paragraphes 1 et 2, la Commission peut, le cas échéant, présenter au Parlement européen et au Conseil une proposition législative de modification du présent règlement.

Article 50
Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Il est applicable à partir du 12 septembre 2025.

L'obligation découlant de l'article 3, paragraphe 1, s'applique aux produits connectés et aux services connexes mis sur le marché après le 12 septembre 2026.

Le chapitre III s'applique en ce qui concerne les obligations de mise à disposition de données au titre du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union, qui entre en vigueur après le 12 septembre 2025.

Le chapitre IV s'applique aux contrats conclus après le 12 septembre 2025.

Le chapitre IV s'applique à partir du 12 septembre 2027 aux contrats conclus le 12 septembre 2025 ou avant cette date, à condition:

a) qu'ils soient à durée indéterminée; ou

b) qu'ils viennent à échéance au moins dix ans à compter du 11 janvier 2024.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 13 décembre 2023.

Par le Parlement européen
La présidente
R. METSOLA

Par le Conseil
Le président
P. NAVARRO RÍOS

Entrée en application progressive :

- 12/09/2025

- 12/09/2026

- 12/09/2025

- 12/09/2025

- 12/09/2027

AIA

AIA

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,
vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,
vu la proposition de la Commission européenne,
après transmission du projet d'acte législatif aux parlements nationaux,
vu l'avis du Comité économique et social européen[1],
vu l'avis de la Banque centrale européenne[2],
vu l'avis du Comité des régions[3],
statuant conformément à la procédure législative ordinaire[4],

considérant ce qui suit:

(1) L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle (ci-après dénommés «systèmes d'IA») dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation. Le présent règlement garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement.

(2) Le présent règlement devrait être appliqué dans le respect des valeurs de l'Union consacrées dans la Charte, en facilitant la protection des personnes physiques, des entreprises, de la démocratie, de l'état de droit et de l'environnement, tout en stimulant l'innovation et l'emploi et en faisant de l'Union un acteur de premier plan dans l'adoption d'une IA digne de confiance.

(3) Les systèmes d'IA peuvent être facilement déployés dans un large éventail de secteurs de l'économie et dans de nombreux pans de la société, y compris transfrontières, et peuvent facilement circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales destinées à faire en sorte que l'IA soit digne de confiance et sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Le fait que les règles nationales divergent

1. JO C 517 du 22.12.2021, p. 56.
2. JO C 115 du 11.3.2022, p. 5.
3. JO C 97 du 28.2.2022, p. 60.
4. Position du Parlement européen du 13 mars 2024 (non encore parue au Journal officiel) et décision du Conseil du 21 mai 2024.

peut entraîner une fragmentation du marché intérieur et peut réduire la sécurité juridique pour les opérateurs qui développent, importent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union afin de parvenir à une IA digne de confiance, et d'éviter les divergences qui entravent la libre circulation, l'innovation, le déploiement et l'adoption des systèmes d'IA et des produits et services connexes au sein du marché intérieur, en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur sur la base de l'article 114 du traité sur le fonctionnement de l'Union européenne. Dans la mesure où le présent règlement contient des règles spécifiques sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel, à savoir des restrictions portant sur l'utilisation de systèmes d'IA pour l'identification biométrique à distance à des fins répressives, sur l'utilisation de systèmes d'IA pour l'évaluation des risques liés à des personnes physiques à des fins répressives, et sur l'utilisation de systèmes d'IA de catégorisation biométrique à des fins répressives, il convient de fonder le présent règlement, pour ce qui est de ces règles spécifiques, sur l'article 16 du traité sur le fonctionnement de l'Union européenne. Compte tenu de ces règles spécifiques et du recours à l'article 16 du traité sur le fonctionnement de l'Union européenne, il convient de consulter le comité européen de la protection des données.

(4) L'IA est une famille de technologies en évolution rapide, contribuant à un large éventail de bienfaits économiques, environnementaux et sociétaux touchant l'ensemble des secteurs économiques et des activités sociales. En fournissant de meilleures prédictions, en optimisant les processus et l'allocation des ressources et en personnalisant les solutions numériques disponibles pour les particuliers et les organisations, le recours à l'IA peut donner des avantages concurrentiels décisifs aux entreprises et produire des résultats bénéfiques pour la société et l'environnement, dans des domaines tels que les soins de santé, l'agriculture, la sécurité des aliments, l'éducation et la formation, les médias, le sport, la culture, la gestion des infrastructures, l'énergie, les transports et la logistique, les services publics, la sécurité, la justice, l'utilisation efficace des ressources et de l'énergie, la surveillance de l'environnement, la préservation et la restauration de la biodiversité et des écosystèmes ainsi que l'atténuation du changement climatique et l'adaptation à celui-ci.

(5) Cependant, en fonction des circonstances concernant son application et son utilisation et du niveau de développement technologique, l'IA peut générer des risques et porter atteinte aux intérêts publics et aux droits fondamentaux protégés par le droit de l'Union. Le préjudice causé peut être matériel ou immatériel, y compris physique, psychologique, sociétal ou économique.

(6) Compte tenu de l'incidence majeure que l'IA peut avoir sur nos sociétés et de la nécessité de bâtir la confiance, l'IA et son cadre réglementaire doivent impérativement être élaborés dans le respect des valeurs de l'Union consacrées à l'article 2 du traité sur l'Union européenne, des droits et libertés fondamentaux prévus par les traités, et, conformément à l'article 6 du traité sur l'Union européenne, de la Charte. Il est indispensable que l'IA soit une technologie axée sur l'humain. Elle devrait servir d'outil aux personnes, dans le but ultime d'accroître le bien-être des humains.

(7) Afin d'assurer un niveau cohérent et élevé de protection des intérêts publics en ce qui concerne la santé, la sécurité et les droits fondamentaux, il convient d'établir des règles communes pour les systèmes d'IA à haut risque. Ces règles devraient être conformes à la Charte, non discriminatoires et compatibles avec les engagements commerciaux internationaux de l'Union. Elles devraient également tenir compte de la déclaration européenne sur les droits et principes numériques pour la décennie numérique et des lignes directrices en matière d'éthique pour une IA digne de confiance rédigées par le groupe d'experts de haut niveau sur l'intelligence artificielle (ci-après dénommé «GEHN IA»).

(8) Un cadre juridique de l'Union établissant des règles harmonisées sur l'IA est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'IA dans le marché intérieur, tout en garantissant un niveau élevé de protection des intérêts publics, comme la santé et la sécurité, et de protection des droits fondamentaux, y compris la démocratie, l'état de droit et la protection de l'environnement, tels qu'ils sont reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, des règles régissant la mise sur le marché, la mise en service et l'utilisation de certains systèmes

d'IA devraient être établies, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services. Ces règles devraient être claires et solides pour protéger les droits fondamentaux, soutenir de nouvelles solutions innovantes, permettre la mise en place d'un écosystème européen d'acteurs publics et privés créant des systèmes d'IA conformes aux valeurs de l'Union, et libérer le potentiel de la transformation numérique dans l'ensemble des régions de l'Union. En établissant ces règles, ainsi que des mesures en faveur de l'innovation mettant un accent particulier sur les petites et moyennes entreprises (PME), parmi lesquelles les jeunes pousses, le présent règlement contribue à la réalisation de l'objectif qui consiste à promouvoir l'approche européenne de l'IA axée sur l'humain et faire de l'UE un acteur mondial de premier plan dans le développement d'une IA sûre, fiable et éthique, ainsi que l'avait formulé le Conseil européen[5], et il garantit la protection de principes éthiques expressément demandée par le Parlement européen[6].

(9) Des règles harmonisées applicables à la mise sur le marché, à la mise en service et à l'utilisation de systèmes d'IA à haut risque devraient être établies conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil[7], à la décision no 768/2008/CE du Parlement européen et du Conseil[8] et au règlement (UE) 2019/1020 du Parlement européen et du Conseil[9] (ci-après dénommé «nouveau cadre législatif»). Les règles harmonisées énoncées dans le présent règlement devraient s'appliquer dans tous les secteurs et, conformément au nouveau cadre législatif, être sans préjudice du droit de l'Union en vigueur, en particulier en ce qui concerne la protection des données, la protection des consommateurs, les droits fondamentaux, l'emploi et la protection des travailleurs, et la sécurité des produits, que le présent règlement vient compléter. En conséquence, tous les droits et recours prévus par ce droit de l'Union pour les consommateurs et les autres personnes sur lesquelles les systèmes d'IA sont susceptibles d'avoir des incidences négatives, y compris en ce qui concerne la réparation de dommages éventuels conformément à la directive 85/374/CEE du Conseil[10], demeurent inchangés et pleinement applicables. En outre, dans le contexte de l'emploi et de la protection des travailleurs, le présent règlement ne devrait donc pas avoir d'incidence sur le droit de l'Union en matière de politique sociale ni sur le droit national du travail, dans le respect du droit de l'Union, en ce qui concerne les conditions d'emploi et de travail, y compris la santé et la sécurité au travail et les relations entre employeurs et travailleurs. Par ailleurs, le présent règlement ne devrait pas porter atteinte à l'exercice des droits fondamentaux reconnus dans les États membres et au niveau de l'Union, notamment le droit ou la liberté de faire grève ou d'entreprendre d'autres actions prévues par les mécanismes de concertation sociale propres aux États membres, ainsi que le droit de négocier, de conclure et d'appliquer des conventions collectives ou de mener des actions collectives conformément au droit national. Le présent règlement ne devrait pas avoir d'incidence sur les dispositions visant à améliorer les conditions de travail dans le cadre du travail via une plateforme, établies dans la directive du Parlement européen et du Conseil relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme. De plus, le présent règlement vise à renforcer l'efficacité de ces droits et recours existants en établissant des exigences et des obligations spécifiques, y compris en ce qui concerne la transparence, la documentation technique et la tenue de registres des systèmes d'IA. Par ailleurs, les obligations imposées aux différents opérateurs intervenant dans la chaîne de valeur de l'IA en vertu du présent règlement devraient s'appliquer sans préjudice du droit natio-

5. Conseil européen, réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) — Conclusions, EUCO 13/20, 2020, p. 6.
6. Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012 (INL).
7. Règlement (CE) no 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) no 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).
8. Décision no 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).
9. Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) no 765/2008 et (UE) no 305/2011 (JO L 169 du 25.6.2019, p. 1).
10. Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux (JO L 210 du 7.8.1985, p. 29).

nal, dans le respect du droit de l'Union, ayant pour effet de limiter l'utilisation de certains systèmes d'IA lorsque ces législations ne relèvent pas du champ d'application du présent règlement ou poursuivent des objectifs légitimes d'intérêt public autres que ceux poursuivis par le présent règlement. Ainsi, le droit national du travail et les lois sur la protection des mineurs, à savoir des personnes âgées de moins de 18 ans, compte tenu de l'observation générale no 25 (2021) de la CNUDE sur les droits de l'enfant en relation avec l'environnement numérique, dans la mesure où ils ne sont pas spécifiques aux systèmes d'IA et poursuivent d'autres objectifs légitimes d'intérêt public, ne devraient pas être affectés par le présent règlement.

(10) Le droit fondamental à la protection des données à caractère personnel est garanti en particulier par les règlements (UE) 2016/679[11] et (UE) 2018/1725[12] du Parlement européen et du Conseil, ainsi que par la directive (UE) 2016/680 du Parlement européen et du Conseil[13] Par ailleurs, la directive 2002/58/CE du Parlement européen et du Conseil[14] protège la vie privée et la confidentialité des communications, y compris en prévoyant des conditions régissant le stockage de données à caractère personnel et non personnel dans des équipements terminaux ainsi que les conditions d'accès à ces données depuis ces équipements. Ces actes législatifs de l'Union servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel. Le présent règlement n'entend pas modifier l'application du droit de l'Union régissant le traitement des données à caractère personnel, ni les tâches et les pouvoirs des autorités de contrôle indépendantes chargées de veiller au respect de ces ins truments. Il n'a pas non plus d'incidence sur les obligations des fournisseurs et des déployeurs de systèmes d'IA en leur qualité de responsables du traitement ou de sous-traitants découlant du droit de l'Union ou du droit national relatif à la protection des données à caractère personnel dans la mesure où la conception, le développement ou l'utilisation de systèmes d'IA implique le traitement de données à caractère personnel. Il convient également de préciser que les personnes concernées continuent de jouir de tous les droits et garanties qui leur sont conférés par le droit de l'Union, dont les droits liés à la prise de décision individuelle entièrement automatisée, y compris le profilage. Des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA établies en vertu du présent règlement devraient faciliter la mise en œuvre effective des droits et autres voies de recours garantis par le droit de l'Union relatif à la protection des données à caractère personnel et d'autres droits fondamentaux, et permettre aux personnes concernées de faire valoir ces droits et autres voies de recours.

cf. RGPD

cf. déployeurs

(11) Le présent règlement devrait être sans préjudice des dispositions relatives à la responsabilité des fournisseurs de services intermédiaires prévue dans le règlement (UE) 2022/2065 du Parlement européen et du Conseil[15].

(12) La notion de «système d'IA» figurant dans le présent règlement devrait être clairement définie et devrait être étroitement alignée sur les travaux des organisations internationales œuvrant dans le domaine de l'IA afin de garantir la sécurité juridique,

cf. RGPD

11. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).
12. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).
13. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).
14. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).
15. Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

et de faciliter la convergence internationale et une large acceptation, tout en offrant la souplesse nécessaire pour tenir compte des évolutions technologiques rapides dans ce domaine. En outre, la définition devrait être fondée sur les caractéristiques essentielles des systèmes d'IA qui la distinguent des systèmes logiciels ou des approches de programmation traditionnels plus simples, et ne devrait pas couvrir les systèmes fondés sur les règles définies uniquement par les personnes physiques pour exécuter automatiquement des opérations. Une caractéristique essentielle des systèmes d'IA est leur capacité d'inférence. Cette capacité d'inférence concerne le processus consistant à générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions, qui peuvent influencer l'environnement physique ou virtuel, et la capacité des systèmes d'IA à inférer des modèles ou des algorithmes, ou les deux, à partir d'entrées ou de données. Les techniques permettant l'inférence lors de la construction d'un système d'IA comprennent des approches d'apprentissage automatique qui apprennent à partir des données la manière d'atteindre certains objectifs, et des approches fondées sur la logique et les connaissances qui font des inférences à partir des connaissances encodées ou de la représentation symbolique de la tâche à résoudre. La capacité d'un système d'IA à faire des inférences va au-delà du traitement de données de base en ce qu'elle permet l'apprentissage, le raisonnement ou la modélisation. Le terme «fondé sur des machines» renvoie au fait que les systèmes d'IA tournent sur des machines. La référence à des objectifs explicites ou implicites souligne que les systèmes d'IA peuvent fonctionner selon des objectifs explicites définis ou des objectifs implicites. Les objectifs du système d'IA peuvent être différents de la destination du système d'IA dans un contexte spécifique. Aux fins du présent règlement, les environnements devraient s'entendre comme étant les contextes dans lesquels les systèmes d'IA fonctionnent, tandis que les sorties générées par le système d'IA correspondent à différentes fonctions exécutées par les systèmes d'IA et consistent en des prévisions, du contenu, des recommandations ou des décisions. Les systèmes d'IA sont conçus pour fonctionner à différents niveaux d'autonomie, ce qui signifie qu'ils bénéficient d'un certain degré d'indépendance dans leur action par rapport à une ingérence humaine et de capacités à fonctionner sans intervention humaine. La faculté d'adaptation dont un système d'IA pourrait faire preuve après son déploiement est liée à des capacités d'auto-apprentissage, qui permettent au système d'évoluer en cours d'utilisation. Les systèmes d'IA peuvent être utilisés seuls ou en tant que composant d'un produit, que le système soit physiquement incorporé dans le produit (intégré) ou qu'il serve la fonctionnalité du produit sans y être incorporé (non intégré).

(13) Il convient d'interpréter la notion de «déployeurs» visée dans le présent règlement comme désignant toute personne physique ou morale, y compris une autorité publique, une agence ou un autre organisme, utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. En fonction du type de système d'IA, l'utilisation du système peut concerner des personnes autres que le déployeur.

cf. déployeurs

(14) Il convient d'interpréter la notion de «données biométriques» utilisée dans le présent règlement à la lumière de la notion de données biométriques au sens de l'article 4, point 14), du règlement (UE) 2016/679, de l'article 3, point 18), du règlement (UE) 2018/1725, et de l'article 3, point 13), de la directive (UE) 2016/680. Des données biométriques peuvent permettre l'authentification, l'identification ou la catégorisation des personnes physiques, ainsi que la reconnaissance de leurs émotions.

cf. RGPD art. 4.14

(15) La notion d'«identification biométrique» visée dans le présent règlement devrait être définie comme la reconnaissance automatisée de caractéristiques physiques, physiologiques et comportementales d'une personne, telles que le visage, les mouvements oculaires, la forme du corps, la voix, la prosodie, la démarche, la posture, le rythme cardiaque, la pression sanguine, l'odeur et la frappe au clavier, aux fins d'établir l'identité d'une personne par comparaison des données biométriques de cette personne avec les données biométriques de personnes stockées dans une base de données de référence, que la personne ait donné son approbation ou non. En sont exclus les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux.

(16) La notion de « catégorisation biométrique» visée dans le présent règlement devrait être définie comme le classement de personnes physiques dans certaines caté-

gories sur la base de leurs données biométriques. Ces catégories spécifiques peuvent concerner des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits liés au comportement ou à la personnalité, la langue, la religion, l'appartenance à une minorité nationale ou encore l'orientation sexuelle ou politique. Cela n'inclut pas les systèmes de catégorisation biométrique qui sont une caractéristique purement accessoire intrinsèquement liée à un autre service commercial, ce qui signifie que cette caractéristique ne peut, pour des raisons techniques objectives, être utilisée sans le service principal, et l'intégration de cette caractéristique ou fonctionnalité n'est pas un moyen de contourner l'applicabilité des règles du présent règlement. Ainsi, les filtres de catégorisation des caractéristiques faciales ou corporelles qui sont utilisés sur les places de marché en ligne pourraient correspondre à ce type de caractéristique accessoire, étant donné qu'ils ne peuvent être utilisés qu'en lien avec le service principal, qui consiste à vendre un produit en permettant au consommateur d'afficher un aperçu du produit porté par lui-même et de l'aider à prendre une décision d'achat. Les filtres utilisés sur les services de réseaux sociaux en ligne qui classent par catégorie les caractéristiques faciales ou corporelles afin de permettre aux utilisateurs d'ajouter ou de modifier des images ou des vidéos pourraient également être considérés comme des fonctionnalités accessoires, étant donné que ce type de filtre ne peut pas être utilisé sans le service principal des services de réseau social consistant à partager des contenus en ligne.

(17) La notion de «système d'identification biométrique à distance» visée dans le présent règlement devrait être définie, sur le plan fonctionnel, comme un système d'IA destiné à identifier des personnes physiques sans leur participation active, en règle générale à distance, par la comparaison des données biométriques d'une personne avec celles contenues dans une base de données de référence, quels que soient la technologie, les processus ou les types de données biométriques particuliers utilisés. Ces systèmes d'identification biométrique à distance sont généralement utilisés pour la perception simultanée de plusieurs personnes ou de leur comportement afin de faciliter sensiblement l'identification de personnes physiques sans leur participation active. Sont exclus les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. Cette exclusion est justifiée par le fait que ces systèmes sont susceptibles d'avoir une incidence mineure sur les droits fondamentaux des personnes physiques par rapport aux systèmes d'identification biométrique à distance qui peuvent être utilisés pour le traitement des données biométriques d'un grand nombre de personnes sans leur participation active. Dans le cas des systèmes «en temps réel», la capture des données biométriques, la comparaison et l'identification se font toutes instantanément, quasi instantanément ou en tout état de cause sans décalage significatif. À cet égard, il convient, en prévoyant la possibilité de légers décalages, d'empêcher le contournement des règles du présent règlement relatives à l'utilisation «en temps réel» des systèmes d'IA concernés. Les systèmes «en temps réel» reposent sur l'utilisation d'éléments «en direct» ou «en léger différé», comme des séquences vidéo, générés par une caméra ou un autre appareil doté de fonctionnalités similaires. Dans le cas des systèmes «a posteriori», en revanche, les données biométriques sont prélevées dans un premier temps et la comparaison et l'identification n'ont lieu qu'après un délai substantiel. Cela suppose des éléments tels que des images ou des séquences vidéo, qui ont été générés par des caméras de télévision en circuit fermé ou des appareils privés avant l'utilisation du système à l'égard des personnes physiques concernées.

(18) La notion de «système de reconnaissance des émotions» visée dans le présent règlement devrait être définie comme un système d'IA servant à identifier les émotions ou les intentions de personnes physiques ou à faire des déductions quant à leurs émotions ou intentions, sur la base de leurs données biométriques. Cette notion renvoie à des émotions ou des intentions telles que le bonheur, la tristesse, la colère, la surprise, le dégoût, la gêne, l'excitation, la honte, le mépris, la satisfaction et l'amusement. Cette notion ne recouvre pas les états physiques, tels que la douleur ou la fatigue, qui comprennent, par exemple, des systèmes utilisés pour déceler l'état de fatigue des pilotes ou des conducteurs professionnels aux fins de la prévention des accidents. Elle ne recouvre pas non plus la simple détection d'expressions, de gestes ou de mouvements dont l'apparence est immédiate, à moins que ceux-ci ne soient utilisés pour identifier ou déduire des émotions. Ces expressions peuvent être des expressions faciales toutes simples telles qu'un froncement de sourcils ou un sourire, ou des

gestes tels qu'un mouvement de mains, de bras ou de tête, ou encore des caractéristiques de la voix d'une personne, comme le fait de parler fort ou de chuchoter.

(19) Aux fins du présent règlement, la notion d'«espace accessible au public» devrait s'entendre comme désignant tout espace physique accessible à un nombre indéterminé de personnes physiques, que l'espace en question soit privé ou public, et indépendamment de l'activité pour laquelle il peut être utilisé, comme pour le commerce, par exemple, magasins, restaurants ou cafés, pour la prestation de services, par exemple, banques, activités professionnelles ou hôtellerie, pour la pratique de sports, par exemple, piscines, salles de sport ou stades, pour les transports, par exemple, gares routières, stations de métro et gares ferroviaires, aéroports ou moyens de transport, pour les divertissements, par exemple, cinémas, théâtres, musées, salles de concert et de conférence, ou pour les loisirs ou autres, par exemple, routes et places publiques, parcs, forêts ou terrains de jeux. Un espace devrait également être classé comme accessible au public si, indépendamment de la capacité potentielle ou des restrictions de sécurité, l'accès est soumis à certaines conditions prédéterminées qui peuvent être remplies par un nombre indéterminé de personnes, telles que l'achat d'un billet ou d'un titre de transport, l'enregistrement préalable ou le fait d'avoir un certain âge. En revanche, un espace ne devrait pas être considéré comme étant accessible au public si l'accès est limité à certaines personnes physiques, définies soit par le droit de l'Union soit par le droit national directement lié à la sûreté ou à la sécurité publiques, ou par la manifestation claire de la volonté de la personne disposant de l'autorité compétente sur l'espace. Le seul fait d'avoir une possibilité d'accès, comme une porte déverrouillée ou une porte ouverte dans une clôture, n'implique pas que l'espace est accessible au public en présence d'indications ou de circonstances suggérant le contraire, comme des signes d'interdiction ou de restriction d'accès. Les locaux des entreprises et des usines, ainsi que les bureaux et les lieux de travail qui sont destinés à être accessibles uniquement aux employés et prestataires de services concernés ne sont pas des espaces accessibles au public. Les espaces accessibles au public ne devraient pas inclure les prisons ni le contrôle aux frontières. D'autres espaces peuvent comprendre à la fois des espaces accessibles au public et des espaces non accessibles au public, comme le hall d'un bâtiment d'habitation privé par lequel il faut passer pour accéder au bureau d'un médecin ou le hall d'un aéroport. Les espaces en ligne ne sont pas couverts, car ce ne sont pas des espaces physiques. Le caractère accessible ou non au public d'un espace donné devrait cependant être déterminé au cas par cas, en tenant compte des particularités de la situation en question.

(20) Afin de tirer le meilleur parti des systèmes d'IA tout en protégeant les droits fondamentaux, la santé et la sécurité et de permettre un contrôle démocratique, il convient que les fournisseurs, les déployeurs et les personnes concernées acquièrent, dans le cadre de la maîtrise de l'IA, les notions nécessaires pour prendre des décisions éclairées concernant les systèmes d'IA. Ces notions peuvent varier en fonction du contexte et peuvent recouvrir le faire de comprendre l'application correcte des éléments techniques au cours de la phase de développement du système d'IA, les mesures à appliquer pendant son utilisation, les moyens appropriés d'interpréter les sorties du système d'IA et, dans le cas des personnes concernées, les connaissances nécessaires pour comprendre comment les décisions prises avec l'aide de l'IA auront une incidence sur elles. Dans le cadre de l'application du présent règlement, la maîtrise de l'IA devrait fournir à tous les acteurs pertinents de la chaîne de valeur de l'IA les connaissances nécessaires pour en garantir le respect approprié et la mise en application correcte. En outre, la mise en œuvre à grande échelle de mesures relatives à la maîtrise de l'IA et l'introduction d'actions de suivi appropriées pourraient contribuer à améliorer les conditions de travail et, à terme, soutenir la consolidation et une trajectoire d'innovation d'une IA digne de confiance dans l'Union. Le Comité européen de l'intelligence artificielle (ci-après dénommé « Comité IA») devrait soutenir la Commission afin de promouvoir les outils de maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA. En coopération avec les parties prenantes concernées, la Commission et les États membres devraient faciliter l'élaboration de codes de conduite volontaires au service de la maîtrise de l'IA chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA.

cf. déployeurs

(21) Afin de garantir des conditions de concurrence équitables et une protection efficace des droits et libertés des citoyens dans toute l'Union, les règles établies par le présent règlement devraient s'appliquer de manière non discriminatoire aux fournisseurs

de systèmes d'IA, qu'ils soient établis dans l'Union ou dans un pays tiers, et aux déployeurs de systèmes d'IA établis dans l'Union.

cf. déployeurs

(22) Compte tenu de leur nature numérique, certains systèmes d'IA devraient relever du présent règlement même lorsqu'ils ne sont pas mis sur le marché, mis en service, ou utilisés dans l'Union. Cela devrait notamment être le cas lorsqu'un opérateur établi dans l'Union confie à un opérateur externe établi dans un pays tiers la tâche d'exécuter certains services ayant trait à une activité devant être réalisée par un système d'IA qui serait considéré comme étant à haut risque. Dans ces circonstances, le système d'IA utilisé dans un pays tiers par l'opérateur pourrait traiter des données légalement collectées et transférées depuis l'Union, et fournir à l'opérateur contractant établi dans l'Union les sorties dudit système d'IA provenant de ce traitement, sans que ce système d'IA soit mis sur le marché, mis en service ou utilisé dans l'Union. Afin d'éviter le contournement des règles du présent règlement et d'assurer une protection efficace des personnes physiques situées dans l'Union, le présent règlement devrait également s'appliquer aux fournisseurs et aux déployeurs de systèmes d'IA qui sont établis dans un pays tiers, dans la mesure les sorties produites par ces systèmes sont destinées à être utilisées dans l'Union. Néanmoins, pour tenir compte des dispositions existantes et des besoins particuliers de coopération future avec les partenaires étrangers avec lesquels des informations et des preuves sont échangées, le présent règlement ne devrait pas s'appliquer aux autorités publiques d'un pays tiers ni aux organisations internationales lorsqu'elles agissent dans le cadre d'accords de coopération ou d'accords internationaux conclus au niveau de l'Union ou au niveau national pour la coopération des services répressifs et judiciaires avec l'Union ou avec les États membres, à condition que le pays tiers concerné ou les organisations internationales concernées fournissent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Le cas échéant, cela peut couvrir les activités des entités chargées par les pays tiers d'exécuter des tâches spécifiques à l'appui de cette coopération policière et judiciaire. De tels cadres de coopération ou accords ont été conclus bilatéralement entre des États membres et des pays tiers ou entre l'Union européenne, Europol et d'autres agences de l'Union, des pays tiers et des organisations internationales. Les autorités compétentes pour la surveillance des autorités répressives et judiciaires au titre du présent règlement devraient évaluer si ces cadres de coopération ou accords internationaux comportent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Les autorités nationales bénéficiaires et les institutions, organes et organismes de l'Union qui utilisent ces sorties dans l'Union demeurent responsables de veiller à ce que leur utilisation soit conforme au droit de l'Union. Lors de la révision de ces accords internationaux ou de la conclusion de nouveaux accords à l'avenir, les parties contractantes devraient tout mettre en œuvre pour aligner ces accords sur les exigences du présent règlement.

cf. déployeurs

(23) Le présent règlement devrait également s'appliquer aux institutions, organes et organismes de l'Union lorsqu'ils agissent en tant que fournisseurs ou déployeurs d'un système d'IA.

cf. déployeurs

(24) Si et dans la mesure où des systèmes d'IA sont mis sur le marché, mis en service ou utilisés avec ou sans modification de ces systèmes à des fins militaires, de défense ou de sécurité nationale, ces systèmes devraient être exclus du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités, par exemple qu'il s'agisse d'une entité publique ou privée. En ce qui concerne l'usage à des fins militaires et de défense, une telle exclusion est justifiée tant par l'article 4, paragraphe 2, du traité sur l'Union européenne que par les spécificités de la politique de défense des États membres et de la politique de défense commune de l'Union relevant du titre V, chapitre 2, du traité sur l'Union européenne, qui sont soumises au droit international public, lequel constitue donc le cadre juridique le plus approprié pour la réglementation des systèmes d'IA dans le contexte de l'utilisation de la force létale et d'autres systèmes d'IA dans le cadre d'activités militaires et de défense. En ce qui concerne l'usage à des fins de sécurité nationale, l'exclusion est justifiée tant par le fait que la sécurité nationale reste de la seule responsabilité de chaque État membre, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, que par la nature spécifique et les besoins opérationnels des activités liées à la sécurité nationale et par les règles nationales spécifiques applicables à ces activités. Néanmoins, si un système d'IA développé, mis sur le marché, mis en service ou utilisé à des fins militaires, de défense ou de sécurité nationale est, temporairement ou définitivement, utilisé en dehors de ce cadre à d'autres fins (par exemple, à des fins civiles ou

humanitaires, à des fins répressives ou de sécurité publique), un tel système relèverait du champ d'application du présent règlement. Dans ce cas, l'entité qui utilise le système d'IA à des fins autres que militaires, de défense ou de sécurité nationale devrait veiller à la mise en conformité du système d'IA avec le présent règlement, à moins qu'il le soit déjà. Les systèmes d'IA mis sur le marché ou mis en service à des fins exclues, à savoir à des fins militaires, de défense ou de sécurité nationale, et à une ou plusieurs fins non exclues, comme à des fins civiles ou répressives, relèvent du champ d'application du présent règlement et les fournisseurs de ces systèmes devraient veiller au respect du présent règlement. En l'occurrence, le fait qu'un système d'IA puisse relever du champ d'application du présent règlement ne devrait pas affecter la possibilité pour les entités exerçant des activités de sécurité nationale, de défense et militaires, indépendamment du type d'entité exerçant ces activités, d'utiliser des systèmes d'IA à des fins de sécurité nationale, militaires et de défense, dont l'utilisation est exclue du champ d'application du présent règlement. Un système d'IA mis sur le marché à des fins civiles ou répressives qui est utilisé avec ou sans modification à des fins militaires, de défense ou de sécurité nationale ne devrait pas relever du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités.

(25) Le présent règlement devrait soutenir l'innovation et respecter la liberté scientifique et ne devrait pas compromettre les activités de recherche et de développement. Il est donc nécessaire d'exclure de son champ d'application les systèmes et modèles d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques. En outre, il est nécessaire de veiller à ce que le présent règlement n'affecte pas autrement les activités de recherche et de développement scientifiques relatives aux systèmes ou modèles d'IA avant leur mise sur le marché ou leur mise en service. En ce qui concerne les activités de recherche, d'essai et de développement axées sur les produits, relatives aux systèmes ou modèles d'IA, les dispositions du présent règlement ne devraient pas non plus s'appliquer avant la mise en service ou la mise sur le marché de ces systèmes et modèles. Cette exclusion est sans préjudice de l'obligation de se conformer au présent règlement lorsqu'un système d'IA relevant du champ d'application du présent règlement est mis sur le marché ou mis en service à la suite de cette activité de recherche et de développement, et sans préjudice de l'application des dispositions relatives aux bacs à sable réglementaires de l'IA et aux essais en conditions réelles. En outre, sans préjudice de l'exclusion des systèmes d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques, tout autre système d'IA susceptible d'être utilisé pour mener une activité de recherche et de développement devrait rester soumis aux dispositions du présent règlement. En tout état de cause, toute activité de recherche et de développement devrait être menée conformément à des normes éthiques et professionnelles reconnues en matière de recherche scientifique et dans le respect du droit de l'Union applicable.

(26) Afin d'introduire un ensemble proportionné et efficace de règles contraignantes pour les systèmes d'IA, il convient de suivre une approche clairement définie fondée sur les risques. Cette approche devrait adapter le type et le contenu de ces règles à l'intensité et à la portée des risques que les systèmes d'IA peuvent générer. Il est donc nécessaire d'interdire certaines pratiques inacceptables en matière d'IA, de fixer des exigences pour les systèmes d'IA à haut risque et des obligations pour les opérateurs concernés, ainsi que de fixer des obligations de transparence pour certains systèmes d'IA.

(27) Si l'approche fondée sur les risques constitue la base d'un ensemble proportionné et efficace de règles contraignantes, il importe de rappeler les lignes directrices en matière d'éthique pour une IA digne de confiance, élaborées en 2019 par le GEHN IA indépendant constitué par la Commission. Dans ces lignes directrices, le GEHN IA a élaboré sept principes éthiques non contraignants pour l'IA, qui sont destinés à contribuer à faire en sorte que l'IA soit digne de confiance et saine sur le plan éthique. Il s'agit des sept principes suivants: action humaine et contrôle humain; robustesse technique et sécurité; respect de la vie privée et gouvernance des données; transparence; diversité, non-discrimination et équité; bien-être sociétal et environnemental; et responsabilité. Sans préjudice des exigences juridiquement contraignantes du présent règlement et de toute autre disposition législative de l'Union applicable, ces lignes directrices contribuent à la conception d'une IA cohérente, fiable et axée sur l'humain, conformément à la Charte et aux valeurs sur lesquelles l'Union est fondée. Conformément aux lignes directrices du GEHN IA, «action humaine et contrôle humain» renvoient au fait que les systèmes d'IA sont développés et utilisés comme un outil au

service des personnes, qui respecte la dignité humaine et l'autonomie de l'individu, et qui fonctionne de manière à pouvoir être contrôlé et supervisé par des êtres humains.«Robustesse technique et sécurité» renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à ce qu'ils soient techniquement robustes en cas de problème et résilients aux tentatives visant à en corrompre l'utilisation ou les performances afin de permettre à des tiers d'en faire une utilisation abusive, et à réduire le plus possible les atteintes involontaires. «Respect de la vie privée et gouvernance des données» renvoient au fait que les systèmes d'IA sont développés et utilisés conformément aux règles en matière de respect de la vie privée et de protection des données, dans le cadre d'un traitement de données répondant à des normes élevées en matière de qualité et d'intégrité. «Transparence» renvoie au fait que les systèmes d'IA sont développés et utilisés de manière à permettre une traçabilité et une explicabilité appropriées, faisant en sorte que les personnes réalisent qu'elles communiquent ou interagissent avec un système d'IA, que les déployeurs soient dûment informés des capacités et des limites de ce système d'IA et que les personnes concernées soient informées de leurs droits. «Diversité, non-discrimination et équité» renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à inclure des acteurs divers et à promouvoir l'égalité d'accès, l'égalité de genre et la diversité culturelle, tout en évitant les effets discriminatoires et les biais injustes, qui sont interdits par le droit de l'Union ou le droit national. «Bien-être sociétal et environnemental» renvoie au fait que les systèmes d'IA sont développés et utilisés d'une manière durable et respectueuse de l'environnement, mais aussi de manière à ce que tous les êtres humains en profitent, tout en surveillant et en évaluant les effets à long terme sur l'individu, la société et la démocratie. Ces principes devraient se retrouver, autant que possible, dans la conception et l'utilisation des modèles d'IA. Ils devraient en tout état de cause servir de base à l'élaboration de codes de conduite au titre du présent règlement. Toutes les parties prenantes, y compris l'industrie, le monde universitaire, la société civile et les organismes de normalisation, sont encouragées à tenir compte, ainsi qu'il convient, des principes éthiques pour l'élaboration de bonnes pratiques et de normes volontaires.

cf. déployeurs

(28) Si l'IA peut être utilisée à de nombreuses fins positives, elle peut aussi être utilisée à mauvais escient et fournir des outils nouveaux et puissants à l'appui de pratiques de manipulation, d'exploitation et de contrôle social. De telles pratiques sont particulièrement néfastes et abusives et devraient être interdites, car elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit, ainsi qu'aux droits fondamentaux consacrés dans la Charte, y compris le droit à la non-discrimination, le droit à la protection des données et à la vie privée et les droits de l'enfant.

(29) Des techniques de manipulation fondées sur l'IA peuvent être utilisées pour persuader des personnes d'adopter des comportements indésirables ou pour les tromper en les poussant à prendre des décisions d'une manière qui met à mal et compromet leur autonomie, leur libre arbitre et leur liberté de choix. La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA ayant pour objectif ou pour effet d'altérer substantiellement les comportements humains, avec le risque de causer des dommages importants, en particulier d'avoir des incidences suffisamment importantes sur la santé physique ou psychologique ou sur les intérêts financiers, sont particulièrement dangereuses et devraient dès lors être interdites. Ces systèmes d'IA font intervenir des composants subliminaux, tels que des stimuli sonores, visuels ou vidéo que l'individu ne peut percevoir, étant donné que ces stimuli échappent à la perception humaine, ou d'autres techniques manipulatrices ou trompeuses qui mettent à mal ou altèrent l'autonomie de la personne, son libre arbitre ou sa liberté de choix de telle sorte que l'individu n'est pas conscient de ces techniques ou, à supposer qu'il le soit, sans qu'il puisse échapper à la duperie ni opposer une résistance ou un contrôle auxdites techniques. Cela pourrait être facilité, par exemple, par des interfaces cerveau-machine ou par la réalité virtuelle étant donné qu'elles permettent d'avoir plus de contrôle sur les stimuli qui sont présentés aux personnes, dans la mesure où elles peuvent en altérer sensiblement le comportement d'une manière très nocive. En outre, des systèmes d'IA peuvent également exploiter les vulnérabilités d'une personne ou d'un groupe particulier de personnes en raison de leur âge, d'un handicap au sens de la directive (UE) 2019/882 du Parlement européen et du Conseil[16], ou d'une situation sociale ou économique spécifique susceptible de rendre ces personnes plus vulnérables à l'exploitation, telles que les personnes vivant dans une extrême pauvreté ou appartenant à des minorités ethniques ou religieuses. De tels systèmes d'IA peuvent

être mis sur le marché, mis en service ou utilisés avec pour objectif ou pour effet d'altérer substantiellement le comportement d'une personne d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à une autre personne ou à des groupes de personnes, y compris des dommages susceptibles de s'accumuler au fil du temps, et il y a lieu, par conséquent, de les interdire. Il peut s'avérer impossible de présumer l'existence d'une intention d'altérer le comportement lorsque cette altération résulte de facteurs externes au système d'IA qui échappent au contrôle du fournisseur ou du déployeur, à savoir de facteurs qui ne peuvent être raisonnablement prévisibles, et partant, ne peuvent être atténués par le fournisseur ou le déployeur du système d'IA. En tout état de cause, il n'est pas nécessaire que le fournisseur ou le déployeur ait l'intention de causer un préjudice important, du moment que ce préjudice résulte de pratiques de manipulation ou d'exploitation reposant sur l'IA. Les interdictions de telles pratiques en matière d'IA complètent les dispositions de la directive 2005/29/CE du Parlement européen et du Conseil[17], notamment concernant le fait que les pratiques commerciales déloyales entraînant des préjudices économiques ou financiers pour les consommateurs sont interdites en toutes circonstances, qu'elles soient mises en place au moyen de systèmes d'IA ou autrement. Les interdictions des pratiques de manipulation et d'exploitation prévues par le présent règlement ne devraient pas affecter les pratiques licites dans le cadre de traitements médicaux tels que le traitement psychologique d'une maladie mentale ou la rééducation physique, lorsque ces pratiques sont effectuées conformément à la législation applicable et aux normes médicales, comme le consentement explicite des personnes ou de leurs représentants légaux. En outre, les pratiques commerciales courantes et légitimes, par exemple dans le domaine de la publicité, qui respectent le droit applicable ne devraient pas, en soi, être considérées comme constituant des pratiques de manipulation préjudiciables reposant sur l'IA.

cf. déployeurs

(30) Il y a lieu d'interdire les systèmes de catégorisation biométrique fondés sur les données biométriques des personnes physiques, comme le visage ou les empreintes digitales, utilisés pour arriver à des déductions ou des inférences concernant les opinions politiques d'un individu, son affiliation à une organisation syndicale, ses convictions religieuses ou philosophiques, sa race, sa vie sexuelle ou son orientation sexuelle. Cette interdiction ne devrait pas couvrir l'étiquetage, le filtrage ou la catégorisation licites des ensembles de données biométriques acquis dans le respect du droit de l'Union ou du droit national en fonction de données biométriques, comme le tri des images en fonction de la couleur des cheveux ou de celle des yeux, qui peuvent par exemple être utilisés dans le domaine répressif.

(31) Les systèmes d'IA permettant la notation sociale des personnes physiques par des acteurs publics ou privés peuvent conduire à des résultats discriminatoires et à l'exclusion de certains groupes. Ils peuvent porter atteinte au droit à la dignité et à la non-discrimination et sont contraires aux valeurs d'égalité et de justice. Ces systèmes d'IA évaluent ou classent les personnes physiques ou les groupes de personnes physiques en fonction de plusieurs points de données liées à leur comportement social dans divers contextes ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites pendant un certain temps. La note sociale obtenue à partir de ces systèmes d'IA peut conduire au traitement préjudiciable ou défavorable de personnes physiques ou de groupes entiers dans des contextes sociaux qui sont dissociés du contexte dans lequel les données ont été initialement générées ou collectées, ou à un traitement préjudiciable disproportionné ou injustifié au regard de la gravité de leur comportement social. Il y a donc lieu d'interdire les systèmes d'IA impliquant de telles pratiques de notation inacceptables et produisant de tels effets préjudiciables ou défavorables. Cette interdiction ne devrait pas avoir d'incidence sur les évaluations licites des personnes physiques qui sont pratiquées dans un but précis, dans le respect du droit de l'Union et du droit national.

16. Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

17. Directive no 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) no 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).

(32) L'utilisation de systèmes d'IA pour l'identification biométrique à distance «en temps réel» de personnes physiques dans des espaces accessibles au public à des fins répressives est particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ce risque de résultats biaisés et d'effets discriminatoires est particulièrement significatif en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. En outre, du fait de l'immédiateté des effets et des possibilités limitées d'effectuer des vérifications ou des corrections supplémentaires, l'utilisation de systèmes fonctionnant en temps réel engendre des risques accrus pour les droits et les libertés des personnes concernées dans le cadre d'activités répressives ou affectées par celles-ci.

(33) L'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans des situations précisément répertoriées et rigoureusement définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance l'emporte sur les risques encourus. Ces situations comprennent la recherche de certaines victimes d'actes criminels, y compris de personnes disparues; certaines menaces pour la vie ou la sécurité physique des personnes physiques, ou des menaces d'attaque terroriste; et la localisation ou l'identification des auteurs ou des suspects des infractions pénales énumérées dans une annexe du présent règlement, lorsque ces infractions pénales sont passibles, dans l'État membre concerné, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins quatre ans et telles qu'elles sont définies dans le droit dudit État membre. Le seuil fixé pour la peine ou la mesure de sûreté privative de liberté prévue par le droit national contribue à garantir que l'infraction soit suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance «en temps réel». En outre, la liste des infractions pénales figurant en annexe du présent règlement sont basées sur les 32 infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil[18], compte tenu du fait que certaines de ces infractions sont, en pratique, susceptibles d'être plus pertinentes que d'autres, dans le sens où le recours à l'identification biométrique à distance «en temps réel» pourrait, vraisemblablement, être nécessaire et proportionné, à des degrés très divers, pour les mesures pratiques de localisation ou d'identification d'un auteur ou d'un suspect de l'une des différentes infractions pénales répertoriées, eu égard également aux différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives. Une menace imminente pour la vie ou pour la sécurité physique des personnes physiques pourrait également résulter d'une grave perturbation d'une infrastructure critique, au sens de l'article 2, point 4), de la directive (UE) 2022/2557 du Parlement européen et du Conseil[19], lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie ou la sécurité physique d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice de la fonction essentielle de l'État. Par ailleurs, le présent règlement devrait préserver la capacité des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile d'effectuer des contrôles d'identité en présence de la personne concernée conformément aux conditions prévues par le droit de l'Union et le droit national pour ces contrôles. En particulier, les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile devraient pouvoir utiliser des systèmes d'information, conformément au droit de l'Union ou au droit national, pour identifier une personne qui, lors d'un contrôle d'identité, soit refuse d'être identifiée, soit n'est pas en mesure de décliner son identité ou de la prouver, sans qu'il leur soit fait obligation par le présent règlement d'obtenir une autorisation préalable. Il peut s'agir, par exemple, d'une personne impliquée dans une infraction, qui ne veut pas ou ne peut pas divulguer son identité aux autorités répressives en raison d'un accident ou de son état de santé.

18. Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).
19. Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

(34) Afin de s'assurer que ces systèmes soient utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune des situations précisément répertoriées et rigoureusement définies, certains éléments devraient être pris en considération, notamment en ce qui concerne la nature de la situation donnant lieu à la demande et les conséquences de l'utilisation pour les droits et les libertés de toutes les personnes concernées, ainsi que les garanties et les conditions associées à l'utilisation. En outre, l'utilisation, à des fins répressives, de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public ne devrait être déployée que pour confirmer l'identité de la personne spécifiquement ciblée et elle devrait être limitée au strict nécessaire dans le temps, ainsi que du point de vue de la portée géographique et personnelle, eu égard en particulier aux preuves ou aux indications concernant les menaces, les victimes ou les auteurs. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public ne devrait être autorisée que si l'autorité répressive compétente a réalisé une analyse d'impact sur les droits fondamentaux et, sauf disposition contraire du présent règlement, a enregistré le système dans la base de données prévue par le présent règlement. La base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

(35) Toute utilisation d'un système d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives devrait être subordonnée à l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre dont la décision est contraignante. Cette autorisation devrait en principe être obtenue avant l'utilisation du système d'IA en vue d'identifier une ou plusieurs personnes. Des exceptions à cette règle devraient être autorisées dans des situations dûment justifiées en raison du caractère urgent, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant de commencer à utiliser le système d'IA. Dans de telles situations d'urgence, l'utilisation du système d'IA devrait être limitée au strict nécessaire et assortie de garanties et de conditions appropriées, telles qu'elles sont déterminées dans le droit national et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. En outre, l'autorité répressive devrait, dans ce genre de situation, solliciter une telle autorisation tout en indiquant les raisons pour lesquelles elle n'a pas été en mesure de le faire plus tôt, sans retard injustifié et au plus tard dans un délai de 24 heures. Lorsqu'une demande d'autorisation est rejetée, l'utilisation de systèmes d'identification biométrique en temps réel liés à cette autorisation devrait cesser immédiatement et toutes les données relatives à cette utilisation devraient être mises au rebut et supprimées. Ces données comprennent les données d'entrée directement acquises par un système d'IA au cours de l'utilisation de ce système, ainsi que les résultats et sorties de l'utilisation liée à cette autorisation. Cela ne devrait pas comprendre les entrées qui sont légalement acquises dans le respect d'un autre droit national ou du droit de l'Union. En tout état de cause, aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne devrait être prise sur la seule base des sorties du système d'identification biométrique à distance.

(36) Afin de s'acquitter de leurs tâches conformément aux exigences énoncées dans le présent règlement ainsi que dans les règles nationales, l'autorité de surveillance du marché concernée et l'autorité nationale chargée de la protection des données devraient être informées de chaque utilisation du système d'identification biométrique en temps réel. Les autorités de surveillance du marché et les autorités nationales chargées de la protection des données auxquelles une notification a été adressée devraient présenter à la Commission un rapport annuel sur l'utilisation des systèmes d'identification biométrique en temps réel.

cf. CNIL

(37) En outre, il convient de prévoir, dans le cadre exhaustif établi par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que dans le cas et dans la mesure où l'État membre concerné a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans des règles détaillées de son droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir une telle possibilité, ou de prévoir une telle possibilité uniquement pour certains objectifs parmi ceux susceptibles de justifier l'utilisation autorisée définis dans le présent règlement. Ces règles nationales devraient être notifiées à la Commission dans les 30 jours suivant leur adoption.

(38) L'utilisation de systèmes d'IA pour l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives passe nécessairement par le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, et qui sont fondées sur l'article 16 du traité sur le fonctionnement de l'Union européenne, devraient s'appliquer en tant que lex specialis pour ce qui est des règles sur le traitement des données biométriques figurant à l'article 10 de la directive (UE) 2016/680, réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible pour les autorités compétentes, lorsqu'elles agissent à des fins répressives en dehors de ce cadre, d'utiliser ces systèmes et de traiter ces données pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement ne vise pas à fournir la base juridique pour le traitement des données à caractère personnel en vertu de l'article 8 de la directive (UE) 2016/680. Cependant, l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique concernant l'utilisation à des fins répressives établi par le présent règlement. L'utilisation à des fins autres que répressives ne devrait donc pas être subordonnée à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées du droit national applicable susceptibles de donner effet à cette autorisation.

(39) Tout traitement de données biométriques et d'autres données à caractère personnel mobilisées lors de l'utilisation de systèmes d'IA pour l'identification biométrique, qui n'est pas lié à l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, réglementée par le présent règlement, devrait rester conforme à toutes les exigences découlant de l'article 10 de la directive (UE) 2016/680. À des fins autres que répressives, l'article 9, paragraphe 1, du règlement (UE) 2016/679 et l'article 10, paragraphe 1, du règlement (UE) 2018/1725 interdisent le traitement de données biométriques sous réserve d'exceptions limitées prévues dans ces articles. En application de l'article 9, paragraphe 1, du règlement (UE) 2016/679, l'utilisation de l'identification biométrique à distance à des fins autres que répressives a déjà fait l'objet de décisions d'interdiction prises par les autorité nationales chargées de la protection des données.

cf. **RGPD** art. 9.1

cf. **RGPD** art. 9.1

cf. CNIL

(40) Conformément à l'article 6 bis du protocole no 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande n'est pas liée par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et l'article 26, paragraphe 10, du présent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées.

(41) Conformément aux articles 2 et 2 bis du protocole no 22 sur la position du Danemark, annexé au traité l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et à l'article 26, paragraphe 10, du pré-

sent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne, ni soumis à leur application, lorsqu'elles concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne.

(42) Conformément à la présomption d'innocence, les personnes physiques dans l'Union devraient toujours être jugées sur leur comportement réel. Une personne physique ne devrait jamais être jugée sur la base d'un comportement prédit par l'IA uniquement sur la base de son profilage, de ses traits de personnalité ou de ses caractéristiques, telles que la nationalité, le lieu de naissance, le lieu de résidence, le nombre d'enfants, le niveau d'endettement ou le type de voiture, sans qu'il existe un motif raisonnable de soupçonner que cette personne est impliquée dans une activité criminelle sur la base de faits objectifs vérifiables et sans évaluation humaine de ceux-ci. Par conséquent, il convient d'interdire les évaluations des risques effectuées en ce qui concerne des personnes physiques dans le but d'évaluer la probabilité que ces dernières commettent une infraction ou de prévoir la survenance d'une infraction pénale, réelle ou potentielle, sur la seule base du profilage de ces personnes physiques ou de l'évaluation de leurs traits de personnalité et caractéristiques. En tout état de cause, cette interdiction ne vise ni ne concerne l'analyse des risques non fondée sur le profilage des personnes ou sur les traits de personnalité et les caractéristiques des individus, tels que les systèmes d'IA utilisant l'analyse des risques pour évaluer la probabilité de fraude financière de la part d'entreprises sur la base de transactions suspectes ou d'outils d'analyse des risques permettant de prédire la probabilité de la localisation de stupéfiants ou de marchandises illicites par les autorités douanières, par exemple sur la base de voies de trafic connues.

(43) Il y a lieu d'interdire la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance, parce que cette pratique ne fait qu'accentuer le sentiment de surveillance de masse et peut entraîner des violations flagrantes des droits fondamentaux, y compris du droit au respect de la vie privée.

(44) La base scientifique des systèmes d'IA visant à identifier ou à inférer les émotions suscite de vives inquiétudes, d'autant plus que l'expression des émotions varie considérablement d'une culture et d'une situation à l'autre, comme d'ailleurs chez un même individu. Les principaux défauts de ces systèmes sont, entre autres, leur fiabilité limitée, leur manque de précision et leur généralisabilité limitée. Par conséquent, les systèmes d'IA qui identifient ou déduisent les émotions ou les intentions de personnes physiques sur la base de leurs données biométriques peuvent conduire à des résultats discriminatoires et peuvent être intrusifs pour les droits et libertés des personnes concernées. Si l'on considère le déséquilibre de pouvoir qui existe dans le cadre du travail ou de l'enseignement, combiné au caractère intrusif de ces systèmes, ces derniers risqueraient de déboucher sur le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de personnes physiques. Par conséquent, il convient d'interdire la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à être utilisés pour déterminer l'état émotionnel de personnes physiques dans des situations liées au lieu de travail et à l'enseignement. Cette interdiction ne devrait pas porter sur les systèmes d'IA mis sur le marché strictement pour des raisons médicales ou de sécurité, tels que les systèmes destinés à un usage thérapeutique.

(45) Le présent règlement devrait être sans effet sur les pratiques interdites par le droit de l'Union, notamment en vertu du droit de la protection des données, de la lutte contre la discrimination, de la protection des consommateurs et de la concurrence.

(46) Les systèmes d'IA à haut risque ne devraient être mis sur le marché de l'Union, mis en service ou utilisés que s'ils satisfont à certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont les sorties sont utilisées d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour d'importants intérêts publics de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union. Sur la base du nouveau cadre législatif, que la Commission a détaillé dans sa communication présentant le «"Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022»[20], la règle

générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union, comme les règlements (UE) 2017/745[21] et (UE) 2017/746[22] du Parlement européen et du Conseil ou la directive 2006/42/CE du Parlement européen et du Conseil[23], peuvent s'appliquer à un produit dès lors que la mise à disposition ou la mise en service ne peut avoir lieu que lorsque le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Dans un souci de cohérence, et afin d'éviter des charges administratives ou des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement et de la législation d'harmonisation de l'Union dont la liste figure en annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de la législation d'harmonisation de l'Union. Les systèmes d'IA désignés comme étant à haut risque devraient être limités aux systèmes qui ont une incidence préjudiciable substantielle sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union et une telle limitation devrait réduire au minimum toute éventuelle restriction au commerce international.

(47) Les systèmes d'IA pourraient avoir un impact négatif sur la santé et la sécurité des citoyens, en particulier lorsque ces systèmes sont utilisés en tant que composants de sécurité de produits. Conformément aux objectifs de la législation d'harmonisation de l'Union visant à faciliter la libre circulation des produits sur le marché intérieur et à garantir que seuls des produits sûrs et conformes à d'autres égards soient mis sur le marché, il est important de dûment prévenir et atténuer les risques pour la sécurité susceptibles d'être créés par un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA. Par exemple, des robots de plus en plus autonomes, que ce soit dans le secteur de l'industrie manufacturière ou des services de soins et d'aide à autrui, devraient pouvoir opérer et remplir leurs fonctions en toute sécurité dans des environnements complexes. De même, dans le secteur de la santé, où les enjeux pour la vie et la santé sont particulièrement importants, les systèmes de diagnostic de plus en plus sophistiqués et les systèmes soutenant les décisions humaines devraient être fiables et précis.

(48) L'ampleur de l'incidence négative du système d'IA sur les droits fondamentaux protégés par la Charte est un critère particulièrement pertinent lorsqu'il s'agit de classer un système d'IA en tant que système à haut risque. Ces droits comprennent le droit à la dignité humaine, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'expression et d'information, la liberté de réunion et d'association, le droit à la non-discrimination, le droit à l'éducation, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, l'égalité de genre, les droits de propriété intellectuelle, le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence, et le droit à une bonne administration. En plus de ces droits, il est important de souligner le fait que les enfants bénéficient de droits spécifiques consacrés à l'article 24 de la Charte et dans la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale no 25 de la CNUDE en ce qui concerne l'environnement numérique), et que ces deux textes considèrent la prise en compte des vulnérabilités des enfants et la fourniture d'une protection et de soins appropriés comme nécessaires au bien-être de l'enfant. Le droit fondamental à un niveau élevé de protection de l'environnement, consacré dans la Charte et mis en œuvre dans les politiques de l'Union, devrait également être pris en considération lors de l'évaluation de la gravité du préjudice qu'un système d'IA peut causer, notamment en ce qui concerne les conséquences pour la santé et la sécurité des personnes.

20. JO C 247 du 29.6.2022, p. 1.
21. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) no 178/2002 et le règlement (CE) no 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).
22. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).
23. Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24).

(49) En ce qui concerne les systèmes d'IA à haut risque constituant des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes entrant dans le champ d'application du règlement (CE) no 300/2008 du Parlement européen et du Conseil[24], du règlement (UE) no 167/2013 du Parlement européen et du Conseil[25], du règlement (UE) no 168/2013 du Parlement européen et du Conseil[26], de la directive 2014/90/UE du Parlement européen et du Conseil[27], de la directive (UE) 2016/797 du Parlement européen et du Conseil[28], du règlement (UE) 2018/858 du Parlement européen et du Conseil[29], du règlement (UE) 2018/1139 du Parlement européen et du Conseil[30] ou du règlement (UE) 2019/2144 du Parlement européen et du Conseil[31], il convient de modifier ces actes pour veiller à ce que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec les mécanismes et les autorités de gouvernance, d'évaluation de la conformité et de contrôle de l'application déjà en place en vertu de ces règlements, des exigences obligatoires applicables aux systèmes d'IA à haut risque définis dans le présent règlement lors de l'adoption d'actes délégués ou d'actes d'exécution pertinents sur la base de ces actes.

(50) En ce qui concerne les systèmes d'IA qui constituent des composants de sécurité de produits relevant de certaines législations d'harmonisation de l'Union dont la liste figure en annexe du présent règlement, ou qui sont eux-mêmes de tels produits, il convient de les classer comme étant à haut risque au titre du présent règlement si le produit concerné est soumis à la procédure d'évaluation de la conformité par un organisme tiers d'évaluation de la conformité conformément à la législation d'harmonisation de l'Union correspondante. Ces produits sont notamment les machines, les jouets, les ascenseurs, les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles, les équipements radio, les équipements sous pression, les équipements pour bateaux de plaisance, les installations à câbles, les appareils brûlant des combustibles gazeux, les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro, l'automobile et l'aviation.

(51) La classification d'un système d'IA comme étant à haut risque en application du présent règlement ne devrait pas nécessairement signifier que le produit utilisant le système d'IA en tant que composant de sécurité, ou que le système d'IA lui-même en tant que produit, est considéré comme étant à haut risque selon les critères établis dans la législation d'harmonisation de l'Union correspondante qui s'applique au produit en question. Tel est notamment le cas pour le règlement (UE) 2017/745 et le règlement (UE) 2017/746, dans le cadre desquels une évaluation de la conformité par un tiers est prévue pour les produits à risque moyen et les produits à haut risque.

(52) En ce qui concerne les systèmes d'IA autonomes, à savoir les systèmes d'IA à haut risque autres que ceux qui constituent des composants de sécurité de produits ou

24. Règlement (CE) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) no 2320/2002 (JO L 97 du 9.4.2008, p. 72).
25. Règlement (UE) no 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1).
26. Règlement (UE) no 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52).
27. Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146).
28. Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44).
29. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).
30. Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) no 2111/2005, (CE) no 1008/2008, (UE) no 996/2010, (UE) no 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) no 552/2004 et (CE) no 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) no 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

qui sont eux-mêmes des produits, il convient de les classer comme étant à haut risque si, au vu de leur destination, ils présentent un risque élevé de causer un préjudice à la santé, à la sécurité ou aux droits fondamentaux des citoyens, en tenant compte à la fois de la gravité et de la probabilité du préjudice éventuel, et s'ils sont utilisés dans un certain nombre de domaines spécifiquement prédéfinis dans le présent règlement. La définition de ces systèmes est fondée sur la même méthode et les mêmes critères que ceux également envisagés pour toute modification ultérieure de la liste des systèmes d'IA à haut risque que la Commission devrait être habilitée à adopter, au moyen d'actes délégués, afin de tenir compte du rythme rapide de l'évolution technologique, ainsi que des changements potentiels dans l'utilisation des systèmes d'IA.

(53) Il importe également de préciser qu'il peut exister des cas spécifiques dans lesquels les systèmes d'IA visés dans des domaines prédéfinis spécifiés dans le présent règlement ne présentent pas un risque important d'atteinte aux intérêts juridiques protégés dans ces domaines parce qu'ils n'ont pas d'incidence substantielle sur la prise de décision ou ne causent pas de préjudice important à ces intérêts. Aux fins du présent règlement, il convient d'entendre par système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision un système d'IA qui n'a pas d'incidence sur la substance et, partant, sur le résultat de la prise de décision, qu'elle soit humaine ou automatisée. Dans les cas où une ou plusieurs des conditions ci-après sont remplies, il pourrait s'agir d'un système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision. La première de ces conditions devrait être que le système d'IA est destiné à accomplir une tâche procédurale étroite, comme transformer des données non structurées en données structurées, classer les documents entrants par catégories ou détecter les doublons parmi un grand nombre d'applications. Ces tâches sont par nature si étroites et limitées qu'elles ne présentent que des risques limités, qui ne sont pas exacerbés par une utilisation d'un système d'IA dans un contexte répertorié parmi les utilisations à haut risque dans la liste figurant en annexe du présent règlement. La deuxième condition devrait être que la tâche effectuée par le système d'IA est destinée à améliorer le résultat d'une activité humaine préalablement réalisée, susceptible d'être utile aux fins des utilisations à haut risque énumérées dans une annexe du présent règlement. Compte tenu de ces caractéristiques, le système d'IA n'ajoute qu'une couche supplémentaire à une activité humaine, ce qui présente par conséquent un risque réduit. Cette condition s'appliquerait par exemple aux systèmes d'IA destinés à améliorer la façon dont un document est rédigé, pour lui donner un ton professionnel ou un style académique ou pour l'adapter à un message de marque défini. La troisième condition devrait être que le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures. Le risque serait réduit parce que l'utilisation du système d'IA intervient après la réalisation d'une évaluation humaine et n'est pas destinée à se substituer à celle-ci ni à l'influencer, sans examen humain approprié. Il s'agit par exemple des systèmes d'IA qui, compte tenu de certaines constantes habituelles observées chez un enseignant au niveau de la notation, peuvent être utilisés pour vérifier a posteriori si l'enseignant s'est éventuellement écarté de ces constantes, de manière à signaler d'éventuelles incohérences ou anomalies. La quatrième condition devrait être que le système d'IA est destiné à exécuter une tâche qui n'est qu'un acte préparatoire à une évaluation pertinente aux fins des systèmes d'IA repris dans la liste figurant dans une annexe du présent règlement et, partant, la probabilité que les sorties produites par le système présentent un risque pour l'évaluation postérieure est très faible. Cette condition s'applique, entre autres, aux solutions intelligentes de traitement des fichiers, qui comprennent diverses fonctions telles que l'indexation, la recherche, le traitement de texte et le traitement de la parole ou le fait de relier des données à d'autres sources de données, ou aux systèmes d'IA utilisés pour la traduction de documents initiaux. En tout état de cause, les systèmes d'IA utilisés dans des cas d'utilisation à haut risque énumérés dans une annexe du présent règlement devraient être considérés comme présentant des risques importants de préjudice pour la santé, la sécurité ou les droits fon-

31. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) no 78/2009, (CE) no 79/2009 et (CE) no 661/2009 du Parlement européen et du Conseil et les règlements (CE) no 631/2009, (UE) no 406/2010, (UE) no 672/2010, (UE) no 1003/2010, (UE) no 1005/2010, (UE) no 1008/2010, (UE) no 1009/2010, (UE) no 19/2011, (UE) no 109/2011, (UE) no 458/2011, (UE) no 65/2012, (UE) no 130/2012, (UE) no 347/2012, (UE) no 351/2012, (UE) no 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

damentaux si le système d'IA implique un profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679, de l'article 3, point 4), de la directive (UE) 2016/680 et de l'article 3, point 5), du règlement (UE) 2018/1725. Afin de garantir la traçabilité et la transparence, un fournisseur qui considère qu'un système d'IA n'est pas à haut risque sur la base des conditions susvisées devrait documenter l'évaluation avant la mise sur le marché ou la mise en service de ce système et fournir cette documentation aux autorités nationales compétentes sur demande. Ce fournisseur devrait être tenu d'enregistrer le système d'IA dans la base de données de l'UE établie en vertu du présent règlement. En vue de fournir des orientations supplémentaires pour la mise en œuvre pratique des critères en fonction desquels des systèmes d'IA répertoriés dans la liste figurant dans une annexe du présent règlement sont, à titre exceptionnel, des systèmes qui ne sont pas à haut risque, la Commission devrait, après consultation du Comité IA, fournir des lignes directrices précisant cette mise en œuvre pratique, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

cf. RGPD art 4.4

(54) Étant donné que les données biométriques constituent une catégorie particulière de données à caractère personnel, il convient de classer comme étant à haut risque plusieurs cas d'utilisation critique des systèmes biométriques, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Le risque de tels résultats biaisés et d'effets discriminatoires est particulièrement important en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. Il convient par conséquent de classer les systèmes d'identification biométrique à distance comme étant à haut risque compte tenu des risques qu'ils présentent. Sont exclus de cette classification les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, parmi lesquelles l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. En outre, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés pour la catégorisation biométrique en fonction d'attributs ou de caractéristiques sensibles protégés en vertu de l'article 9, paragraphe 1, du règlement (UE) 2016/679 sur la base de données biométriques, dans la mesure où ils ne sont pas interdits par le présent règlement, et les systèmes de reconnaissance des émotions qui ne sont pas interdits en vertu du présent règlement. Les systèmes biométriques destinés à être utilisés uniquement dans le but de permettre la cybersécurité et les mesures de protection des données à caractère personnel ne devraient pas être considérés comme des systèmes d'IA à haut risque.

cf. RGPD art. 9.1

(55) En ce qui concerne la gestion et l'exploitation des infrastructures critiques, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans le cadre de la gestion et de l'exploitation des infrastructures numériques critiques visées à l'annexe, point 8, de la directive (UE) 2022/2557, du trafic routier et de l'approvisionnement en eau, gaz, électricité et chauffage, car leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations importantes dans le déroulement normal des activités sociales et économiques. Les composants de sécurité des infrastructures critiques, y compris des infrastructures numériques critiques, sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures critiques ou la santé et la sécurité des personnes et des biens, mais qui ne sont pas nécessaires au fonctionnement du système. La défaillance ou le mauvais fonctionnement de ces composants pourrait directement entraîner des risques pour l'intégrité physique des infrastructures critiques et, partant, des risques pour la santé et la sécurité des personnes et des biens. Les composants destinés à être utilisés uniquement à des fins de cybersécurité ne devraient pas être considérés comme des composants de sécurité. Les systèmes de surveillance de la pression de l'eau ou les systèmes de commande des alarmes incendie dans les centres d'informatique en nuage sont des exemples de composants de sécurité de ces infrastructures critiques.

(56) Le déploiement de systèmes d'IA dans l'éducation est important pour promouvoir une éducation et une formation numériques de qualité et pour permettre à tous les apprenants et enseignants d'acquérir et de partager les aptitudes et compétences numériques nécessaires, y compris l'éducation aux médias, ainsi que l'esprit critique, pour participer activement à l'économie, à la société et aux processus démocratiques. Tou-

tefois, les systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, en particulier pour déterminer l'accès ou l'admission, pour affecter des personnes à des établissements ou programmes d'enseignement et de formation professionnelle à tous les niveaux, pour évaluer les acquis d'apprentissage des personnes, pour évaluer le niveau d'enseignement approprié d'une personne et influencer substantiellement le niveau d'enseignement et de formation dont bénéficiera cette personne ou auquel elle pourra avoir accès ou pour surveiller les étudiants au cours des épreuves et détecter les comportements interdits dans ce cadre devraient être classés comme étant à haut risque, car ils peuvent déterminer le parcours éducatif et professionnel d'une personne et peut par conséquent avoir une incidence sur la capacité de cette personne à assurer sa propre subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent être particulièrement intrusifs et mener à des violations du droit à l'éducation et à la formation ainsi que du droit à ne pas subir de discriminations, et perpétuer des schémas historiques de discrimination, par exemple à l'encontre des femmes, de certains groupes d'âge, des personnes handicapées ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle.

(57) Les systèmes d'IA utilisés pour des questions liées à l'emploi, à la gestion de la main-d'œuvre et à l'accès à l'emploi indépendant, en particulier pour le recrutement et la sélection de personnes, pour la prise de décisions affectant les conditions des relations professionnelles, ainsi que la promotion et la résiliation des relations professionnelles contractuelles, pour l'attribution de tâches fondée sur le comportement individuel, les traits de personnalité ou les caractéristiques personnelles et pour le suivi ou l'évaluation des personnes dans le cadre de relations professionnelles contractuelles, devraient également être classés comme étant à haut risque car ces systèmes peuvent avoir une incidence considérable sur les perspectives de carrière et les moyens de subsistance de ces personnes ainsi que sur les droits des travailleurs. Les relations professionnelles contractuelles en question devraient concerner également, de manière significative, celles qui lient les employés et les personnes qui fournissent des services sur des plateformes telles que celles visées dans le programme de travail de la Commission pour 2021. Tout au long du processus de recrutement et lors de l'évaluation, de la promotion ou du maintien des personnes dans des relations professionnelles contractuelles, les systèmes d'IA peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge et des personnes handicapées, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent aussi porter atteinte à leurs droits fondamentaux à la protection des données et à la vie privée.

(58) Un autre domaine dans lequel l'utilisation des systèmes d'IA mérite une attention particulière est l'accès et le droit à certains services et prestations essentiels, publics et privés, devant permettre aux personnes de participer pleinement à la société ou d'améliorer leur niveau de vie. En particulier, les personnes physiques qui demandent à bénéficier ou bénéficient de prestations et services essentiels d'aide publique de la part des pouvoirs publics, à savoir des services de soins de santé, des prestations de sécurité sociale, des services sociaux fournissant une protection dans des cas tels que la maternité, la maladie, les accidents du travail, la dépendance ou la vieillesse et la perte d'emploi et l'aide sociale et au logement, sont généralement tributaires de ces prestations et services et se trouvent dans une situation vulnérable par rapport aux autorités compétentes. Lorsqu'ils sont utilisés pour déterminer si ces prestations et services devraient être accordés, refusés, réduits, révoqués ou récupérés par les autorités, y compris pour déterminer si les bénéficiaires y ont légitimement droit, les systèmes d'IA peuvent avoir une grande incidence sur les moyens de subsistance des personnes et porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, à la non-discrimination, à la dignité humaine ou à un recours effectif, et devraient donc être classés comme étant à haut risque. Néanmoins, le présent règlement ne devrait pas entraver la mise en place et l'utilisation, dans l'administration publique, d'approches innovantes qui bénéficieraient d'une utilisation plus large de systèmes d'IA conformes et sûrs, à condition que ces systèmes n'entraînent pas de risque élevé pour les personnes physiques et morales. En outre, les systèmes d'IA utilisés pour évaluer la note de crédit ou la solvabilité des personnes physiques devraient être classés en tant que systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes à des ressources financières ou à des services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à ces fins peuvent conduire à la discrimination entre personnes ou groupes et perpétuer des schémas historiques de discrimination, tels que ceux fondés sur les origines raciales ou ethniques, le sexe, les

handicaps, l'âge ou l'orientation sexuelle, ou peuvent créer de nouvelles formes d'incidences discriminatoires. Toutefois, les systèmes d'IA prévus par le droit de l'Union aux fins de détecter les fraudes dans l'offre de services financiers et à des fins prudentielles pour calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance ne devraient pas être considérés comme étant à haut risque au titre du présent règlement. Par ailleurs, les systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-santé et vie peuvent avoir une incidence significative sur les moyens de subsistance de ces personnes et, s'ils ne sont pas dûment conçus, développés et utilisés, peuvent porter atteinte à leurs droits fondamentaux et entraîner de graves conséquences pour leur vie et leur santé, y compris l'exclusion financière et la discrimination. Enfin, les systèmes d'IA utilisés pour évaluer et hiérarchiser les appels d'urgence émis par des personnes physiques ou pour envoyer des services d'intervention d'urgence ou établir des priorités dans l'envoi de tels services, y compris la police, les pompiers et les secours, ainsi que dans l'utilisation des systèmes de tri des patients admis dans les services de santé d'urgence, devraient aussi être classés comme étant à haut risque car ils prennent des décisions dans des situations très critiques pour la vie, la santé et les biens des personnes.

(59) Compte tenu du rôle et de la responsabilité des autorités répressives, les actions menées par celles-ci qui supposent certaines utilisations de systèmes d'IA sont caractérisées par un degré important de déséquilibre des forces et peuvent conduire à la surveillance, à l'arrestation ou à la privation de la liberté d'une personne physique ainsi qu'à d'autres conséquences négatives sur des droits fondamentaux garantis par la Charte. En particulier, si le système d'IA n'est pas entraîné avec des données de haute qualité, ne répond pas aux exigences voulues en termes de performance, d'exactitude ou de robustesse, ou n'est pas correctement conçu et testé avant d'être mis sur le marché ou mis en service, il risque de traiter des personnes de manière discriminatoire ou, plus généralement, incorrecte ou injuste. En outre, l'exercice de droits fondamentaux procéduraux importants, tels que le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que les droits de la défense et la présomption d'innocence, pourrait être entravé, en particulier lorsque ces systèmes d'IA ne sont pas suffisamment transparents, explicables et documentés. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, un certain nombre de systèmes d'IA destinés à être utilisés dans un contexte répressif où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter des conséquences négatives, conserver la confiance du public et garantir que des comptes soient rendus et que des recours puissent être exercés. Compte tenu de la nature des activités et des risques y afférents, ces systèmes d'IA à haut risque devraient inclure en particulier les systèmes d'IA destinés à être utilisés par les autorités répressives ou pour leur compte ou par les institutions, organes et organismes de l'Union pour aider les autorités répressives à évaluer le risque qu'une personne physique ne devienne victime d'infractions pénales, tels que les polygraphes et instruments similaires, à évaluer la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites relatives à des infractions pénales, et, dans la mesure où cela n'est pas interdit par le présent règlement, à évaluer le risque d'infraction ou de récidive d'une personne physique non seulement sur la base du profilage de personnes physiques, mais aussi sur la base de l'évaluation des traits de personnalité, des caractéristiques ou des antécédents judiciaires de personnes physiques ou de groupes, à des fins de profilage dans le cadre de la détection d'infractions pénales, d'enquêtes et de poursuites en la matière. Les systèmes d'IA spécifiquement destinés à être utilisés pour des procédures administratives par les autorités fiscales et douanières ainsi que par les cellules de renseignement financier effectuant des tâches administratives d'analyse d'informations dans le cadre de la législation de l'Union relative à la lutte contre le blanchiment des capitaux ne devraient pas être classés comme des systèmes d'IA à haut risque utilisés par les autorités répressives à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. L'utilisation des outils d'IA par les autorités répressives et d'autres autorités pertinentes ne devrait pas devenir un facteur d'inégalité ou d'exclusion. Les conséquences de l'utilisation des outils d'IA sur les droits de la défense des suspects ne devraient pas être ignorées, en particulier la difficulté d'obtenir des informations utiles sur le fonctionnement de ces outils et, partant, la difficulté de saisir la justice pour contester leurs résultats, en particulier pour les personnes physiques faisant l'objet d'une enquête.

(60) Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières touchent des personnes qui se trouvent souvent

dans une situation particulièrement vulnérable et qui sont tributaires du résultat des actions des autorités publiques compétentes. L'exactitude, la nature non discriminatoire et la transparence des systèmes d'IA utilisés dans ces contextes sont donc particulièrement importantes pour garantir le respect des droits fondamentaux des personnes concernées, en particulier leurs droits à la libre circulation, à la non-discrimination, à la protection de la vie privée et des données à caractère personnel, à une protection internationale et à une bonne administration. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou pour leur compte ou par les institutions, organes et organismes de l'Union chargés de tâches dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières, tels que les polygraphes et instruments similaires, pour évaluer certains risques présentés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ou l'asile, et pour aider les autorités publiques compétentes à procéder à l'examen, y compris l'évaluation connexe de la fiabilité des éléments de preuve, des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, aux fins de détecter, de reconnaître ou d'identifier des personnes physiques dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, à l'exception de la vérification des documents de voyage. Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières couverts par le présent règlement devraient être conformes aux exigences procédurales pertinentes fixées par le règlement (CE) no 810/2009 du Parlement européen et du Conseil[32], la directive 2013/32/UE du Parlement européen et du Conseil[33] et tout autre acte législatif pertinent de l'Union. Les systèmes d'IA ne devraient en aucun cas être utilisés par les États membres ou les institutions, organes ou organismes de l'Union dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières comme moyen de contourner les obligations internationales qui leur incombent en vertu de la convention des Nations unies relative au statut des réfugiés, signée à Genève le 28 juillet 1951, telle que modifiée par le protocole du 31 janvier 1967. Ils ne devraient pas non plus être utilisés pour enfreindre de quelque manière que ce soit le principe de non-refoulement ou pour refuser des voies d'accès légales sûres et effectives au territoire de l'Union, y compris le droit à la protection internationale.

(61) Certains systèmes d'IA destinés à être utilisés pour l'administration de la justice et les processus démocratiques devraient être classés comme étant à haut risque, compte tenu de leur incidence potentiellement significative sur la démocratie, l'état de droit, les libertés individuelles ainsi que le droit à un recours effectif et à accéder à un tribunal impartial. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés par une autorité judiciaire ou pour le compte de celle-ci pour aider les autorités judiciaires à rechercher et à interpréter les faits et la loi, et à appliquer la loi à un ensemble concret de faits. Les systèmes d'IA destinés à être utilisés par des organismes de règlement extrajudiciaire des litiges à ces fins devraient également être considérés comme étant à haut risque lorsque les résultats des procédures de règlement extrajudiciaire des litiges produisent des effets juridiques pour les parties. L'utilisation d'outils d'IA peut soutenir le pouvoir de décision des juges ou l'indépendance judiciaire, mais ne devrait pas les remplacer, car la décision finale doit rester une activité humaine. La classification des systèmes d'IA comme étant à haut risque ne devrait cependant pas s'étendre aux systèmes d'IA destinés à être utilisés pour des activités administratives purement accessoires qui n'ont aucune incidence sur l'administration réelle de la justice dans des cas individuels, telles que l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre membres du personnel ou les tâches administratives.

(62) Sans préjudice des règles prévues dans le règlement (UE) 2024/900 du Parlement européen et du Conseil[34], et afin de faire face aux risques d'ingérence extérieure indue dans le droit de vote consacré à l'article 39 de la Charte et d'effets négatifs sur la

32. Règlement (CE) no 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).
33. Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 180 du 29.6.2013, p. 60).

démocratie et l'état de droit, les systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums devraient être classés comme étant à haut risque, à l'exception des systèmes d'IA dont les sorties ne touchent pas directement les personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique.

(63) Le fait qu'un système d'IA soit classé comme étant à haut risque au titre du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est licite au titre d'autres actes législatifs de l'Union ou au titre du droit national compatible avec le droit de l'Union, concernant notamment la protection des données à caractère personnel ou l'utilisation de polygraphes et d'instruments similaires ou d'autres systèmes d'analyse de l'état émotionnel des personnes physiques. Toute utilisation de ce type devrait continuer à être subordonnée aux exigences applicables découlant de la Charte et des actes applicables du droit dérivé de l'Union et du droit national. Le présent règlement ne saurait être considéré comme constituant un fondement juridique pour le traitement des données à caractère personnel, y compris des catégories particulières de données à caractère personnel, le cas échéant, sauf disposition contraire expresse du présent règlement.

(64) Afin d'atténuer les risques liés aux systèmes d'IA à haut risque mis sur le marché ou mis en service et de garantir un niveau élevé de fiabilité, certaines exigences obligatoires devraient s'appliquer aux systèmes d'IA à haut risque, en tenant compte de la destination du système d'IA et du contexte de son utilisation et en fonction du système de gestion des risques à mettre en place par le fournisseur. Les mesures adoptées par les fournisseurs pour se conformer aux exigences obligatoires du présent règlement devraient tenir compte de l'état de la technique généralement reconnu en matière d'IA, et être proportionnées et effectives pour atteindre les objectifs du présent règlement. Reposant sur le nouveau cadre législatif, tel que précisé dans la communication de la Commission intitulée «"Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022», la règle générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union peuvent être applicables à un produit donné, étant donné que la mise à disposition ou la mise en service ne peut avoir lieu que si le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Les dangers des systèmes d'IA couverts par les exigences du présent règlement concernent des aspects différents de ceux qui sont énoncés dans la législation d'harmonisation existante de l'Union, et, par conséquent, les exigences du présent règlement compléteraient l'ensemble existant de la législation d'harmonisation de l'Union. Par exemple, les machines ou les dispositifs médicaux incorporant un système d'IA peuvent présenter des risques qui ne sont pas couverts par les exigences essentielles en matière de santé et de sécurité énoncées dans la législation harmonisée pertinente de l'Union, étant donné que cette législation sectorielle ne traite pas des risques spécifiques aux systèmes d'IA. Cela implique d'appliquer conjointement et de manière complémentaire les divers actes législatifs. Dans un souci de cohérence, et afin d'éviter une charge administrative et des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif et dont la liste figure dans une annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de cette législation harmonisée de l'Union. Cette souplesse pourrait signifier, par exemple, que le fournisseur décide d'intégrer une partie des processus d'essai et de déclaration nécessaires, ainsi que des informations et de la documentation requises en vertu du présent règlement dans la documentation et les procédures existantes requises en vertu de la législation d'harmonisation de l'Union en vigueur reposant sur le nouveau cadre législatif et dont la liste figure en annexe du présent règlement. Cela ne devrait en aucun cas porter atteinte à l'obligation qu'a le fournisseur de se conformer à toutes les exigences applicables.

34. Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique (JO L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

(65) Le système de gestion des risques devrait consister en un processus itératif continu planifié et se dérouler sur l'ensemble du cycle de vie d'un système d'IA à haut risque. Ce processus devrait viser à identifier et à atténuer les risques des systèmes d'IA qui se posent pour la santé, la sécurité et les droits fondamentaux. Le système de gestion des risques devrait être régulièrement réexaminé et mis à jour afin de garantir le maintien de son efficacité, ainsi que la justification et la documentation de toutes les décisions et mesures importantes prises en vertu du présent règlement. Ce processus devrait garantir que le fournisseur détermine les risques ou les incidences négatives et mette en œuvre des mesures d'atténuation des risques connus et raisonnablement prévisibles des systèmes d'IA pour la santé, la sécurité et les droits fondamentaux à la lumière de leur destination et de leur mauvaise utilisation raisonnablement prévisible, y compris les risques éventuels découlant de l'interaction entre les systèmes d'IA et l'environnement dans lequel ils fonctionnent. Le système de gestion des risques devrait adopter les mesures de gestion des risques les plus appropriées à la lumière de l'état de la technique en matière d'IA. Lorsqu'il détermine les mesures de gestion des risques les plus appropriées, le fournisseur devrait documenter et expliquer les choix effectués et, le cas échéant, associer des experts et des parties prenantes externes. Lorsqu'il s'agit de déterminer la mauvaise utilisation raisonnablement prévisible des systèmes d'IA à haut risque, le fournisseur devrait couvrir les utilisations des systèmes d'IA dont on peut raisonnablement prévoir, bien qu'elles ne soient pas directement couvertes par la destination et prévues dans la notice d'utilisation, qu'elles résultent d'un comportement humain aisément prévisible dans le contexte des caractéristiques et de l'utilisation spécifiques d'un système d'IA donné. Toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé, la sécurité ou les droits fondamentaux, devraient figurer dans la notice d'utilisation fournie par le fournisseur. Il s'agit de veiller à ce que le déployeur en ait connaissance et en tienne compte lors de l'utilisation du système d'IA à haut risque. La détermination et la mise en œuvre de mesures d'atténuation des risques en cas de mauvaise utilisation prévisible au titre du présent règlement ne devraient pas nécessiter de la part du fournisseur, pour remédier à la mauvaise utilisation prévisible, des mesures d'entraînement supplémentaires spécifiques pour le système d'IA à haut risque. Les fournisseurs sont toutefois encouragés à envisager de telles mesures d'entraînement supplémentaires pour atténuer les mauvaises utilisations raisonnablement prévisibles, si cela est nécessaire et approprié.

cf. déployeurs

(66) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la gestion des risques, la qualité et la pertinence des jeux de données utilisés, la documentation technique et la tenue de registres, la transparence et la fourniture d'informations aux déployeurs, le contrôle humain, ainsi que la robustesse, l'exactitude et la sécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux. Aucune autre mesure moins contraignante pour le commerce n'étant raisonnablement disponible, ces exigences ne constituent pas des restrictions injustifiées aux échanges.

cf. déployeurs

(67) Les données de haute qualité et l'accès à ces données jouent un rôle essentiel pour ce qui est de fournir une structure et d'assurer le bon fonctionnement de nombreux systèmes d'IA, en particulier lorsque des techniques axées sur l'entraînement de modèles sont utilisées, afin de garantir que le système d'IA à haut risque fonctionne comme prévu et en toute sécurité et qu'il ne devient pas une source de discrimination interdite par le droit de l'Union. Les jeux de données d'entraînement, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques de gouvernance et de gestion des données appropriées. Les jeux de données d'entraînement, de validation et de test, y compris les étiquettes, devraient être pertinents, suffisamment représentatifs et, dans toute la mesure du possible, exempts d'erreurs et complets au regard de la destination du système. Afin de faciliter le respect du droit de l'Union sur la protection des données, tel que le règlement (UE) 2016/679, les pratiques en matière de gouvernance et de gestion des données devraient inclure, dans le cas des données à caractère personnel, la transparence quant à la finalité initiale de la collecte des données. Les jeux de données devraient également posséder les propriétés statistiques voulues, y compris en ce qui concerne les personnes ou groupes de personnes pour lesquels le système d'IA à haut risque est destiné à être utilisé, en accordant une attention particulière à l'atténuation des éventuels biais dans les jeux de données qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées

cf. RGPD

pour les opérations futures («boucles de rétroaction»). Des biais peuvent, par exemple, être inhérents à des jeux de données sous-jacents, en particulier lorsque des données historiques sont utilisées, ou générés lorsque les systèmes sont mis en œuvre dans des conditions réelles. Les résultats produits par les systèmes d'IA pourraient être influencés par ces biais inhérents, qui ont tendance à se renforcer progressivement et ainsi à perpétuer et à amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes vulnérables, y compris les groupes ethniques ou raciaux. L'exigence selon laquelle les jeux de données doivent être dans toute la mesure du possible complets et exempts d'erreurs ne devrait pas avoir d'effet sur l'utilisation de techniques respectueuses de la vie privée dans le contexte du développement et de la mise à l'essai des systèmes d'IA. En particulier, les jeux de données devraient prendre en considération, dans la mesure requise au regard de leur destination, les propriétés, les caractéristiques ou les éléments qui sont propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA est destiné à être utilisé. Les exigences relatives à la gouvernance des données peuvent être respectées en faisant appel à des tiers qui proposent des services de conformité certifiés, y compris la vérification de la gouvernance des données, l'intégrité des jeux de données et les pratiques d'entraînement, de validation et de mise à l'essai des données, dans la mesure où le respect des exigences du présent règlement en matière de données est garanti.

(68) Pour le développement et l'évaluation de systèmes d'IA à haut risque, certains acteurs, tels que les fournisseurs, les organismes notifiés et d'autres entités concernées, telles que les pôles européens d'innovation numérique, les installations d'expérimentation et d'essai et les centres de recherche, devraient être en mesure d'avoir accès à des jeux de données de haute qualité dans leurs domaines d'activité liés au présent règlement et d'utiliser de tels jeux de données. Les espaces européens communs des données créés par la Commission et la facilitation du partage de données d'intérêt public entre les entreprises et avec le gouvernement seront essentiels pour fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA. Par exemple, dans le domaine de la santé, l'espace européen des données de santé facilitera l'accès non discriminatoire aux données de santé et l'entraînement d'algorithmes d'IA à l'aide de ces jeux de données, d'une manière respectueuse de la vie privée, sûre, rapide, transparente et digne de confiance, et avec une gouvernance institutionnelle appropriée. Les autorités compétentes concernées, y compris les autorités sectorielles, qui fournissent ou facilitent l'accès aux données peuvent aussi faciliter la fourniture de données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA.

(69) Le droit au respect de la vie privée et à la protection des données à caractère personnel doit être garanti tout au long du cycle de vie du système d'IA. À cet égard, les principes de minimisation et de protection des données dès la conception et par défaut, tels qu'énoncés dans le droit de l'Union sur la protection des données, sont applicables lorsque des données à caractère personnel sont traitées. Les mesures prises par les fournisseurs pour garantir le respect de ces principes peuvent inclure non seulement l'anonymisation et le cryptage, mais aussi l'utilisation d'une technologie qui permet l'introduction d'algorithmes dans les données ainsi que l'entraînement des systèmes d'IA sans transmission entre parties ou copie des données brutes ou structurées elles-mêmes, sans préjudice des exigences en matière de gouvernance des données prévues par le présent règlement.

(70) Afin de protéger le droit d'autrui contre la discrimination qui pourrait résulter des biais dans les systèmes d'IA, les fournisseurs devraient, à titre exceptionnel, et dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques et à la suite de l'application de toutes les conditions applicables prévues par le présent règlement en plus des conditions énoncées dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680, être en mesure de traiter également des catégories particulières de données à caractère personnel, pour des raisons d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et de l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725.

cf. RGPD

cf. RGPD art. 9.2.g

(71) Il est essentiel de disposer d'informations compréhensibles sur la manière dont les systèmes d'IA à haut risque ont été développés et sur leur fonctionnement tout au long

de leur durée de vie afin de permettre la traçabilité de ces systèmes, de vérifier le respect des exigences du présent règlement et de surveiller le fonctionnement des systèmes en question et d'assurer leur surveillance après commercialisation. Cela nécessite la tenue de registres et la disponibilité d'une documentation technique contenant les informations nécessaires pour évaluer la conformité du système d'IA avec les exigences pertinentes et faciliter la surveillance après commercialisation. Ces informations devraient notamment porter sur les caractéristiques générales, les capacités et les limites du système, sur les algorithmes, les données et les processus d'entraînement, de mise à l'essai et de validation utilisés, ainsi que sur le système de gestion des risques mis en place et être établies de façon claire et exhaustive. La documentation technique devrait être dûment tenue à jour tout au long de la durée de vie du système d'IA. Par ailleurs, les systèmes d'IA à haut risque devraient permettre, sur le plan technique, l'enregistrement automatique des événements, au moyen de journaux, tout au long de la durée de vie du système.

(72) Afin de répondre aux préoccupations liées à l'opacité et à la complexité de certains systèmes d'IA et d'aider les déployeurs à remplir les obligations qui leur incombent en vertu du présent règlement, la transparence devrait être requise pour les systèmes d'IA à haut risque avant leur mise sur le marché ou leur mise en service. Les systèmes d'IA à haut risque devraient être conçus de manière à permettre aux déployeurs de comprendre le fonctionnement du système d'IA, d'évaluer sa fonctionnalité et de comprendre ses forces et ses limites. Les systèmes d'IA à haut risque devraient être accompagnés d'informations appropriées sous la forme d'une notice d'utilisation. Ces informations devraient inclure les caractéristiques, les capacités et les limites de la performance du système d'IA. Il s'agirait des informations sur les éventuelles circonstances connues et prévisibles liées à l'utilisation du système d'IA à haut risque, y compris l'action des déployeurs susceptible d'influencer le comportement et la performance du système, dans le cadre desquelles le système d'IA peut entraîner des risques pour la santé, la sécurité et les droits fondamentaux, sur les changements qui ont été déterminés au préalable et évalués à des fins de conformité par le fournisseur et sur les mesures de contrôle humain pertinentes, y compris les mesures visant à faciliter l'interprétation des sorties du système d'IA par les déployeurs. La transparence, y compris la notice d'utilisation jointe au système, devrait aider les déployeurs à utiliser celui-ci et à prendre des décisions en connaissance de cause. Les déployeurs devraient, entre autres, être mieux à même de faire le bon choix quant au système qu'ils ont l'intention d'utiliser à la lumière des obligations qui leur sont applicables, d'être informés sur les utilisations prévues et interdites et d'utiliser le système d'IA correctement et le cas échéant. Afin d'améliorer la lisibilité et l'accessibilité des informations figurant dans la notice d'utilisation, il convient, le cas échéant, d'inclure des exemples illustratifs, par exemple sur les limitations et sur les utilisations prévues et interdites du système d'IA. Les fournisseurs devraient veiller à ce que toute la documentation, y compris la notice d'utilisation, contienne des informations utiles, complètes, accessibles et compréhensibles, compte tenu des besoins et des connaissances prévisibles des déployeurs visés. La notice d'utilisation devrait être mise à disposition dans une langue aisément compréhensible par les déployeurs visés, déterminée par l'État membre concerné.

cf. déployeurs

(73) Les systèmes d'IA à haut risque devraient être conçus et développés de manière à ce que les personnes physiques puissent superviser leur fonctionnement et veiller à ce qu'ils soient utilisés comme prévu et à ce que leurs incidences soient prises en compte tout au long de leur cycle de vie. À cette fin, des mesures appropriées de contrôle humain devraient être établies par le fournisseur du système avant sa mise sur le marché ou sa mise en service. En particulier, le cas échéant, de telles mesures devraient garantir que le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent pas être ignorées par le système lui-même, que le système répond aux ordres de l'opérateur humain et que les personnes physiques auxquelles le contrôle humain a été confié ont les compétences, la formation et l'autorité nécessaires pour s'acquitter de ce rôle. Il est également essentiel, le cas échéant, de veiller à ce que les systèmes d'IA à haut risque comprennent des mécanismes destinés à guider et à informer une personne physique à laquelle le contrôle humain a été confié, afin qu'elle puisse décider en connaissance de cause s'il faut intervenir, à quel moment et de quelle manière, pour éviter des conséquences négatives ou des risques, ou arrêter le système s'il ne fonctionne pas comme prévu. Compte tenu des conséquences importantes pour les personnes en cas d'erreur dans les correspondances établies par certains systèmes d'identification biométrique, il convient de prévoir pour ces systèmes une exigence de contrôle humain accru, de manière qu'aucune mesure ou décision ne puisse être prise

par le déployeur sur la base de l'identification obtenue par le système, à moins qu'elle n'ait été vérifiée et confirmée séparément par au moins deux personnes physiques. Ces personnes pourraient provenir d'une ou de plusieurs entités et compter parmi elles la personne qui fait fonctionner le système ou l'utilise. Cette exigence ne devrait pas entraîner de charges ou de retards inutiles, et il pourrait suffire que les vérifications effectuées séparément par les différentes personnes soient automatiquement enregistrées dans les journaux générés par le système. Compte tenu des spécificités des domaines que sont les activités répressives, la migration, les contrôles aux frontières et l'asile, cette exigence ne devrait pas s'appliquer lorsque le droit de l'Union ou le droit national considère que cette application est disproportionnée.

(74) Les systèmes d'IA à haut risque devraient produire des résultats d'une qualité constante tout au long de leur cycle de vie et assurer un niveau approprié d'exactitude, de robustesse et de cybersécurité, au vu de leur destination et conformément à l'état de la technique généralement reconnu. La Commission et les organisations et parties prenantes concernées sont encouragées à tenir dûment compte de l'atténuation des risques et des incidences négatives du système d'IA. Le niveau attendu des indicateurs de performance devrait être indiqué dans la notice d'utilisation jointe au système. Les fournisseurs sont instamment invités à communiquer ces informations aux déployeurs d'une manière claire et aisément compréhensible, sans malentendus ou déclarations trompeuses. Le droit de l'Union en matière de métrologie légale, y compris les directives 2014/31/UE[35] et 2014/32/UE[36] du Parlement européen et du Conseil, vise à garantir l'exactitude des mesures et à contribuer à la transparence et à la loyauté des transactions commerciales. Dans ce contexte, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, la Commission devrait encourager, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure pour les systèmes d'IA. Ce faisant, la Commission devrait prendre note des partenaires internationaux travaillant sur la métrologie et les indicateurs de mesure pertinents relatifs à l'IA et collaborer avec ceux-ci.

cf. déployeurs

(75) La robustesse technique est une exigence essentielle pour les systèmes d'IA à haut risque. Il convient qu'ils soient résilients face aux comportements préjudiciables ou, plus généralement, indésirables pouvant résulter de limites intrinsèques aux systèmes ou dues à l'environnement dans lequel les systèmes fonctionnent (par exemple les erreurs, les défaillances, les incohérences et les situations inattendues). Par conséquent, des mesures techniques et organisationnelles devraient être prises pour garantir la robustesse des systèmes d'IA à haut risque, par exemple en concevant et développant des solutions techniques appropriées pour prévenir ou réduire au minimum les comportements préjudiciables ou, plus généralement, indésirables. Ces solutions techniques peuvent comprendre, par exemple, des mécanismes permettant au système d'interrompre son fonctionnement en toute sécurité (mesures de sécurité après défaillance) en présence de certaines anomalies ou en cas de fonctionnement en dehors de certaines limites déterminées au préalable. L'absence de protection contre ces risques pourrait avoir des incidences sur la sécurité ou entraîner des violations des droits fondamentaux, par exemple en raison de décisions erronées ou de sorties inexactes ou biaisées générées par le système d'IA.

(76) La cybersécurité joue un rôle crucial pour ce qui est de garantir la résilience des systèmes d'IA face aux tentatives de détourner leur utilisation, leur comportement ou leur performance ou de compromettre leurs propriétés de sûreté par des tiers malveillants exploitant les vulnérabilités du système. Les cyberattaques contre les systèmes d'IA peuvent passer par des ressources propres à l'IA, telles que les jeux de données d'entraînement (par exemple pour l'empoisonnement de données) ou l'entraînement des modèles (par exemple pour des attaques contradictoires ou des attaques par inférence d'appartenance), ou exploiter les vulnérabilités des ressources numériques du système d'IA ou de l'infrastructure TIC sous-jacente. Pour garantir un niveau de cybersécurité adapté aux risques, des mesures appropriées, telles que des contrôles de

35. Directive 2014/31/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des instruments de pesage à fonctionnement non automatique (JO L 96 du 29.3.2014, p. 107).
36. Directive 2014/32/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'instruments de mesure (JO L 96 du 29.3.2014, p. 149).

sécurité, devraient donc être prises par les fournisseurs de systèmes d'IA à haut risque, en tenant également compte, si nécessaire, de l'infrastructure TIC sous-jacente.

(77) Sans préjudice des exigences relatives à la robustesse et à l'exactitude énoncées dans le présent règlement, les systèmes d'IA à haut risque qui relèvent du champ d'application du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, conformément audit règlement, peuvent démontrer leur conformité avec les exigences de cybersécurité du présent règlement en satisfaisant aux exigences essentielles de cybersécurité énoncées audit règlement. Lorsqu'ils satisfont aux exigences essentielles du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, les systèmes d'IA à haut risque devraient être réputés conformes aux exigences de cybersécurité énoncées dans le présent règlement dans la mesure où le respect de ces exigences est démontré dans la déclaration UE de conformité, ou dans des parties de celle-ci, délivrée en vertu dudit règlement. À cette fin, l'évaluation des risques en matière de cybersécurité associés à un produit comportant des éléments numériques classé comme système d'IA à haut risque conformément au présent règlement, effectuée en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, devrait tenir compte des risques pesant sur la cyberrésilience d'un système d'IA en ce qui concerne les tentatives de tiers non autorisés de modifier son utilisation, son comportement ou sa performance, y compris les vulnérabilités spécifiques à l'IA telles que l'empoisonnement des données ou les attaques hostiles, ainsi que, le cas échéant, les risques pesant sur les droits fondamentaux, comme l'exige le présent règlement.

(78) La procédure d'évaluation de la conformité prévue par le présent règlement devrait s'appliquer en ce qui concerne les exigences essentielles de cybersécurité d'un produit comportant des éléments numériques relevant du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et classé comme système d'IA à haut risque en vertu du présent règlement. Toutefois, l'application de cette règle ne devrait pas entraîner de réduction du niveau d'assurance nécessaire pour les produits critiques comportant des éléments numériques couverts par le règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques. Par conséquent, par dérogation à cette règle, les systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et sont également considérés comme des produits critiques importants comportant des éléments numériques en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe du présent règlement, sont soumis aux dispositions relatives à l'évaluation de la conformité du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques en ce qui concerne les exigences essentielles de cybersécurité énoncées dans ledit règlement. Dans ce cas, les dispositions respectives relatives à l'évaluation de la conformité fondée sur le contrôle interne énoncées à l'annexe du présent règlement devraient s'appliquer à tous les autres aspects couverts par le présent règlement. En s'appuyant sur les connaissances et l'expertise de l'ENISA en ce qui concerne la politique de cybersécurité et les tâches qui lui sont confiées en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil[37], la Commission devrait coopérer avec l'ENISA sur les questions liées à la cybersécurité des systèmes d'IA.

(79) Il convient qu'une personne physique ou morale spécifique, définie comme étant le fournisseur, assume la responsabilité de la mise sur le marché ou de la mise en service d'un système d'IA à haut risque, indépendamment du fait que cette personne physique ou morale soit ou non la personne qui a conçu ou développé le système.

37. Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

(80) En leur qualité de signataires de la convention des Nations unies relative aux droits des personnes handicapées, l'Union et les États membres sont légalement tenus de protéger les personnes handicapées contre la discrimination et de promouvoir leur égalité, de veiller à ce que les personnes handicapées aient accès, au même titre que les autres, aux technologies et aux systèmes d'information et de communication, ainsi que de garantir le respect de leur vie privée. Compte tenu de l'importance et de l'utilisation croissantes des systèmes d'IA, l'application des principes de conception universelle à toutes les nouvelles technologies et à tous les nouveaux services devrait garantir un accès complet et égal à toute personne potentiellement concernée par les technologies d'IA ou les utilisant, y compris les personnes handicapées, d'une manière qui tienne pleinement compte de leur dignité et de leur diversité intrinsèques. Il est donc essentiel que les fournisseurs garantissent la pleine conformité avec les exigences en matière d'accessibilité, y compris la directive (UE) 2016/2102 du Parlement européen et du Conseil[38] et la directive (UE) 2019/882. Les fournisseurs devraient veiller au respect de ces exigences dès la conception. Les mesures nécessaires devraient donc être aussi intégrées que possible dans la conception des systèmes d'IA à haut risque.

(81) Le fournisseur devrait mettre en place un système solide de gestion de la qualité, garantir le respect de la procédure d'évaluation de la conformité requise, rédiger la documentation pertinente et mettre en place un système solide de surveillance après commercialisation. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations en matière de systèmes de gestion de la qualité en vertu du droit sectoriel pertinent de l'Union devraient avoir la possibilité d'intégrer les éléments du système de gestion de la qualité prévus par le présent règlement dans le système de gestion de la qualité existant prévu dans cet autre droit sectoriel de l'Union. La complémentarité entre le présent règlement et le droit sectoriel existant de l'Union devrait également être prise en compte dans les futures activités ou orientations de normalisation de la Commission. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque destinés à être utilisés exclusivement par elles peuvent adopter et mettre en œuvre les règles relatives au système de gestion de la qualité dans le cadre du système de gestion de la qualité adopté au niveau national ou régional, selon le cas, en tenant compte des spécificités du secteur, ainsi que des compétences et de l'organisation de l'autorité publique concernée.

(82) Pour permettre le contrôle de l'application du présent règlement et créer des conditions de concurrence équitables pour les opérateurs, et compte tenu des différentes formes de mise à disposition des produits numériques, il est important de veiller à ce que, en toutes circonstances, une personne établie dans l'Union puisse fournir aux autorités toutes les informations nécessaires sur la conformité d'un système d'IA. Par conséquent, avant de mettre leurs systèmes d'IA à disposition dans l'Union, les fournisseurs établis dans des pays tiers devraient nommer, par mandat écrit, un mandataire établi dans l'Union. Ce mandataire joue un rôle capital en ce sens qu'il veille à la conformité des systèmes d'IA à haut risque mis sur le marché ou mis en service dans l'Union par des fournisseurs qui ne sont pas établis dans l'Union et sert à ces derniers de point de contact établi dans l'Union.

(83) Compte tenu de la nature et de la complexité de la chaîne de valeur des systèmes d'IA, et conformément au nouveau cadre législatif, il est essentiel de garantir la sécurité juridique et de faciliter le respect du présent règlement. Par conséquent, il est nécessaire de préciser le rôle et les obligations spécifiques des opérateurs concernés tout au long de ladite chaîne de valeur, tels que les importateurs et les distributeurs qui peuvent contribuer au développement des systèmes d'IA. Dans certaines situations, ces opérateurs pourraient jouer plus d'un rôle en même temps et devraient donc remplir toutes les obligations pertinentes associées à ces rôles. Par exemple, un opérateur pourrait agir à la fois en tant que distributeur et importateur.

(84) Afin de garantir la sécurité juridique, il est nécessaire de préciser que, dans certaines conditions particulières, tout distributeur, importateur, déployeur ou autre tiers devrait être considéré comme un fournisseur d'un système d'IA à haut risque et, par conséquent, assumer toutes les obligations correspondantes. Tel serait le cas si cette

cf. déployeurs

38. Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

partie met son nom ou sa marque sur un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles stipulant que les obligations sont attribuées d'une autre manière. Tel serait aussi le cas si cette partie apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service et de telle sorte qu'il demeure un système d'IA à haut risque conformément au présent règlement, ou si elle modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé comme étant à haut risque et qui a déjà été mis sur le marché ou mis en service, de telle sorte que le système d'IA devient un système d'IA à haut risque conformément au présent règlement. Ces dispositions devraient s'appliquer sans préjudice de dispositions plus spécifiques établies dans certains actes législatifs de l'Union en matière d'harmonisation reposant sur le nouveau cadre législatif avec lesquels le présent règlement devrait s'appliquer. Par exemple, l'article 16, paragraphe 2, du règlement (UE) 2017/745, qui dispose que certaines modifications ne devraient pas être considérées comme des modifications d'un dispositif susceptibles d'influer sur sa conformité avec les exigences applicables, devrait continuer de s'appliquer aux systèmes d'IA à haut risque constituant des dispositifs médicaux au sens dudit règlement.

(85) Les systèmes d'IA à usage général peuvent être utilisés comme des systèmes d'IA à haut risque en tant que tels ou comme des composants d'autres systèmes d'IA à haut risque. Dès lors, en raison de leur nature particulière, et afin de garantir un partage équitable des responsabilités tout au long de la chaîne de valeur de l'IA, les fournisseurs de systèmes d'IA à usage général, indépendamment du fait que ces systèmes puissent être utilisés comme des systèmes d'IA à haut risque en tant que tels par d'autres fournisseurs ou comme des composants de systèmes d'IA à haut risque, et sauf dispositions contraires du présent règlement, devraient coopérer étroitement avec les fournisseurs des systèmes d'IA à haut risque concernés afin de leur permettre de se conformer aux obligations pertinentes prévues par le présent règlement et avec les autorités compétentes établies en vertu du présent règlement.

(86) Lorsque, dans les conditions prévues par le présent règlement, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA ne devrait plus être considéré comme le fournisseur aux fins du présent règlement, et lorsque ce fournisseur n'a pas expressément exclu le changement du système d'IA en un système d'IA à haut risque, ce fournisseur devrait néanmoins coopérer étroitement, mettre à disposition les informations nécessaires et fournir l'accès technique raisonnablement attendu et toute autre assistance qui sont requis pour le respect des obligations énoncées dans le présent règlement, notamment en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque.

(87) En outre, lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit relevant du champ d'application de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit défini par cette législation devrait se conformer aux obligations du fournisseur établies dans le présent règlement et devrait, en particulier, garantir que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement.

(88) Tout au long de la chaîne de valeur de l'IA, plusieurs parties fournissent souvent des systèmes, des outils et des services d'IA, mais aussi des composants ou des processus que le fournisseur intègre dans le système d'IA avec plusieurs objectifs, dont l'entraînement de modèles, le réentraînement de modèles, la mise à l'essai et l'évaluation de modèles, l'intégration dans des logiciels ou d'autres aspects du développement de modèles. Ces parties ont un rôle important à jouer dans la chaîne de valeur vis-à-vis du fournisseur du système d'IA à haut risque dans lequel leurs systèmes, outils, services, composants ou processus d'IA sont intégrés, et devraient fournir à ce fournisseur, en vertu d'un accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaires sur la base de l'état de la technique généralement reconnu, afin de lui permettre de se conformer pleinement aux obligations énoncées dans le présent règlement, sans compromettre leurs propres droits de propriété intellectuelle ou secrets d'affaires.

(89) Les tiers qui rendent accessibles au public des outils, services, processus ou composants d'IA autres que des modèles d'IA à usage général ne devraient pas être tenus de se conformer aux exigences visant les responsabilités tout au long de la chaîne de valeur de l'IA, en particulier à l'égard du fournisseur qui les a utilisés ou intégrés,

lorsque ces outils, services, processus ou composants d'IA sont rendus accessibles sous licence libre et ouverte. Les développeurs d'outils, de services, de processus ou de composants d'IA libres et ouverts autres que les modèles d'IA à usage général devraient être encouragés à mettre en œuvre des pratiques documentaires largement adoptées, telles que les cartes modèles et les fiches de données, afin d'accélérer le partage d'informations tout au long de la chaîne de valeur de l'IA, ce qui permettrait de promouvoir des systèmes d'IA fiables dans l'Union.

(90) La Commission pourrait élaborer et recommander des clauses contractuelles types volontaires à établir entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque, afin de faciliter la coopération tout au long de la chaîne de valeur. Lorsqu'elle élabore des clauses contractuelles types volontaires, la Commission devrait aussi tenir compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques.

(91) Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux potentiellement associés à leur utilisation, notamment en ce qui concerne la nécessité d'assurer un suivi adéquat de la performance d'un système d'IA dans un contexte réel, il convient de définir des responsabilités spécifiques pour les déployeurs. Les déployeurs devraient en particulier prendre des mesures techniques et organisationnelles appropriées pour pouvoir utiliser les systèmes d'IA à haut risque conformément à la notice d'utilisation, et certaines autres obligations devraient être prévues en ce qui concerne la surveillance du fonctionnement des systèmes d'IA et la tenue de registres, selon le cas. En outre, les déployeurs devraient veiller à ce que les personnes chargées de mettre en œuvre la notice d'utilisation et au contrôle humain des systèmes énoncées dans le présent règlement possèdent les compétences nécessaires, en particulier un niveau adéquat de maîtrise, de formation et d'autorité en matière d'IA pour s'acquitter correctement de ces tâches. Ces obligations devraient être sans préjudice des autres obligations des déployeurs en ce qui concerne les systèmes d'IA à haut risque en vertu du droit de l'Union ou du droit national.

cf. déployeurs

(92) Le présent règlement est sans préjudice de l'obligation qu'ont les employeurs d'informer ou d'informer et de consulter les travailleurs ou leurs représentants en vertu du droit et des pratiques nationales ou de l'Union, y compris la directive 2002/14/CE du Parlement européen et du Conseil[39], sur les décisions de mise en service ou d'utilisation de systèmes d'IA. Il reste nécessaire de veiller à ce que les travailleurs et leurs représentants soient informés du déploiement prévu de systèmes d'IA à haut risque sur le lieu de travail lorsque les conditions de cette obligation d'information ou d'information et de consultation figurant dans d'autres instruments juridiques ne sont pas remplies. En outre, ce droit à l'information est accessoire et nécessaire à l'objectif de protection des droits fondamentaux qui sous-tend le présent règlement. Par conséquent, il convient de prévoir une obligation d'information à cet effet dans le présent règlement, sans porter atteinte aux droits existants des travailleurs.

(93) Si des risques liés aux systèmes d'IA peuvent découler de la manière dont ces systèmes sont conçus, ils peuvent également provenir de la manière dont ces systèmes d'IA sont utilisés. Les déployeurs de systèmes d'IA à haut risque jouent donc un rôle essentiel pour ce qui est de garantir la protection des droits fondamentaux, en complétant les obligations du fournisseur lors du développement du système d'IA. Les déployeurs sont les mieux placés pour comprendre comment le système d'IA à haut risque sera utilisé concrètement et peuvent donc identifier les risques importants potentiels qui n'étaient pas prévus au cours de la phase de développement, en raison d'une connaissance plus précise du contexte d'utilisation et des personnes ou groupes de personnes susceptibles d'être concernés, y compris les groupes vulnérables. Les déployeurs de systèmes d'IA à haut risque énumérés dans une annexe du présent règlement contribuent également de façon essentielle à informer les personnes physiques et devraient, lorsqu'ils prennent des décisions ou facilitent la prise de décisions concernant des personnes physiques, selon le cas, informer lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Cette information devrait comprendre la destination du système et le type de décisions prises. Les

cf. déployeurs

39. Directive 2002/14/CE du Parlement européen et du Conseil du 11 mars 2002 établissant un cadre général relatif à l'information et la consultation des travailleurs dans la Communauté européenne (JO L 80 du 23.3.2002, p. 29).

déployeurs devraient aussi informer les personnes physiques de leur droit à une explication prévu par le présent règlement. En ce qui concerne les systèmes d'IA à haut risque utilisés à des fins répressives, cette obligation devrait être mise en œuvre conformément à l'article 13 de la directive (UE) 2016/680.

(94) Tout traitement de données biométriques intervenant dans l'utilisation de systèmes d'IA à des fins d'identification biométrique de nature répressive doit être conforme à l'article 10 de la directive (UE) 2016/680, qui n'autorise un tel traitement que lorsque cela est strictement nécessaire, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre. Une telle utilisation, lorsqu'elle est autorisée, doit également respecter les principes énoncés à l'article 4, paragraphe 1, de la directive (UE) 2016/680, notamment la licéité, la loyauté et la transparence, la limitation des finalités, l'exactitude et la limitation de la conservation.

(95) Sans préjudice du droit de l'Union applicable, en particulier le règlement (UE) 2016/679 et la directive (UE) 2016/680, et compte tenu de la nature intrusive des systèmes d'identification biométrique à distance a posteriori, l'utilisation de systèmes d'identification biométrique à distance a posteriori devrait être soumise à des garanties. Les systèmes d'identification biométrique à distance a posteriori devraient toujours être utilisés d'une manière proportionnée, légitime et strictement nécessaire, et donc ciblée, en ce qui concerne les personnes à identifier, le lieu et la portée temporelle et fondée sur un jeu de données fermé d'images vidéo légalement acquises. En tout état de cause, les systèmes d'identification biométrique à distance a posteriori ne devraient pas être utilisés dans le cadre d'activités répressives pour mener à une surveillance aveugle. Les conditions d'identification biométrique à distance a posteriori ne devraient en aucun cas constituer une base permettant de contourner les conditions applicables en ce qui concerne l'interdiction et les exceptions strictes pour l'identification biométrique à distance en temps réel.

cf. RGPD

(96) Afin de garantir efficacement la protection des droits fondamentaux, les déployeurs de systèmes d'IA à haut risque qui sont des organismes de droit public ou des entités privées fournissant des services publics et des déployeurs de certains systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, tels que des entités bancaires ou d'assurance, devraient procéder à une analyse d'impact de ces systèmes concernant les droits fondamentaux avant de les mettre en service. Les services à caractère public importants pour les personnes peuvent également être fournis par des entités privées. Les entités privées fournissant de tels services publics sont liées à des missions d'intérêt public dans des domaines tels que l'éducation, les soins de santé, les services sociaux, le logement et l'administration de la justice. L'analyse d'impact concernant les droits fondamentaux vise à ce que le déployeur identifie les risques spécifiques pour les droits des personnes ou groupes de personnes susceptibles d'être concernés et à ce qu'il détermine les mesures à prendre en cas de matérialisation de ces risques. L'analyse d'impact devrait être réalisée avant le premier déploiement du système d'IA à haut risque et être mise à jour lorsque le déployeur estime que l'un des facteurs pertinents a changé. L'analyse d'impact devrait identifier les processus pertinents du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination, et devrait indiquer la durée pendant laquelle le système est destiné à être utilisé et selon quelle fréquence ainsi que les catégories spécifiques de personnes physiques et de groupes susceptibles d'être concernés dans le contexte spécifique d'utilisation. L'analyse devrait aussi déterminer les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les droits fondamentaux de ces personnes ou groupes. Afin que cette analyse soit réalisée correctement, le déployeur devrait tenir compte des informations pertinentes, y compris, mais sans s'y limiter, les informations communiquées par le fournisseur du système d'IA à haut risque dans la notice d'utilisation. À la lumière des risques recensés, les déployeurs devraient déterminer les mesures à prendre en cas de matérialisation de ces risques, y compris, par exemple, les dispositions en matière de gouvernance dans ce contexte spécifique d'utilisation, telles que les dispositions pour le contrôle humain conformément à la notice d'utilisation ou les procédures de traitement des plaintes et de recours, en ce qu'elles pourraient contribuer à atténuer les risques pour les droits fondamentaux dans des cas d'utilisation concrets. Après avoir réalisé cette analyse d'impact, le déployeur devrait en informer l'autorité de surveillance du marché concernée. Le cas échéant, pour recueillir les informations pertinentes nécessaires à la réalisation de l'analyse d'impact, les déployeurs de systèmes d'IA à haut risque, en particulier lorsque des systèmes d'IA sont utilisés dans le secteur public, pourraient associer les parties pre-

cf. déployeurs

nantes concernées, y compris les représentants de groupes de personnes susceptibles d'être concernés par le système d'IA, les experts indépendants et les organisations de la société civile, à la réalisation de cette analyse d'impact et à la conception des mesures à prendre en cas de matérialisation des risques. Le Bureau européen de l'intelligence artificielle (ci-après dénommé «Bureau de l'IA») devrait élaborer un modèle de questionnaire afin de faciliter la mise en conformité et de réduire la charge administrative pesant sur les déployeurs.

(97) La notion de modèles d'IA à usage général devrait être clairement définie et distincte de la notion de systèmes d'IA afin de garantir la sécurité juridique. La définition devrait se fonder sur les principales caractéristiques fonctionnelles d'un modèle d'IA à usage général, en particulier la généralité et la capacité d'exécuter de manière compétente un large éventail de tâches distinctes. Ces modèles sont généralement entraînés avec de grandes quantités de données, au moyen de diverses méthodes, telles que l'apprentissage auto-supervisé, non supervisé ou par renforcement. Les modèles d'IA à usage général peuvent être mis sur le marché de différentes manières, notamment au moyen de bibliothèques, d'interfaces de programmation d'applications (API), de téléchargements directs ou de copies physiques. Ces modèles peuvent être modifiés ou affinés et ainsi se transformer en nouveaux modèles. Bien que les modèles d'IA soient des composants essentiels des systèmes d'IA, ils ne constituent pas en soi des systèmes d'IA. Les modèles d'IA nécessitent l'ajout d'autres composants, tels qu'une interface utilisateur, pour devenir des systèmes d'IA. Les modèles d'IA sont généralement intégrés dans les systèmes d'IA et en font partie. Le présent règlement prévoit des règles spécifiques pour les modèles d'IA à usage général et pour les modèles d'IA à usage général qui présentent des risques systémiques, lesquelles devraient également s'appliquer lorsque ces modèles sont intégrés dans un système d'IA ou en font partie. Il convient de considérer que les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer une fois que ces modèles sont mis sur le marché. Lorsque le fournisseur d'un modèle d'IA à usage général intègre un propre modèle dans son propre système d'IA qui est mis à disposition sur le marché ou mis en service, ce modèle devrait être considéré comme étant mis sur le marché et, par conséquent, les obligations prévues par le présent règlement pour les modèles devraient continuer de s'appliquer en plus de celles applicables aux systèmes d'IA. Les obligations prévues pour les modèles ne devraient en aucun cas s'appliquer lorsqu'un propre modèle est utilisé pour des processus purement internes qui ne sont pas essentiels à la fourniture d'un produit ou d'un service à des tiers et que les droits des personnes physiques ne sont pas affectés. Compte tenu de leurs effets potentiellement très négatifs, les modèles d'IA à usage général présentant un risque systémique devraient toujours être soumis aux obligations pertinentes prévues par le présent règlement. La définition ne devrait pas couvrir les modèles d'IA utilisés avant leur mise sur le marché aux seules fins d'activités de recherche, de développement et de prototypage. Cela est sans préjudice de l'obligation de se conformer au présent règlement lorsque, à la suite de telles activités, un modèle est mis sur le marché.

(98) Alors que la généralité d'un modèle pourrait, entre autres, également être déterminée par un nombre de paramètres, les modèles comptant au moins un milliard de paramètres et entraînés à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle devraient être considérés comme présentant une généralité significative et exécutant de manière compétente un large éventail de tâches distinctes.

(99) Les grands modèles d'IA génératifs sont un exemple typique d'un modèle d'IA à usage général, étant donné qu'ils permettent la production flexible de contenus, tels que du texte, de l'audio, des images ou de la vidéo, qui peuvent aisément s'adapter à un large éventail de tâches distinctes.

(100) Lorsqu'un modèle d'IA à usage général est intégré dans un système d'IA ou en fait partie, ce système devrait être considéré comme un système d'IA à usage général lorsque, en raison de cette intégration, ce système a la capacité de répondre à divers usages. Un système d'IA à usage général peut être utilisé directement ou être intégré dans d'autres systèmes d'IA.

(101) Les fournisseurs de modèles d'IA à usage général ont un rôle et une responsabilité particuliers tout au long de la chaîne de valeur de l'IA, étant donné que les modèles qu'ils fournissent peuvent constituer la base d'une série de systèmes en aval, souvent fournis par des fournisseurs en aval, qui nécessitent une bonne compréhension des modèles et de leurs capacités, à la fois pour permettre l'intégration de ces modèles

dans leurs produits et pour remplir les obligations qui leur incombent en vertu du présent règlement ou d'autres règlements. Par conséquent, des mesures de transparence proportionnées devraient être prévues, y compris l'élaboration et la tenue à jour de la documentation, et la fourniture d'informations sur le modèle d'IA à usage général en vue de son utilisation par les fournisseurs en aval. La documentation technique devrait être élaborée et tenue à jour par le fournisseur de modèles d'IA à usage général afin qu'elle puisse être mise, sur demande, à la disposition du Bureau de l'IA et des autorités nationales compétentes. L'ensemble minimal d'éléments à inclure dans cette documentation devrait figurer dans des annexes spécifiques du présent règlement. La Commission devrait être habilitée à modifier ces annexes par voie d'actes délégués à la lumière des évolutions technologiques.

(102)Les logiciels et les données, y compris les modèles, publiés dans le cadre d'une licence libre et ouverte grâce à laquelle ils peuvent être partagés librement et qui permet aux utilisateurs de librement consulter, utiliser, modifier et redistribuer ces logiciels et données ou leurs versions modifiées peuvent contribuer à la recherche et à l'innovation sur le marché et offrir d'importantes possibilités de croissance pour l'économie de l'Union. Les modèles d'IA à usage général publiés sous licence libre et ouverte devraient être considérés comme garantissant des niveaux élevés de transparence et d'ouverture si leurs paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. La licence devrait également être considérée comme libre et ouverte lorsqu'elle permet aux utilisateurs d'exploiter, de copier, de distribuer, d'étudier, de modifier et d'améliorer les logiciels et les données, y compris les modèles, à condition que le fournisseur initial du modèle soit crédité et que les conditions de distribution identiques ou comparables soient respectées.

(103)Les composants d'IA libres et ouverts couvrent les logiciels et les données, y compris les modèles et les modèles à usage général, outils, services ou processus d'un système d'IA. Les composants d'IA libres et ouverts peuvent être fournis par différents canaux, y compris leur développement dans des référentiels ouverts. Aux fins du présent règlement, les composants d'IA qui sont fournis contre paiement ou monétisés, y compris par la fourniture d'un soutien technique ou d'autres services, notamment au moyen d'une plateforme logicielle, liés au composant d'IA, ou l'utilisation de données à caractère personnel pour des raisons autres qu'aux fins exclusives de l'amélioration de la sécurité, de la compatibilité ou de l'interopérabilité des logiciels, à l'exception des transactions entre micro-entreprises, ne devraient pas bénéficier des exceptions prévues pour les composants d'IA libres et ouverts. La mise à disposition de composants d'IA au moyen de référentiels ouverts ne devrait pas, en soi, constituer une monétisation.

(104)Les fournisseurs de modèles d'IA à usage général qui sont publiés sous licence libre et ouverte et dont les paramètres, y compris les poids, les informations sur l'architecture des modèles et les informations sur l'utilisation des modèles, sont rendus publics devraient faire l'objet d'exceptions en ce qui concerne les exigences en matière de transparence imposées pour les modèles d'IA à usage général, à moins que les modèles ne puissent être considérés comme présentant un risque systémique, auquel cas le fait que les modèles soient transparents et accompagnés d'une licence ouverte ne devrait pas être considéré comme une raison suffisante pour exclure le respect des obligations prévues par le présent règlement. En tout état de cause, étant donné que la publication de modèles d'IA à usage général sous licence libre et ouverte ne révèle pas nécessairement des informations importantes sur le jeu de données utilisé pour l'entraînement ou de réglage fin du modèle et sur la manière dont le respect de la législation sur le droit d'auteur a été assuré, l'exception prévue pour les modèles d'IA à usage général en ce qui concerne les exigences en matière de transparence ne devrait pas concerner l'obligation de produire un résumé du contenu utilisé pour l'entraînement des modèles ni l'obligation de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur, en particulier pour identifier et respecter la réservation de droits au titre de l'article 4, paragraphe 3, de la directive (UE) 2019/790 du Parlement européen et du Conseil[40].

40. Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

(105)Les modèles d'IA à usage général, en particulier les grands modèles d'IA génératifs, capables de générer du texte, des images et d'autres contenus, présentent des possibilités d'innovation uniques mais aussi des défis pour les artistes, les auteurs et les autres créateurs, et la manière dont leur contenu créatif est créé, distribué, utilisé et consommé. Le développement et l'entraînement de ces modèles requièrent un accès à de grandes quantités de texte, d'images, de vidéos et d'autres données. Les techniques de fouille de textes et de données peuvent être largement utilisées dans ce contexte pour extraire et analyser ces contenus, qui peuvent être protégés par le droit d'auteur et les droits voisins. Toute utilisation d'un contenu protégé par le droit d'auteur nécessite l'autorisation du titulaire de droits concerné, à moins que des exceptions et limitations pertinentes en matière de droit d'auteur ne s'appliquent. La directive (UE) 2019/790 a introduit des exceptions et des limitations autorisant les reproductions et extractions d'œuvres ou d'autres objets protégés aux fins de la fouille de textes et de données, sous certaines conditions. En vertu de ces règles, les titulaires de droits peuvent choisir de réserver leurs droits sur leurs œuvres ou autres objets protégés afin d'empêcher la fouille de textes et de données, à moins que celle-ci ne soit effectuée à des fins de recherche scientifique. Lorsque les droits d'exclusion ont été expressément réservés de manière appropriée, les fournisseurs de modèles d'IA à usage général doivent obtenir une autorisation des titulaires de droits s'ils souhaitent procéder à une fouille de textes et de données sur ces œuvres.

(106)Les fournisseurs qui mettent des modèles d'IA à usage général sur le marché de l'Union devraient veiller au respect des obligations pertinentes prévues par le présent règlement. À cette fin, les fournisseurs de modèles d'IA à usage général devraient mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et les droits voisins, en particulier pour identifier et respecter la réservation de droits exprimées par les titulaires de droits conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790. Tout fournisseur qui met un modèle d'IA à usage général sur le marché de l'Union devrait se conformer à cette obligation, quelle que soit la juridiction dans laquelle se déroulent les actes pertinents au titre du droit d'auteur qui sous-tendent l'entraînement de ces modèles d'IA à usage général. Cela est nécessaire pour garantir des conditions de concurrence équitables entre les fournisseurs de modèles d'IA à usage général, lorsqu'aucun fournisseur ne devrait pouvoir obtenir un avantage concurrentiel sur le marché de l'Union en appliquant des normes en matière de droit d'auteur moins élevées que celles prévues dans l'Union.

(107)Afin d'accroître la transparence concernant les données utilisées dans le cadre de l'entraînement préalable et de l'entraînement des modèles d'IA à usage général, y compris le texte et les données protégés par la législation sur le droit d'auteur, il convient que les fournisseurs de ces modèles élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner les modèles d'IA à usage général. Tout en tenant dûment compte de la nécessité de protéger les secrets d'affaires et les informations commerciales confidentielles, ce résumé devrait être généralement complet en termes de contenu plutôt que détaillé sur le plan technique afin d'aider les parties ayant des intérêts légitimes, y compris les titulaires de droits d'auteur, à exercer et à faire respecter les droits que leur confère la législation de l'Union, par exemple en énumérant les principaux jeux ou collections de données utilisés pour entraîner le modèle, tels que les archives de données ou bases de données publiques ou privées de grande ampleur, et en fournissant un texte explicatif sur les autres sources de données utilisées. Il convient que le Bureau de l'IA fournisse un modèle de résumé, qui devrait être simple et utile et permettre au fournisseur de fournir le résumé requis sous forme descriptive.

(108)En ce qui concerne l'obligation imposée aux fournisseurs de modèles d'IA à usage général de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et de mettre à la disposition du public un résumé du contenu utilisé pour l'entraînement, le Bureau de l'IA devrait vérifier si le fournisseur a rempli cette obligation sans vérifier ou évaluer œuvre par œuvre les données d'entraînement en ce qui concerne le respect du droit d'auteur. Le présent règlement n'affecte pas l'application des règles en matière de droit d'auteur prévues par la législation de l'Union.

(109)Le respect des obligations applicables aux fournisseurs de modèles d'IA à usage général devrait correspondre et être proportionné au type de fournisseur de modèles, excluant la nécessité de se conformer pour les personnes qui développent ou utilisent des modèles à des fins non professionnelles ou de recherche scientifique, lesquelles

devraient néanmoins être encouragées à se conformer volontairement à ces exigences. Sans préjudice de la législation de l'Union sur le droit d'auteur, le respect de ces obligations devrait tenir dûment compte de la taille du fournisseur et permettre aux PME, y compris aux jeunes pousses, de recourir à des méthodes simplifiées de mise en conformité qui ne devraient pas représenter un coût excessif et décourager l'utilisation de tels modèles. En cas de modification ou de réglage fin d'un modèle, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient se limiter à cette modification ou à ce réglage fin, par exemple en complétant la documentation technique existante avec des informations sur les modifications, y compris les nouvelles sources de données d'entraînement, aux fins de conformité avec les obligations relatives à la chaîne de valeur prévues par le présent règlement.

(110)Les modèles d'IA à usage général pourraient présenter des risques systémiques qui comprennent, sans s'y limiter, tout effet négatif réel ou raisonnablement prévisible en rapport avec des accidents majeurs, des perturbations de secteurs critiques et des conséquences graves pour la santé et la sécurité publiques, tout effet négatif réel ou raisonnablement prévisible sur les processus démocratiques, la sécurité publique et la sécurité économique, et la diffusion de contenus illicites, faux ou discriminatoires. Les risques systémiques devraient être perçus comme augmentant avec les capacités et la portée du modèle, peuvent survenir tout au long du cycle de vie du modèle et sont influencés par les conditions de mauvaise utilisation, la fiabilité du modèle, l'équité et la sécurité du modèle, le niveau d'autonomie du modèle, son accès aux outils, les modalités nouvelles ou combinées, les stratégies de publication et de distribution, le potentiel de suppression des garde-fous et d'autres facteurs. En particulier, les approches internationales ont jusqu'à présent mis en évidence la nécessité de prêter attention aux risques liés à une potentielle mauvaise utilisation intentionnelle ou à des problèmes non intentionnels de contrôle liés à l'alignement sur l'intention humaine, aux risques chimiques, biologiques, radiologiques et nucléaires, tels que les moyens d'abaisser les barrières à l'entrée, y compris pour la mise au point, l'acquisition ou l'utilisation d'armes, aux cybercapacités offensives, tels que les moyens permettant la découverte, l'exploitation ou l'utilisation opérationnelle de vulnérabilités, aux effets de l'interaction et de l'utilisation des outils, y compris, par exemple, la capacité de contrôler les systèmes physiques et d'interférer avec les infrastructures critiques, aux risques liés à la possibilité que les modèles fassent des copies d'eux-mêmes ou «s'auto-reproduisent» ou qu'ils entraînent d'autres modèles, à la manière dont les modèles peuvent donner lieu à des préjugés et des discriminations préjudiciables présentant des risques pour les individus, les communautés ou les sociétés, à la facilitation de la désinformation ou au préjudice porté à la vie privée par des menaces pour les valeurs démocratiques et les droits de l'homme, et au risque qu'un événement particulier entraîne une réaction en chaîne s'accompagnant d'effets négatifs considérables qui pourraient aller jusqu'à affecter toute une ville, tout un secteur d'activité ou toute une communauté.

(111)Il convient d'établir une méthode de classification des modèles d'IA à usage général en tant que modèle d'IA à usage général présentant des risques systémiques. Étant donné que les risques systémiques résultent de capacités particulièrement élevées, un modèle d'IA à usage général devrait être considéré comme présentant des risques systémiques s'il a des capacités à fort impact, évaluées sur la base de méthodologies et d'outils techniques appropriés, ou une incidence significative sur le marché intérieur en raison de sa portée. Les capacités à fort impact des modèles d'IA à usage général sont des capacités égales ou supérieures aux capacités des modèles d'IA à usage général les plus avancés. L'éventail complet des capacités d'un modèle pourrait être mieux compris après sa mise sur le marché ou lorsque les déployeurs interagissent avec le modèle. Selon l'état de la technique au moment de l'entrée en vigueur du présent règlement, la quantité cumulée de calculs utilisée pour l'entraînement du modèle d'IA à usage général mesurée en opérations en virgule flottante est l'une des approximations pertinentes pour les capacités du modèle. La quantité cumulée de calculs utilisée pour l'entraînement inclut les calculs utilisés pour l'ensemble des activités et méthodes destinées à renforcer les capacités du modèle avant le déploiement, telles que l'entraînement préalable, la production de données synthétiques et le réglage fin. Par conséquent, il convient de fixer un seuil initial d'opérations en virgule flottante, qui, s'il est atteint par un modèle d'IA à usage général, conduit à présumer qu'il s'agit d'un modèle d'IA à usage général présentant des risques systémiques. Ce seuil devrait être ajusté au fil du temps pour tenir compte des évolutions technologiques et industrielles, telles que les améliorations algorithmiques ou l'amélioration de l'efficacité des matériels, et être complété par des critères de référence et des indicateurs pour la

cf. déployeurs

capacité du modèle. À cette fin, le Bureau de l'IA devrait coopérer avec la communauté scientifique, l'industrie, la société civile et d'autres experts. Les seuils, ainsi que les outils et les critères de référence pour l'évaluation des capacités à fort impact, devraient être de bons indicateurs de la généralité et des capacités des modèles d'IA à usage général ainsi que du risque systémique qui y est associé, et pourraient tenir compte de la manière dont le modèle sera mis sur le marché ou du nombre d'utilisateurs qu'il pourrait affecter. Afin de compléter ce système, la Commission devrait avoir la possibilité de prendre des décisions individuelles désignant un modèle d'IA à usage général comme modèle d'IA à usage général présentant un risque systémique s'il est constaté que ce modèle a des capacités ou une incidence équivalentes à celles relevant du seuil fixé. Ces décisions devraient être prises sur la base d'une évaluation globale des critères de désignation des modèles d'IA à usage général présentant un risque systémique énoncés dans une annexe du présent règlement, tels que la qualité ou la taille du jeu de données d'entraînement, le nombre d'utilisateurs professionnels et finaux du modèle, ses modalités d'entrée et de sortie, son niveau d'autonomie et d'évolutivité, ou les outils auxquels il a accès. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique, la Commission devrait tenir compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique.

(112)Il convient également d'établir de façon précise une procédure de classification d'un modèle d'IA à usage général présentant un risque systémique. Il convient de présumer qu'un modèle d'IA à usage général qui atteint le seuil applicable pour les capacités à fort impact est un modèle d'IA à usage général présentant un risque systémique. Le fournisseur devrait informer le Bureau de l'IA au plus tard deux semaines après que les exigences ont été remplies ou qu'il a été établi qu'un modèle d'IA à usage général répondra aux exigences qui conduisent à la présomption. Cela est particulièrement important en ce qui concerne le seuil d'opérations en virgule flottante, car l'entraînement des modèles d'IA à usage général nécessite une planification considérable qui inclut l'allocation préalable des ressources de calcul, et, par conséquent, les fournisseurs de modèles d'IA à usage général sont en mesure de savoir si leur modèle atteindra le seuil avant l'achèvement de l'entraînement. Dans le cadre de cette information, le fournisseur devrait pouvoir démontrer que, en raison de ses caractéristiques spécifiques, un modèle d'IA à usage général ne présente pas, exceptionnellement, de risques systémiques et qu'il ne devrait donc pas être classé comme modèle d'IA à usage général présentant des risques systémiques. Ces éléments d'information sont utiles pour le Bureau de l'IA en ce qu'ils lui permettent d'anticiper la mise sur le marché de modèles d'IA à usage général présentant des risques systémiques, et les fournisseurs peuvent ainsi commencer à coopérer avec le Bureau de l'IA à un stade précoce. Ils sont particulièrement importants en ce qui concerne les modèles d'IA à usage général qu'il est prévu de publier en tant que source ouverte, étant donné que, après la publication des modèles de source ouverte, les mesures nécessaires pour garantir le respect des obligations prévues par le présent règlement peuvent être plus difficiles à mettre en œuvre.

(113)Si la Commission prend connaissance du fait qu'un modèle d'IA à usage général satisfait aux exigences de classification en tant que modèle d'IA à usage général présentant un risque systémique, qui n'était pas connu auparavant ou dont le fournisseur concerné n'avait pas informé la Commission, celle-ci devrait être habilitée à désigner ce modèle comme tel. Un système d'alertes qualifiées devrait garantir que le Bureau de l'IA est informé par le panel scientifique des modèles d'IA à usage général qui devraient éventuellement être classés comme modèles d'IA à usage général présentant un risque systémique, en plus des activités de suivi du Bureau de l'IA.

(114)Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient être soumis non seulement aux obligations prévues pour les fournisseurs de modèles d'IA à usage général mais aussi à des obligations visant à identifier et à atténuer ces risques et à garantir un niveau adéquat de protection de la cybersécurité, que les modèles en question soient fournis en tant que modèles autonomes ou qu'ils soient intégrés dans un système ou un produit d'IA. Pour atteindre ces objectifs, le présent règlement devrait exiger des fournisseurs qu'ils effectuent les évaluations nécessaires des modèles, en particulier avant leur première mise sur le marché, y compris la réalisation et la documentation d'essais contradictoires des modèles, ainsi que, le cas échéant, au moyen d'essais internes ou externes indépendants. En outre, les fournisseurs de modèles d'IA à usage général présentant des risques systémiques

devraient évaluer et atténuer en permanence les risques systémiques, y compris, par exemple, en mettant en place des politiques de gestion des risques, telles que des processus de responsabilité et de gouvernance, en mettant en œuvre une surveillance après commercialisation, en prenant des mesures appropriées tout au long du cycle de vie du modèle et en coopérant avec les acteurs pertinents tout au long de la chaîne de valeur de l'IA.

(115)Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient évaluer et atténuer les éventuels risques systémiques. Si, malgré les efforts déployés pour recenser et prévenir les risques liés à un modèle d'IA à usage général susceptible de présenter des risques systémiques, le développement ou l'utilisation du modèle cause un incident grave, le fournisseur de modèle d'IA à usage général devrait, sans retard injustifié, réaliser un suivi de l'incident et communiquer toute information pertinente et toute mesure corrective éventuelle à la Commission et aux autorités nationales compétentes. En outre, les fournisseurs devraient garantir un niveau approprié de protection en matière de cybersécurité en ce qui concerne le modèle et son infrastructure physique, le cas échéant, tout au long du cycle de vie du modèle. La protection en matière de cybersécurité contre les risques systémiques associés à une utilisation malveillante ou à des attaques devrait tenir dûment compte des fuites accidentelles du modèle, des publications non autorisées, du contournement des mesures de sécurité ainsi que de la défense contre les cyberattaques, l'accès non autorisé ou le vol de modèle. Une telle protection pourrait être facilitée par la sécurisation des poids du modèle, des algorithmes, des serveurs et des jeux de données, notamment au moyen de mesures de sécurité opérationnelle relatives à la sécurité de l'information, de politiques spécifiques en matière de cybersécurité, de solutions techniques établies adéquates, et de contrôles de l'accès physique ou informatique, qui soient adaptés aux circonstances particulières et aux risques encourus.

(116)Le Bureau de l'IA devrait encourager et faciliter l'élaboration, le réexamen et l'adaptation des codes de bonne pratique, en tenant compte des approches internationales. Tous les fournisseurs de modèles d'IA à usage général pourraient être invités à participer. Afin de veiller à ce que les codes de bonne pratique correspondent à l'état de la technique et prennent dûment en compte un ensemble divers de perspectives, le Bureau de l'IA devrait collaborer avec les autorités nationales compétentes concernées et pourrait, selon qu'il convient, consulter les organisations de la société civile et d'autres parties prenantes et experts pertinents, notamment le groupe scientifique, pour l'élaboration de ces codes. Les codes de bonne pratique devraient traiter des obligations incombant aux fournisseurs de modèles d'IA à usage général, et de modèles d'IA à usage général présentant des risques systémiques. En outre, en ce qui concerne les risques systémiques, les codes de bonne pratique devraient contribuer à établir une taxinomie des risques reprenant le type et la nature des risques systémiques au niveau de l'Union, ainsi que leur source. Les codes de bonne pratique devraient également mettre l'accent sur une évaluation des risques et des mesures d'atténuation spécifiques.

(117)Les codes de bonne pratique devraient constituer un outil central pour assurer le bon respect des obligations qui incombent aux fournisseurs de modèles d'IA à usage général au titre du présent règlement. Les fournisseurs devraient pouvoir s'appuyer sur des codes de bonne pratique pour démontrer qu'ils respectent leurs obligations. Par voie d'actes d'exécution, la Commission pourrait décider d'approuver un code de bonnes pratiques et de lui conférer une validité générale au sein de l'Union ou, à défaut, de fixer des règles communes pour la mise en œuvre des obligations pertinentes si un code de bonnes pratiques ne peut pas être mis au point avant que le présent règlement ne devienne applicable, ou si un tel code n'est pas considéré comme adéquat par le Bureau de l'IA. Dès lors qu'une norme harmonisée est publiée et jugée appropriée par le Bureau de l'IA au regard des obligations pertinentes, les fournisseurs devraient bénéficier de la présomption de conformité lorsqu'ils respectent une norme européenne harmonisée. En outre, les fournisseurs de modèles d'IA à usage général devraient être en mesure de démontrer la conformité en utilisant d'autres moyens adéquats en l'absence de codes de bonne pratique ou de normes harmonisées ou s'ils choisissent de ne pas s'appuyer sur ceux-ci.

(118)Le présent règlement régit les systèmes et modèles d'IA en instituant certaines exigences et obligations visant les acteurs du marché concernés qui les mettent sur le marché, les mettent en service ou les utilisent dans l'Union, complétant ainsi les obligations incombant aux fournisseurs de services intermédiaires qui intègrent de tels

systèmes ou modèles dans leurs services relevant du règlement (UE) 2022/2065. Dans la mesure où ces systèmes ou modèles sont intégrés dans des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne, ils sont soumis au cadre de gestion des risques établi par le règlement (UE) 2022/2065. Par conséquent, il devrait être présumé que les obligations correspondantes du présent règlement sont remplies, à moins que des risques systémiques importants non couverts par le règlement (UE) 2022/2065 n'apparaissent et ne soient recensés dans de tels modèles. Dans ce contexte, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont tenus d'évaluer les risques systémiques découlant de la conception, du fonctionnement et de l'utilisation de leurs services, y compris la manière dont la conception des systèmes algorithmiques utilisés dans un service pourrait contribuer à ces risques, ainsi que les risques systémiques découlant de mauvaises utilisations éventuelles. Ces fournisseurs sont également tenus de prendre les mesures d'atténuation appropriées pour assurer le respect des droits fondamentaux.

(119)Compte tenu du rythme rapide de l'innovation et de l'évolution technologique des services numériques relevant du champ d'application de différents instruments du droit de l'Union, en particulier à la lumière de l'utilisation et de la perception de leurs destinataires, les systèmes d'IA régis par le présent règlement pourraient être fournis en tant que services intermédiaires ou parties de ceux-ci au sens du règlement (UE) 2022/2065, qui devrait être interprété de manière neutre sur le plan technologique. Par exemple, les systèmes d'IA pourraient être utilisés pour fournir des moteurs de recherche en ligne, en particulier, dans la mesure où un système d'IA tel qu'un dialogueur réalise des recherches sur, en principe, tous les sites web, puis en intègre les résultats dans ses connaissances existantes et utilise les connaissances mises à jour pour générer une sortie unique qui combine différentes sources d'information.

(120)En outre, les obligations imposées aux fournisseurs et aux déployeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties produites par ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation.

cf. déployeurs

(121)La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec le présent règlement, suivant les technologies les plus récentes, et de promouvoir l'innovation ainsi que la compétitivité et la croissance dans le marché unique. Le respect des normes harmonisées telles que définies à l'article 2, point 1) c), du règlement (UE) no 1025/2012 du Parlement européen et du Conseil[41], qui doivent normalement tenir compte des évolutions technologiques les plus récentes, devrait être un moyen pour les fournisseurs de démontrer la conformité avec les exigences du présent règlement. Il convient donc d'encourager une représentation équilibrée des intérêts en associant toutes les parties prenantes concernées à l'élaboration des normes, en particulier les PME, les organisations de consommateurs et les acteurs environnementaux et sociaux, conformément aux articles 5 et 6 du règlement (UE) no 1025/2012. Afin de faciliter le respect de la législation, les demandes de normalisation devraient être formulées par la Commission sans retard injustifié. Lorsqu'elle élabore les demandes de normalisation, la Commission devrait consulter le forum consultatif et le Comité IA afin de recueillir l'expertise pertinente. Toutefois, en l'absence de références pertinentes à des normes harmonisées, la Commission devrait être en mesure d'établir, au moyen d'actes d'exécution, et après consultation du forum consultatif, des spécifications communes pour certaines exigences au titre du présent règlement. Les spécifications communes devraient être une solution de repli exceptionnelle pour faciliter l'obligation du four-

41. Règlement (UE) no 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision no 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

nisseur de se conformer aux exigences du présent règlement, lorsque la demande de normalisation n'a été acceptée par aucune des organisations européennes de normalisation, ou lorsque les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux, ou lorsque les normes harmonisées ne sont pas conformes à la demande, ou lorsque l'adoption d'une norme harmonisée appropriée accuse des retards. Lorsqu'un tel retard dans l'adoption d'une norme harmonisée est dû à la complexité technique de ladite norme, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Lorsqu'elle élabore des spécifications communes, la Commission est encouragée à coopérer avec des partenaires internationaux et des organismes internationaux de normalisation.

(122)Il convient que, sans préjudice de l'utilisation de normes harmonisées et de spécifications communes, les fournisseurs d'un système d'IA à haut risque qui a été entraîné et testé avec des données reflétant le cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel il est destiné à être utilisé soient présumés comme se conformant à la mesure pertinente prévue au titre de l'exigence en matière de gouvernance des données énoncée dans le présent règlement. Sans préjudice des exigences liées à la robustesse et à l'exactitude énoncées dans le présent règlement, conformément à l'article 54, paragraphe 3, du règlement (UE) 2019/881, les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité en vertu dudit règlement et dont les références ont été publiées au Journal officiel de l'Union européenne devraient être présumés conformes aux exigences de cybersécurité du présent règlement dans la mesure où le certificat de cybersécurité ou la déclaration de conformité, ou des parties de ceux-ci, couvrent l'exigence de cybersécurité du présent règlement. Cet aspect demeure sans préjudice du caractère volontaire dudit schéma de cybersécurité.

(123)Afin de garantir un niveau élevé de fiabilité des systèmes d'IA à haut risque, ces systèmes devraient être soumis à une évaluation de la conformité avant leur mise sur le marché ou leur mise en service.

(124)Afin de réduire au minimum la charge pesant sur les opérateurs et d'éviter les éventuels doubles emplois, la conformité avec les exigences du présent règlement des systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation existante de l'Union fondée sur le nouveau cadre législatif devrait être évaluée dans le cadre de l'évaluation de la conformité déjà prévue en vertu de cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas avoir d'incidence sur la logique, la méthode ou la structure générale propres à l'évaluation de la conformité au titre de la législation d'harmonisation de l'Union pertinente.

(125)Compte tenu de la complexité des systèmes d'IA à haut risque et des risques qui y sont associés, il importe d'élaborer une procédure d'évaluation de la conformité adéquat faisant intervenir les organismes notifiés pour ces systèmes, dite «évaluation de conformité par un tiers». Toutefois, étant donné l'expérience actuelle des organismes professionnels de certification avant mise sur le marché dans le domaine de la sécurité des produits et de la nature différente des risques encourus, il convient de limiter, au moins dans une phase initiale d'application du présent règlement, le champ d'application des évaluations de la conformité réalisées par un tiers aux systèmes d'IA à haut risque autres que ceux liés à des produits. Par conséquent, l'évaluation de la conformité de ces systèmes devrait en règle générale être réalisée par le fournisseur sous sa propre responsabilité, à la seule exception des systèmes d'IA destinés à être utilisés à des fins de biométrie.

(126)Afin de procéder à des évaluations de la conformité par un tiers lorsque cela est nécessaire, les organismes notifiés devraient être notifiés en vertu du présent règlement par les autorités nationales compétentes, sous réserve qu'ils satisfassent à un ensemble d'exigences portant en particulier sur leur indépendance, leur compétence, l'absence de conflits d'intérêts et les exigences appropriées en matière de cybersécurité. La notification de ces organismes devrait être envoyée par les autorités nationales compétentes à la Commission et aux autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission, conformément à l'annexe I, article R23, de la décision no 768/2008/CE.

(127)Conformément aux engagements pris par l'Union au titre de l'accord de l'Organisation mondiale du commerce sur les obstacles techniques au commerce, il convient de faciliter la reconnaissance mutuelle des résultats des évaluations de la conformité produits par les organismes d'évaluation de la conformité compétents, indépendamment du territoire sur lequel ils sont établis, à condition que ces organismes d'évaluation de la conformité établis en vertu du droit d'un pays tiers satisfassent aux exigences applicables en vertu du présent règlement et que l'Union ait conclu un accord en ce sens. Dans ce contexte, la Commission devrait étudier activement d'éventuels instruments internationaux à cette fin et, en particulier, œuvrer à la conclusion d'accords de reconnaissance mutuelle avec des pays tiers.

(128)Conformément à la notion communément établie de modification substantielle pour les produits réglementés par la législation d'harmonisation de l'Union, chaque fois que survient une modification susceptible d'avoir une incidence sur la conformité d'un système d'IA à haut risque avec le présent règlement (par exemple, un changement de système d'exploitation ou d'architecture logicielle) ou que la destination du système change, il convient de considérer ledit système d'IA comme un nouveau système d'IA devant être soumis à nouvelle procédure d'évaluation de la conformité. Cependant, les changements intervenant sur l'algorithme et la performance de systèmes d'IA qui continuent à «apprendre» après avoir été mis sur le marché ou mis en service, à savoir l'adaptation automatique de la façon dont les fonctions sont exécutées, ne devraient pas constituer une modification substantielle, à condition que ces changements aient été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité.

(129)Le marquage «CE» devrait être apposé sur les systèmes d'IA à haut risque pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans le marché intérieur. Pour les systèmes d'IA à haut risque intégrés à un produit, un marquage «CE» physique devrait être apposé, éventuellement complété par un marquage «CE» numérique. Pour les systèmes d'IA à haut risque fournis uniquement sous forme numérique, il convient d'utiliser un marquage «CE» numérique. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque qui satisfont aux exigences fixées dans le présent règlement et portent le marquage «CE».

(130)Dans certaines conditions, la disponibilité rapide de technologies innovantes peut être cruciale pour la santé et la sécurité des personnes, pour la protection de l'environnement et la lutte contre le changement climatique et pour la société dans son ensemble. Il convient donc que, pour des motifs exceptionnels liés à la sécurité publique ou à la protection de la vie et de la santé des personnes physiques, à la protection de l'environnement et à la protection d'actifs industriels et d'infrastructures d'importance majeure, les autorités de surveillance du marché puissent autoriser la mise sur le marché ou la mise en service de systèmes d'IA qui n'ont pas fait l'objet d'une évaluation de la conformité. Dans des situations dûment justifiées, prévues dans le présent règlement, les autorités répressives ou les autorités de protection civile peuvent mettre en service un système d'IA à haut risque spécifique sans avoir obtenu l'autorisation de l'autorité de surveillance du marché, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation.

(131)Afin de faciliter les travaux de la Commission et des États membres dans le domaine de l'IA et d'accroître la transparence à l'égard du public, les fournisseurs de systèmes d'IA à haut risque autres que ceux liés à des produits relevant du champ d'application de la législation d'harmonisation existante de l'Union en la matière, ainsi que les fournisseurs qui considèrent qu'un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement n'est pas à haut risque sur la base d'une dérogation, devraient être tenus de s'enregistrer eux-mêmes et d'enregistrer les informations relatives à leur système d'IA dans une base de données de l'UE, qui sera établie et gérée par la Commission. Avant d'utiliser un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement, les déployeurs de systèmes d'IA à haut risque qui sont des autorités, des agences ou des organismes publics devraient s'enregistrer dans une telle base de données et sélectionner le système qu'ils envisagent d'utiliser. Les autres déployeurs devraient être autorisés à le faire volontairement. Cette section de la base de données de l'UE devrait être accessible au public sans frais, et les informations qu'elle contient devraient être consultables grâce à une navigation aisée et être facilement compréhensibles et lisibles par machine. La base de données de l'UE devrait également être

cf. déployeurs

conviviale, par exemple en offrant des fonctionnalités de recherche, y compris par mots-clés, afin de permettre au grand public de trouver les informations pertinentes devant être transmises au moment de l'enregistrement des systèmes d'IA à haut risque et les informations sur le cas d'utilisation de systèmes d'IA à haut risque, énoncés dans une annexe du présent règlement, auquel les systèmes d'IA à haut risque correspondent. Toute modification substantielle de systèmes d'IA à haut risque devrait également être enregistrée dans la base de données de l'UE. En ce qui concerne les systèmes d'IA à haut risque dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, les obligations en matière d'enregistrement devraient être remplies dans une section non publique sécurisée de la base de données de l'UE. L'accès à la section non publique sécurisée devrait être strictement réservé à la Commission, ainsi qu'aux autorités de surveillance du marché pour ce qui est de la section nationale de cette base de données les concernant. Les systèmes d'IA à haut risque dans le domaine des infrastructures critiques ne devraient être enregistrés qu'au niveau national. La Commission devrait faire fonction de responsable du traitement pour la base de données de l'UE, conformément au règlement (UE) 2018/1725. Afin de garantir que la base de données de l'UE soit pleinement opérationnelle une fois déployée, la procédure de création de la base de données devrait prévoir le développement de spécifications fonctionnelles par la Commission et un rapport d'audit indépendant. La Commission devrait tenir compte des risques liés à la cybersécurité dans l'accomplissement de ses missions en tant que responsable du traitement des données dans la base de données de l'UE. Afin de maximiser la disponibilité et l'utilisation de la base de données de l'UE, y compris les informations mises à disposition par son intermédiaire, la base de données de l'UE devrait être conforme aux exigences prévues par la directive (UE) 2019/882.

(132)Certains systèmes d'IA destinés à interagir avec des personnes physiques ou à générer du contenu peuvent présenter des risques spécifiques d'usurpation d'identité ou de tromperie, qu'ils soient ou non considérés comme étant à haut risque. Dans certaines circonstances, l'utilisation de ces systèmes devrait donc être soumise à des obligations de transparence spécifiques sans préjudice des exigences et obligations relatives aux systèmes d'IA à haut risque et sous réserve d'exemptions ciblées destinées à tenir compte des besoins spécifiques des activités répressives. En particulier, les personnes physiques devraient être avisées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Lors de la mise en œuvre de cette obligation, les caractéristiques des personnes physiques appartenant à des groupes vulnérables en raison de leur âge ou d'un handicap devraient être prises en compte dans la mesure où le système d'IA est destiné à interagir également avec ces groupes. En outre, les personnes physiques devraient être mises au courant lorsqu'elles sont exposées à des systèmes d'IA qui, en traitant leurs données biométriques, peuvent identifier ou déduire les émotions ou intentions de ces personnes ou les affecter à des catégories spécifiques. Ces catégories spécifiques peuvent avoir trait à des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits personnels, l'origine ethnique, les préférences et les intérêts personnels. Ces informations et notifications devraient être fournies dans des formats accessibles aux personnes handicapées.

(133)Divers systèmes d'IA peuvent générer de grandes quantités de contenu de synthèse qu'il devient de plus en plus difficile pour les êtres humains de distinguer du contenu authentique généré par des humains. La large disponibilité et les capacités croissantes de ces systèmes ont des conséquences importantes sur l'intégrité de l'écosystème informationnel et la confiance en celui-ci, ce qui pose de nouveaux risques de désinformation et de manipulation à grande échelle, de fraude, d'usurpation d'identité et de tromperie des consommateurs. Compte tenu de ces effets, du rythme rapide de l'évolution technologique et de la nécessité de nouvelles méthodes et techniques pour déterminer l'origine des informations, il convient d'exiger que les fournisseurs de ces systèmes intègrent des solutions techniques permettant le marquage dans un format lisible par machine et la détection du fait que les sorties ont été générées ou manipulées par un système d'IA, et non par un être humain. De telles techniques et méthodes devraient être aussi fiables, interopérables, efficaces et solides que la technologie le permet, et tenir compte des techniques disponibles ou d'une combinaison de ces techniques, telles que les filigranes, les identifications de métadonnées, les méthodes cryptographiques permettant de prouver la provenance et l'authenticité du contenu, les méthodes d'enregistrement, les empreintes digitales ou d'autres techniques, selon qu'il convient. Lorsqu'ils mettent en œuvre cette obligation, les fournisseurs devraient

également tenir compte des spécificités et des limites des différents types de contenu, ainsi que des évolutions technologiques et du marché pertinentes dans le domaine, tels qu'elles ressortent de l'état de la technique généralement reconnu. Ces techniques et méthodes peuvent être mises en œuvre au niveau du système d'IA ou au niveau du modèle d'IA, y compris pour les modèles d'IA à usage général qui génèrent du contenu, ce qui facilitera l'accomplissement de cette obligation par le fournisseur en aval du système d'IA. Dans un souci de proportionnalité, il convient d'envisager que cette obligation de marquage ne s'applique pas aux systèmes d'IA qui remplissent une fonction d'assistance pour la mise en forme standard ou les systèmes d'IA qui ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique.

cf. déployeurs

(134)Outre les solutions techniques utilisées par les fournisseurs du système, les déployeurs qui se servent d'un système d'IA pour générer ou manipuler des images ou des contenus audio ou vidéo présentant une ressemblance sensible avec des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques (hypertrucages), devraient aussi déclarer de manière claire et reconnaissable que le contenu a été créé ou manipulé par une IA en étiquetant les sorties d'IA en conséquence et en mentionnant son origine artificielle. Le respect de cette obligation de transparence ne devrait pas être interprété comme indiquant que l'utilisation du système d'IA ou des sorties qu'il génère entrave le droit à la liberté d'expression et le droit à la liberté des arts et des sciences garantis par la Charte, en particulier lorsque le contenu fait partie d'un travail ou d'un programme manifestement créatif, satirique, artistique; de fiction ou analogue, sous réserve de garanties appropriées pour les droits et libertés de tiers. Dans ces cas, l'obligation de transparence s'appliquant aux hypertrucages au titre du présent règlement se limite à la divulgation de l'existence de tels contenus générés ou manipulés, d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre, y compris son exploitation et son utilisation normales, tout en préservant l'utilité et la qualité de l'œuvre. En outre, il convient d'envisager une obligation d'information similaire en ce qui concerne le texte généré ou manipulé par l'IA dans la mesure où celui-ci est publié dans le but d'informer le public sur des questions d'intérêt public, à moins que le contenu généré par l'IA n'ait fait l'objet d'un processus d'examen humain ou de contrôle éditorial et qu'une personne physique ou morale assume la responsabilité éditoriale pour la publication du contenu.

(135)Sans préjudice de la nature obligatoire et de la pleine applicabilité des obligations de transparence, la Commission peut également encourager et faciliter l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA, y compris pour favoriser des modalités pratiques visant, selon qu'il convient, à rendre les mécanismes de détection accessibles et à faciliter la coopération avec d'autres acteurs tout au long de la chaîne de valeur, à diffuser les contenus ou à vérifier leur authenticité et leur provenance pour permettre au public de reconnaître efficacement les contenus générés par l'IA.

(136)Les obligations incombant aux fournisseurs et aux déployeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties de ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation. L'exigence relative à l'étiquetage des contenus générés par des systèmes d'IA au titre du présent règlement est sans préjudice de l'obligation prévue à l'article 16, paragraphe 6, du règlement (UE) 2022/2065 imposant aux fournisseurs de services d'hébergement de traiter les signalements de contenus illégaux qu'ils reçoivent au titre de l'article 16, paragraphe 1, dudit règlement, et elle ne devrait pas influencer l'évaluation et la décision quant à l'illégalité du contenu en question. Cette évaluation ne devrait être effectuée qu'au regard des règles régissant la légalité du contenu.

cf. déployeurs

(137)Le respect des obligations de transparence applicables aux systèmes d'IA relevant du présent règlement ne devrait pas être interprété comme indiquant que l'utilisa-

tion du système d'IA ou de ses sorties est licite en vertu du présent règlement ou d'autres actes législatifs de l'Union et des États membres et devrait être sans préjudice d'autres obligations de transparence pour les déployeurs de systèmes d'IA prévues par le droit de l'Union ou le droit national.

(138)L'IA est une famille de technologies en évolution rapide qui nécessite la mise en place d'un contrôle réglementaire et d'un espace sûr et contrôlé pour l'expérimentation, garantissant également une innovation responsable et l'intégration de garanties et de mesures d'atténuation des risques appropriées. Pour garantir un cadre juridique favorable à l'innovation, à l'épreuve du temps et résilient face aux perturbations, les États membres devraient veiller à ce que leurs autorités nationales compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national pour faciliter le développement et la mise à l'essai de systèmes d'IA innovants sous un contrôle réglementaire strict avant que ces systèmes ne soient mis sur le marché ou mis en service d'une autre manière. Les États membres pourraient également satisfaire à cette obligation en participant à des bacs à sable réglementaires déjà existants ou en établissant conjointement un bac à sable avec les autorités compétentes d'un ou de plusieurs États membres, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants. Les bacs à sable réglementaires de l'IA pourraient être mis en place sous forme physique, numérique ou hybride et admettre des produits tant physiques que numériques. Les autorités chargées de les mettre en place devraient également veiller à ce que les bacs à sable réglementaires de l'IA disposent des ressources appropriées pour assurer leur fonctionnement, y compris les ressources financières et humaines.

(139)Les bacs à sable réglementaires de l'IA devraient avoir pour objectif de favoriser l'innovation dans le domaine de l'IA en créant un environnement contrôlé d'expérimentation et d'essai au stade du développement et de la précommercialisation afin de garantir la conformité des systèmes d'IA innovants avec le présent règlement et d'autres dispositions pertinentes du droit de l'Union et du droit national. De plus, les bacs à sable réglementaires de l'IA devraient viser à renforcer la sécurité juridique pour les innovateurs ainsi que le contrôle et la compréhension, par les autorités compétentes, des possibilités, des risques émergents et des conséquences de l'utilisation de l'IA, de faciliter l'apprentissage réglementaire pour les autorités et les entreprises, y compris en vue d'ajustements futurs du cadre juridique, de soutenir la coopération et l'échange de bonnes pratiques avec les autorités participant au bac à sable réglementaire de l'IA, et d'accélérer l'accès aux marchés, notamment en supprimant les obstacles pour les PME, y compris les jeunes pousses. Les bacs à sable réglementaires de l'IA devraient être largement disponibles dans toute l'Union, et il convient de prêter une attention particulière à leur accessibilité pour les PME, y compris les jeunes pousses. La participation au bac à sable réglementaire de l'IA devrait se concentrer sur les questions qui créent une insécurité juridique pour les fournisseurs et les fournisseurs potentiels avant d'innover, d'expérimenter l'IA dans l'Union et de contribuer à un apprentissage réglementaire fondé sur des données probantes. La surveillance des systèmes d'IA dans le bac à sable réglementaire de l'IA devrait donc porter sur leur développement, leur entraînement, leur mise à l'essai et leur validation avant que les systèmes ne soient mis sur le marché ou mis en service, ainsi que sur la notion et la survenance de modifications substantielles susceptibles de nécessiter une nouvelle procédure d'évaluation de la conformité. Tout risque important recensé lors du développement et de la mise à l'essai de ces systèmes d'IA devrait donner lieu à des mesures d'atténuation adéquates et, à défaut, à la suspension du processus de développement et d'essai. Au besoin, les autorités nationales compétentes mettant en place des bacs à sable réglementaires de l'IA devraient coopérer avec d'autres autorités concernées, y compris celles qui supervisent la protection des droits fondamentaux, et pourraient permettre la participation d'autres acteurs de l'écosystème de l'IA, tels que les organisations nationales ou européennes de normalisation, les organismes notifiés, les installations d'essai et d'expérimentation, les laboratoires de recherche et d'expérimentation, les pôles européens d'innovation numérique, ainsi que les parties prenantes et les organisations de la société civile concernées. Pour assurer une mise en œuvre uniforme dans toute l'Union et des économies d'échelle, il convient d'établir des règles communes pour la mise en place des bacs à sable réglementaires de l'IA ainsi qu'un cadre de coopération entre les autorités compétentes intervenant dans la surveillance des bacs à sable. Les bacs à sable réglementaires de l'IA établis en vertu du présent règlement devraient être sans préjudice d'autres actes législatifs autorisant la création d'autres bacs à sable en vue de garantir le respect de dispositions de droit autres que le présent règlement. Le cas échéant, les autorités compétentes concernées

chargées de ces autres bacs à sable réglementaires devraient prendre en considération les avantages de l'utilisation de ces bacs à sable également aux fins d'assurer la conformité des systèmes d'IA avec le présent règlement. Sous réserve d'un accord entre les autorités nationales compétentes et les participants au bac à sable réglementaire de l'IA, il peut également être procédé à des essais en conditions réelles supervisés dans le cadre du bac à sable réglementaire de l'IA.

(140)Le présent règlement devrait constituer la base juridique pour l'utilisation, par les fournisseurs et fournisseurs potentiels du bac à sable réglementaire de l'IA, des données à caractère personnel collectées à d'autres fins pour le développement de certains systèmes d'IA d'intérêt public dans le cadre du bac à sable réglementaire de l'IA, uniquement dans des conditions déterminées, conformément à l'article 6, paragraphe 4, et à l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et aux articles 5, 6 et 10 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, et de l'article 10 de la directive (UE) 2016/680. Toutes les autres obligations des responsables du traitement et tous les autres droits des personnes concernées en vertu des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680 restent applicables. En particulier, le présent règlement ne devrait pas constituer une base juridique au sens de l'article 22, paragraphe 2, point b), du règlement (UE) 2016/679 et de l'article 24, paragraphe 2, point b), du règlement (UE) 2018/1725. Les fournisseurs et fournisseurs potentiels participant au bac à sable réglementaire de l'IA devraient prévoir des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs orientations et en agissant rapidement et de bonne foi pour atténuer adéquatement tout risque important recensé pour la sécurité, la santé et les droits fondamentaux susceptible de survenir au cours du développement, de la mise à l'essai et de l'expérimentation dans ledit bac à sable.

cf. **RGPD** art. 6.4, art. 9.2.g

cf. RGPD

cf. RGPD art. 22.2.b

(141)Afin d'accélérer le processus de développement et la mise sur le marché des systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, il importe que les fournisseurs ou fournisseurs potentiels de ces systèmes puissent également bénéficier d'un régime particulier pour soumettre ces systèmes à des essais en conditions réelles sans participer à un bac à sable réglementaire de l'IA. Toutefois, dans de tels cas, compte tenu des conséquences possibles de ces essais sur des personnes physiques, il convient de veiller à ce que le présent règlement introduise des garanties et des conditions appropriées et suffisantes pour les fournisseurs ou fournisseurs potentiels. Ces garanties devraient comprendre, entre autres, une demande de consentement éclairé de la part des personnes physiques pour participer à des essais en conditions réelles, sauf en ce qui concerne les services répressifs lorsque la recherche d'un consentement éclairé empêcherait que le système d'IA ne soit mis à l'essai. Le consentement des participants à la participation à ces essais au titre du présent règlement est distinct et sans préjudice du consentement des personnes concernées au traitement de leurs données à caractère personnel en vertu de la législation applicable en matière de protection des données. Il importe également important de réduire les risques au minimum et de permettre aux autorités compétentes d'exercer un contrôle et, par conséquent, d'exiger des fournisseurs potentiels qu'ils disposent d'un plan d'essais en conditions réelles présenté à l'autorité de surveillance du marché compétente, d'enregistrer les essais dans des sections spécifiques de la base de données de l'UE, sous réserve de quelques exceptions limitées, de fixer des limitations de la période pendant laquelle les essais peuvent être menés et d'exiger des garanties supplémentaires pour les personnes appartenant à certains groupes vulnérables, ainsi qu'un accord écrit définissant les rôles et les responsabilités des fournisseurs potentiels et des déployeurs et établissant un contrôle effectif par le personnel compétent participant aux essais en conditions réelles. En outre, il convient d'envisager des garanties supplémentaires pour veiller à ce que les prédictions, recommandations ou décisions d'un système d'IA puissent être infirmées et ignorées de manière effective et à ce que les données à caractère personnel soient protégées et supprimées lorsque les personnes concernées ont retiré leur consentement à participer aux essais, sans qu'il soit porté atteinte aux droits dont elles disposent en tant que personnes concernées en vertu du droit de l'Union en matière de protection des données. En ce qui concerne le transfert de données, il convient en outre d'envisager que les données collectées et traitées aux fins des essais en conditions réelles ne soient transférées vers des pays tiers que lorsque des garanties appropriées et applicables en vertu du droit de l'Union sont en place, en particulier conformément aux bases pour le transfert de données à caractère personnel prévues par le droit de l'Union en matière de protection des données, et que des garanties appropriées soient mises en place pour les données à carac-

cf. déployeurs

tère non personnel conformément au droit de l'Union, notamment les règlements (UE) 2022/868[42] et (UE) 2023/2854[43] du Parlement européen et du Conseil.

(142)Afin de veiller à ce que l'IA engendre des résultats bénéfiques sur le plan social et environnemental, les États membres sont encouragés à soutenir et à promouvoir la recherche et le développement de solutions d'IA propices à tels résultats, telles que des solutions fondées sur l'IA destinées à renforcer l'accessibilité pour les personnes handicapées, à réduire les inégalités socio-économiques ou à atteindre les objectifs environnementaux, en y affectant des ressources suffisantes, y compris des financements publics et de l'Union, et, lorsqu'il convient et pour autant que les critères d'éligibilité et de sélection soient remplis, en envisageant des projets spécifiques qui poursuivent ces objectifs. Ces projets devraient être fondés sur le principe d'une coopération interdisciplinaire entre les développeurs d'IA, les experts en matière d'inégalité et de non-discrimination, d'accessibilité, de droits des consommateurs, de droits environnementaux et numériques, ainsi que les universitaires.

(143)Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des PME, y compris les jeunes pousses, qui sont des fournisseurs ou des déployeurs de systèmes d'IA bénéficient d'une attention particulière. À cette fin, les États membres devraient prendre des initiatives à l'intention de ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. Les États membres devraient fournir aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union un accès prioritaire aux bacs à sable réglementaires de l'IA, à condition qu'elles remplissent les conditions d'éligibilité et les critères de sélection et sans exclure que d'autres fournisseurs et fournisseurs potentiels accèdent aux bacs à sable pour autant que les mêmes conditions et critères soient remplis. Les États membres devraient utiliser les canaux de communication existants, et en établissent de nouveaux s'il y a lieu, avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, le cas échéant, les autorités publiques locales afin de soutenir les PME tout au long de leur trajectoire de développement en leur fournissant des orientations et en répondant à leurs questions concernant la mise en œuvre du présent règlement. Le cas échéant, ces canaux devraient collaborer pour créer des synergies et assurer la cohérence des orientations fournies aux PME, y compris les jeunes pousses, et aux déployeurs. En outre, les États membres devraient faciliter la participation des PME et d'autres parties concernées aux processus d'élaboration de la normalisation. Par ailleurs, les intérêts et les besoins spécifiques des fournisseurs qui sont des PME, y compris des jeunes pousses, devraient être pris en considération lorsque les organismes notifiés fixent les redevances d'évaluation de la conformité. La Commission devrait évaluer régulièrement les coûts de certification et de mise en conformité pour les PME, y compris les jeunes pousses, en menant des consultations transparentes, et devrait collaborer avec les États membres pour réduire ces coûts. Par exemple, les frais de traduction liés à la documentation obligatoire et à la communication avec les autorités peuvent représenter un coût important pour les fournisseurs et d'autres opérateurs, en particulier pour ceux de plus petite envergure. Les États membres devraient éventuellement veiller à ce qu'une des langues qu'ils choisissent et acceptent pour la documentation pertinente des fournisseurs et pour la communication avec les opérateurs soit une langue comprise par le plus grand nombre possible de déployeurs transfrontières. Afin de répondre aux besoins spécifiques des PME, y compris les jeunes pousses, la Commission devrait fournir des modèles normalisés pour les domaines qui relèvent du présent règlement, sur demande du Comité IA. En outre, la Commission devrait compléter les efforts déployés par les États membres en mettant en place une plateforme d'information unique présentant des informations facilement exploitables concernant le présent règlement à l'intention de tous les fournisseurs et déployeurs, en organisant des campagnes de communication appropriées pour faire connaître les obligations découlant du présent règlement, et en évaluant et en promouvant la convergence des bonnes pratiques dans les procédures de passation de marchés publics relatifs aux systèmes d'IA. Les entreprises qui jusqu'à récemment relevaient des

cf. déployeurs

42. Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

43. Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

«petites entreprises» au sens de l'annexe à la recommandation 2003/361/CE de la Commission[44] devraient avoir accès à ces mesures de soutien, étant donné que ces nouvelles moyennes entreprises peuvent parfois manquer des ressources juridiques et de la formation nécessaires pour avoir une bonne compréhension du présent règlement et en respecter les dispositions.

(144)Afin de promouvoir et de protéger l'innovation, la plateforme d'IA à la demande, ainsi que l'ensemble des programmes et projets de financement pertinents de l'Union, tels que le programme pour une Europe numérique et Horizon Europe, mis en œuvre par la Commission et les États membres au niveau national ou de l'Union, selon qu'il convient, devraient contribuer à la réalisation des objectifs du présent règlement.

(145)Afin de réduire au minimum les risques pour la mise en œuvre résultant du manque de connaissances et d'expertise sur le marché, ainsi que de faciliter la mise en conformité des fournisseurs, en particulier des PME, y compris les jeunes pousses, et des organismes notifiés avec les obligations qui leur incombent au titre du présent règlement, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'expérimentation et d'essai mis en place par la Commission et les États membres au niveau de l'Union ou au niveau national devraient contribuer à la mise en œuvre du présent règlement. Dans le cadre de leurs missions et domaines de compétence respectifs, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'expérimentation et d'essai sont notamment en mesure d'apporter un soutien technique et scientifique aux fournisseurs et aux organismes notifiés.

(146)En outre, au vu de la très petite taille de certains opérateurs et afin d'assurer la proportionnalité en ce qui concerne les coûts de l'innovation, il convient de permettre aux microentreprises de satisfaire à l'une des obligations les plus coûteuses, à savoir celle de mettre en place un système de gestion de la qualité, d'une manière simplifiée qui réduirait la charge administrative et les coûts pour ces entreprises sans affecter le niveau de protection et la nécessité de se conformer aux exigences applicables aux systèmes d'IA à haut risque. La Commission devrait élaborer des lignes directrices pour préciser quels éléments du système de gestion de la qualité les microentreprises doivent respecter dans le système simplifié.

(147)Il convient que la Commission facilite, dans la mesure du possible, l'accès aux installations d'expérimentation et d'essai pour les organismes, groupes ou laboratoires qui ont été créés ou accrédités en vertu d'une législation d'harmonisation de l'Union pertinente et qui accomplissent des tâches dans le cadre de l'évaluation de la conformité des produits ou dispositifs couverts par la législation d'harmonisation de l'Union en question. C'est en particulier le cas en ce qui concerne les groupes d'experts, les laboratoires spécialisés et les laboratoires de référence dans le domaine des dispositifs médicaux conformément aux règlements (UE) 2017/745 et (UE) 2017/746.

(148)Le présent règlement devrait établir un cadre de gouvernance qui permette à la fois de coordonner et de soutenir l'application du présent règlement au niveau national, ainsi que de renforcer les capacités au niveau de l'Union et d'intégrer les parties prenantes dans le domaine de l'IA. La mise en œuvre et le contrôle de l'application effectifs du présent règlement requièrent un cadre de gouvernance qui permette de coordonner et de renforcer l'expertise centrale au niveau de l'Union. Le Bureau de l'IA a été créé par voie d'une décision de la Commission[45] et a pour mission d'approfondir l'expertise et de renforcer les capacités de l'Union dans le domaine de l'IA ainsi que de contribuer à la mise en œuvre de la législation de l'Union sur l'IA. Les États membres devraient faciliter l'accomplissement des missions du Bureau de l'IA en vue de soutenir le développement de l'expertise de l'Union et des capacités au niveau de l'Union et de renforcer le fonctionnement du marché unique numérique. En outre, il convient d'établir un Comité IA composé de représentants des États membres, un groupe scientifique visant à intégrer la communauté scientifique et un forum consultatif visant à recueillir les contributions des parties concernées en vue de la mise en œuvre du présent règlement, au niveau de l'Union et au niveau national. Le dévelop-

44. Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).
45. Décision de la Commission du 24 janvier 2024 créant le Bureau européen de l'intelligence artificielle (C/2024/390).

pement de l'expertise et des capacités de l'Union devrait également consister à utiliser les ressources et l'expertise existantes, en particulier grâce à des synergies avec les structures établies dans le contexte de l'application au niveau de l'Union d'autres dispositions législatives et à des synergies avec des initiatives connexes au niveau de l'Union, telles que l'entreprise commune EuroHPC et les installations de mise à l'essai de l'IA et d'expérimentations relevant du programme pour une Europe numérique.

(149)Afin de faciliter une mise en œuvre aisée, efficace et harmonisée du présent règlement, il convient de créer un Comité IA. Ce Comité IA devrait tenir compte des différents intérêts de l'écosystème de l'IA et être composé de représentants des États membres. Le Comité IA devrait être chargé d'un certain nombre de tâches consultatives, parmi lesquelles la formulation d'avis, de recommandations, de conseils ou la contribution à des orientations sur des questions liées à la mise en œuvre du présent règlement, y compris sur les questions relatives à l'exécution, les spécifications techniques ou les normes existantes concernant les exigences établies dans le présent règlement, et la fourniture de conseils à la Commission et aux États membres ainsi qu'à leurs autorités nationales compétentes sur des questions spécifiques liées à l'IA. Afin d'offrir une certaine souplesse aux États membres dans la désignation de leurs représentants au sein du Comité IA, ces représentants peuvent être toute personne appartenant à des entités publiques qui devraient avoir les compétences et les pouvoirs nécessaires pour faciliter la coordination au niveau national et contribuer à l'accomplissement des tâches du Comité IA. Le Comité IA devrait établir deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes sur des questions liées respectivement à la surveillance du marché et aux organismes notifiés. Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020. Conformément à l'article 33 dudit règlement, la Commission devrait apporter son soutien aux activités du sous-groupe permanent en procédant à des évaluations ou à des études du marché, en particulier en vue de recenser les aspects du présent règlement appelant une coordination particulière urgente entre les autorités de surveillance du marché. Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le Comité IA devrait également coopérer, lorsqu'il y a lieu, avec les organes, groupes d'experts et réseaux compétents de l'Union actifs dans le contexte de dispositions législatives pertinentes de l'Union, notamment ceux qui agissent au titre de la législation applicable de l'Union en matière de données, et de produits et services numériques.

(150)En vue d'assurer la participation des parties prenantes à la mise en œuvre et à l'application du présent règlement, il convient d'établir un forum consultatif chargé de conseiller le Comité IA et la Commission et de leur fournir une expertise technique. Afin d'assurer une représentation diversifiée et équilibrée des parties prenantes tenant compte des différents intérêts commerciaux et non commerciaux et, au sein de la catégorie des intérêts commerciaux, eu égard aux PME et autres entreprises, le forum consultatif devrait être composé, entre autres, de représentants du secteur, des jeunes pousses, des PME, du milieu universitaire, de la société civile, y compris les partenaires sociaux, ainsi que de l'Agence des droits fondamentaux, de l'ENISA, du Comité européen de normalisation (CEN), du Comité européen de normalisation électrotechnique (CENELEC) et de l'Institut européen de normalisation des télécommunications (ETSI).

(151)Afin de soutenir la mise en œuvre et le contrôle du respect du présent règlement, en particulier les activités de suivi du Bureau de l'IA concernant les modèles d'IA à usage général, il convient d'établir un groupe scientifique composé d'experts indépendants. Les experts indépendants constituant le groupe scientifique devraient être choisis en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA. Ils devraient s'acquitter de leurs tâches avec impartialité et objectivité et veiller à la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Afin de permettre le renforcement des capacités nationales nécessaires au contrôle effectif du respect du présent règlement, les États membres devraient être en mesure de solliciter l'aide de la réserve d'experts constituant le groupe scientifique pour leurs activités répressives.

(152)Afin de soutenir un contrôle de l'application adéquat en ce qui concerne les systèmes d'IA et de renforcer les capacités des États membres, il convient de créer et de mettre à la disposition des États membres des structures de soutien de l'Union pour les essais en matière d'IA.

(153)Les États membres jouent un rôle clé dans l'application et le contrôle du respect du présent règlement. À cet égard, chaque État membre devrait désigner au moins une autorité notifiante et au moins une autorité de surveillance du marché en tant qu'autorités nationales compétentes chargées de contrôler l'application et la mise en œuvre du présent règlement. Les États membres peuvent décider de désigner une entité publique, quel qu'en soit le type, qui soit chargée d'exécuter les tâches des autorités nationales compétentes au sens du présent règlement, en fonction de leurs caractéristiques et besoins organisationnels nationaux spécifiques. Afin d'accroître l'efficacité de l'organisation du côté des États membres et de définir un point de contact unique avec le public et les homologues au niveau des États membres et de l'Union, chaque État membre devrait désigner une autorité de surveillance du marché pour tenir le rôle de point de contact unique.

(154)Les autorités nationales compétentes devraient exercer leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver les principes d'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités devraient s'abstenir de toute action incompatible avec leurs fonctions et devraient être soumis aux règles de confidentialité prévues par le présent règlement.

(155)Afin de veiller à ce que les fournisseurs de systèmes d'IA à haut risque puissent prendre en considération l'expérience acquise dans l'utilisation de systèmes d'IA à haut risque pour améliorer leurs systèmes et le processus de conception et de développement, ou qu'ils puissent prendre d'éventuelles mesures correctives en temps utile, tous les fournisseurs devraient avoir mis en place un système de surveillance après commercialisation. Le cas échéant, la surveillance après commercialisation devrait comprendre une analyse de l'interaction avec d'autres systèmes d'IA, y compris d'autres dispositifs et logiciels. La surveillance après commercialisation ne devrait pas couvrir les données opérationnelles sensibles des utilisateurs de systèmes d'IA qui sont des autorités répressives. Ce système est aussi essentiel pour garantir que les risques potentiels découlant des systèmes d'IA qui continuent à «apprendre» après avoir été mis sur le marché ou mis en service puissent être traités plus efficacement et en temps utile. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système pour signaler aux autorités compétentes tout incident grave résultant de l'utilisation de leurs systèmes d'IA, à savoir un incident ou un dysfonctionnement entraînant la mort ou une atteinte grave à la santé, une perturbation grave et irréversible de la gestion et de l'exploitation des infrastructures critiques, des infractions aux obligations découlant du droit de l'Union visant à protéger les droits fondamentaux ou une atteinte grave aux biens ou à l'environnement.

(156)Afin de garantir un contrôle approprié et efficace du respect des exigences et obligations énoncées par le présent règlement, qui fait partie de la législation d'harmonisation de l'Union, le système de surveillance du marché et de mise en conformité des produits établi par le règlement (UE) 2019/1020 devrait s'appliquer dans son intégralité. Les autorités de surveillance du marché désignées en vertu du présent règlement devraient disposer de tous les pouvoirs d'exécution prévus par le présent règlement et par le règlement (UE) 2019/1020, et elles devraient exercer leurs pouvoirs et s'acquitter de leurs tâches de manière indépendante, impartiale et sans parti pris. Bien que la majorité des systèmes d'IA ne fassent pas l'objet d'exigences et obligations particulières au titre du présent règlement, les autorités de surveillance du marché peuvent prendre des mesures à l'égard de tous les systèmes d'IA lorsqu'ils présentent un risque conformément au présent règlement. En raison de la nature spécifique des institutions, agences et organes de l'Union relevant du champ d'application du présent règlement, il convient de désigner le Contrôleur européen de la protection des données comme autorité compétente pour la surveillance du marché en ce qui les concerne. Cela devrait être sans préjudice de la désignation des autorités nationales compétentes par les États membres. Les activités de surveillance du marché ne devraient pas affecter la capacité des entités surveillées à s'acquitter de leurs tâches de manière indépendante, lorsque cette indépendance constitue une exigence du droit de l'Union.

(157)Le présent règlement est sans préjudice des compétences, des tâches, des pouvoirs et de l'indépendance des autorités ou organismes publics nationaux compétents qui contrôlent l'application du droit de l'Union en matière de protection des droits fondamentaux, y compris les organismes chargés des questions d'égalité et les autorités de protection des données. Lorsque leur mandat l'exige, ces autorités ou organismes publics nationaux devraient également avoir accès à toute documentation créée en vertu du présent règlement. Une procédure de sauvegarde spécifique devrait être mise en place pour garantir une application adéquate et en temps utile opposable aux systèmes d'IA présentant un risque pour la santé, la sécurité et les droits fondamentaux. La procédure applicable à ces systèmes d'IA présentant un risque devrait être appliquée aux systèmes d'IA à haut risque présentant un risque, aux systèmes interdits qui ont été mis sur le marché, mis en service ou utilisés en violation des interdictions concernant des pratiques définies par le présent règlement, et aux systèmes d'IA qui ont été mis à disposition en violation des exigences de transparence énoncées dans le présent règlement et qui présentent un risque.

cf. CNIL

(158)Le droit de l'Union en matière de services financiers comprend des règles et des exigences en matière de gouvernance interne et de gestion des risques qui sont applicables aux établissements financiers réglementés dans le cadre de la fourniture de ces services, y compris lorsqu'ils font usage de systèmes d'IA. Afin d'assurer la cohérence de l'application et du contrôle du respect des obligations découlant du présent règlement et des règles et exigences pertinentes prévues par les actes juridiques de l'Union sur les services financiers, les autorités compétentes chargées de la surveillance et du contrôle de l'application de ces actes juridiques, en particulier les autorités compétentes au sens du règlement (UE) no 575/2013 du Parlement européen et du Conseil[46] et des directives 2008/48/CE[47], 2009/138/CE[48], 2013/36/UE[49], 2014/17/UE[50] et (UE) 2016/97[51] du Parlement européen et du Conseil, devraient être désignées, dans les limites de leurs compétences respectives, comme les autorités compétentes aux fins de la surveillance de la mise en œuvre du présent règlement, y compris pour les activités de surveillance du marché, en ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements financiers réglementés et surveillés, à moins que les États membres ne décident de désigner une autre autorité pour remplir ces tâches de surveillance du marché. Ces autorités compétentes devraient disposer, en vertu du présent règlement et du règlement (UE) 2019/1020, de tous les pouvoirs nécessaires pour faire respecter les exigences et obligations du présent règlement, y compris le pouvoir d'effectuer des activités de surveillance du marché ex post qui peuvent être intégrées, le cas échéant, dans leurs mécanismes et procédures de surveillance existants au titre du droit de l'Union en matière de services financiers. Il convient d'envisager que, lorsqu'elles agissent en tant qu'autorités de surveillance du marché au titre du présent règlement, les autorités nationales responsables de la surveillance des établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) no 1024/2013 du Conseil[52], doivent communiquer sans délai à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt pour les missions de surveillance prudentielle de la Banque centrale européenne telles qu'elles sont définies dans ledit règlement.

46. Règlement (UE) no 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) no 648/2012 (JO L 176 du 27.6.2013, p. 1).
47. Directive 2008/48/CE du Parlement européen et du Conseil du 23 avril 2008 concernant les contrats de crédit aux consommateurs et abrogeant la directive 87/102/CEE du Conseil (JO L 133 du 22.5.2008, p. 66).
48. Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (JO L 335 du 17.12.2009, p. 1).
49. Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).
50. Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) no 1093/2010 (JO L 60 du 28.2.2014, p. 34).
51. Directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances (JO L 26 du 2.2.2016, p. 19).
52. Règlement (UE) no 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

Pour renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit régis par la directive 2013/36/UE, il convient aussi d'intégrer certaines des obligations procédurales des fournisseurs en ce qui concerne la gestion des risques, la surveillance après commercialisation et la documentation dans les obligations et procédures existantes au titre de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient aussi être envisagées en ce qui concerne le système de gestion de la qualité des fournisseurs et l'obligation de suivi imposée aux déployeurs de systèmes d'IA à haut risque dans la mesure où les dispositions y afférentes s'appliquent aux établissements de crédit régis par la directive 2013/36/UE. Le même régime devrait s'appliquer aux entreprises d'assurance et de réassurance et aux sociétés holding d'assurance relevant de la directive 2009/138/CE, aux intermédiaires d'assurance relevant de la directive (UE) 2016/97, ainsi qu'aux autres types d'établissements financiers soumis à des exigences en matière de gouvernance, de dispositifs ou de processus internes établis en vertu des dispositions pertinentes du droit de l'Union en matière de services financiers afin d'assurer la cohérence et l'égalité de traitement dans le secteur financier.

cf. déployeurs

(159)Chaque autorité de surveillance du marché chargée des systèmes d'IA à haut risque dans le domaine de la biométrie énumérés dans une annexe du présent règlement, dans la mesure où ces systèmes sont utilisés à des fins liées aux activités répressives, à la migration, à l'asile et à la gestion des contrôles aux frontières ou à l'administration de la justice et aux processus démocratiques, devrait disposer de pouvoirs effectifs en matière d'enquête et de mesures correctives, y compris au minimum le pouvoir d'obtenir l'accès à toutes les données à caractère personnel traitées et à toutes les informations nécessaires à l'accomplissement de ses tâches. Les autorités de surveillance du marché devraient être en mesure d'exercer leurs pouvoirs en toute indépendance. Toute restriction de leur accès à des données opérationnelles sensibles au titre du présent règlement devrait être sans préjudice des pouvoirs qui leur sont conférés par la directive (UE) 2016/680. Aucune exclusion concernant la divulgation de données aux autorités nationales chargées de la protection des données au titre du présent règlement ne devrait avoir d'incidence sur les pouvoirs actuels ou futurs de ces autorités au-delà du champ d'application du présent règlement.

cf. CNIL

(160)Les autorités de surveillance du marché et la Commission devraient être en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener par les autorités de surveillance du marché ou par les autorités de surveillance du marché conjointement avec la Commission, visant à promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser et de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont recensés comme présentant un risque grave dans au moins deux États membres. Les activités conjointes visant à promouvoir le respect de la législation devraient être menées conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA devrait assurer la coordination centrale des enquêtes conjointes.

(161)Il est nécessaire de clarifier les responsabilités et les compétences au niveau de l'Union et au niveau national en ce qui concerne les systèmes d'IA qui reposent sur des modèles d'IA à usage général. Afin d'éviter les chevauchements de compétences, lorsqu'un système est fondé sur un modèle d'IA à usage général et que le modèle et le système sont fournis par le même fournisseur, la surveillance devrait avoir lieu au niveau de l'Union par l'intermédiaire du Bureau de l'IA, qui devrait disposer à cette fin des pouvoirs d'une autorité de surveillance du marché au sens du règlement (UE) 2019/1020. Dans tous les autres cas, les autorités nationales de surveillance du marché demeurent chargées de la surveillance des systèmes d'IA. Toutefois, pour les systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque, les autorités de surveillance du marché devraient coopérer avec le Bureau de l'IA pour mener les évaluations de la conformité, et informer le Comité IA et les autres autorités de surveillance du marché en conséquence. En outre, toute autorité de surveillance du marché devrait être en mesure de solliciter l'assistance du Bureau de l'IA lorsqu'elle n'est pas en mesure de conclure une enquête sur un système d'IA à haut risque parce qu'elle ne peut accéder à certaines informations liées au modèle d'IA à usage général sur lequel repose ce système. Dans de tels cas, la procédure relative à l'assistance mutuelle pour les cas transfrontières prévue au chapitre VI du règlement (UE) 2019/1020 devrait s'appliquer mutatis mutandis.

cf. déployeurs

(162)Afin de tirer le meilleur parti de l'expertise centralisée de l'Union et des synergies au niveau de l'Union, les pouvoirs de surveillance et de contrôle du respect des obligations incombant aux fournisseurs de modèles d'IA à usage général devraient relever de la compétence de la Commission. Le Bureau de l'IA devrait être en mesure de prendre toutes les mesures nécessaires pour contrôler la mise en œuvre effective du présent règlement en ce qui concerne les modèles d'IA à usage général. Il devrait être en mesure d'enquêter sur d'éventuelles infractions aux règles incombant aux fournisseurs de modèles d'IA à usage général, aussi bien de sa propre initiative, selon les résultats de ses activités de surveillance, ou sur demande des autorités de surveillance du marché conformément aux conditions prévues par le présent règlement. Afin de contribuer à une surveillance effective par le Bureau de l'IA, celui-ci devrait donner la possibilité aux fournisseurs en aval d'introduire des réclamations concernant d'éventuelles infractions aux règles relatives aux fournisseurs de modèles et systèmes d'IA à usage général.

(163)En vue de compléter les systèmes de gouvernance des modèles d'IA à usage général, le groupe scientifique devrait soutenir les activités de surveillance du Bureau de l'IA et pourrait, dans certains cas, soumettre au Bureau de l'IA des alertes qualifiées qui déclenchent des mesures de suivi telles que des enquêtes. Cela devrait être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général présente un risque concret et identifiable au niveau de l'Union. Cela devrait aussi être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général remplit les critères qui conduiraient à une classification en tant que modèle d'IA à usage général présentant un risque systémique. Afin que le groupe scientifique dispose des informations nécessaires à l'exécution de ces tâches, il devrait exister un mécanisme permettant au groupe scientifique de demander à la Commission d'exiger du fournisseur qu'il fournisse des documents ou des informations.

(164)Le Bureau de l'IA devrait être en mesure de prendre les mesures nécessaires pour contrôler la mise en œuvre effective et le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général énoncées dans le présent règlement. Le Bureau de l'IA devrait être en mesure d'enquêter sur d'éventuelles infractions conformément aux pouvoirs qui lui sont conférés au titre du présent règlement, y compris en exigeant des documents et des informations, en réalisant des évaluations, ainsi qu'en exigeant que des mesures soient prises par les fournisseurs de modèles d'IA à usage général. Lors de la réalisation des évaluations, afin de tirer parti d'une expertise indépendante, le Bureau de l'IA devrait pouvoir faire appel à des experts indépendants pour réaliser les évaluations en son nom. Le respect des obligations devrait pouvoir être imposé, entre autres, par des demandes de prendre des mesures appropriées, y compris des mesures d'atténuation des risques dans le cas de risques systémiques recensés, ainsi qu'en restreignant la mise à disposition du modèle sur le marché, en le retirant ou en le rappelant. À titre de garantie, lorsque cela est nécessaire en sus des droits procéduraux prévus par le présent règlement, les fournisseurs de modèles d'IA à usage général devraient jouir des droits procéduraux prévus à l'article 18 du règlement (UE) 2019/1020, qui devraient s'appliquer mutatis mutandis, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

(165)Le développement de systèmes d'IA autres que les systèmes d'IA à haut risque dans le respect des exigences du présent règlement peut conduire à une plus large adoption d'une IA éthique et digne de confiance dans l'Union. Les fournisseurs de systèmes d'IA qui ne sont pas à haut risque devraient être encouragés à établir des codes de conduite, accompagnés de mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire de tout ou partie des exigences obligatoires applicables aux systèmes d'IA à haut risque, adaptés en fonction de la destination des systèmes et des risques plus faibles encourus et tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur, tels que les cartes modèles et les fiches de données. Les fournisseurs et, le cas échéant, les déployeurs de tous les systèmes d'IA, à haut risque ou non, et modèles d'IA devraient aussi être encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, par exemple, aux éléments des lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance, à la durabilité environnementale, aux mesures relatives à la maîtrise de l'IA, à la conception et au développement inclusifs et diversifiés des systèmes d'IA, y compris en prêtant attention aux personnes vulnérables et à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes avec la contribution, le cas échéant, de parties prenantes concernées telles que les organisations d'entreprises et de

cf. déployeurs

la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs à la conception et au développement des systèmes d'IA, ainsi qu'à la diversité des équipes de développement, y compris l'équilibre hommes-femmes. Afin que les codes de conduite volontaires portent leurs effets, ils devraient s'appuyer sur des objectifs clairs et des indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs. Ils devraient également être élaborés de manière inclusive, selon qu'il convient, avec la participation des parties prenantes concernées telles que les organisations d'entreprises et de la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs. La Commission peut élaborer des initiatives, y compris de nature sectorielle, pour faciliter la suppression des obstacles techniques entravant l'échange transfrontière de données pour le développement de l'IA, notamment en ce qui concerne l'infrastructure d'accès aux données et l'interopérabilité sémantique et technique des différents types de données.

(166)Il importe que les systèmes d'IA liés à des produits qui ne sont pas à haut risque au titre du présent règlement et qui ne sont donc pas tenus d'être conformes aux exigences énoncées pour les systèmes d'IA à haut risque soient néanmoins sûrs lorsqu'ils sont mis sur le marché ou mis en service. Pour contribuer à cet objectif, l'application du règlement (UE) 2023/988 du Parlement européen et du Conseil[53] constituerait un filet de sécurité.

(167)Afin d'assurer une coopération constructive et en toute confiance entre les autorités compétentes au niveau de l'Union et au niveau national, toutes les parties intervenant dans l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans le cadre de l'exécution de leurs tâches, conformément au droit de l'Union et au droit national. Elles devraient s'acquitter de leurs tâches et activités de manière à protéger, en particulier, les droits de propriété intellectuelle, les informations commerciales confidentielles et les secrets d'affaires, la mise en œuvre effective du présent règlement, les intérêts en matière de sécurité nationale et publique, l'intégrité des procédures pénales et administratives et l'intégrité des informations classifiées.

(168)Le respect des dispositions du présent règlement devrait pouvoir être imposé au moyen de sanctions et d'autres mesures d'exécution. Les États membres devraient prendre toutes les mesures nécessaires pour que les dispositions du présent règlement soient mises en œuvre et, notamment, prévoir des sanctions effectives, proportionnées et dissuasives en cas de violation de ces dispositions, et dans le respect du principe non bis in idem. Afin de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation du présent règlement, il convient d'établir le montant maximal pour la fixation des amendes administratives pour certaines infractions spécifiques. Pour évaluer le montant des amendes, les États membres devraient, dans chaque cas d'espèce, tenir compte de toutes les caractéristiques propres à la situation spécifique, en prenant notamment en considération la nature, la gravité et la durée de l'infraction et ses conséquences, ainsi que la taille du fournisseur, en particulier s'il s'agit d'une PME, y compris les jeunes pousses. Le Contrôleur européen de la protection des données devrait avoir le pouvoir d'infliger des amendes aux institutions, agences et organes de l'Union relevant du présent règlement.

(169)Le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général au titre du présent règlement devrait pouvoir être imposé, entre autres, au moyen d'amendes. À cette fin, des niveaux appropriés d'amendes devraient également être fixés pour les infractions à ces obligations, y compris le non-respect de mesures demandées par la Commission en vertu au présent règlement, sous réserve de délais de prescription appropriés conformément du principe de proportionnalité. Toutes les décisions prises par la Commission au titre du présent règlement sont soumises au contrôle de la Cour de justice de l'Union européenne conformément au traité sur le fonctionnement de l'Union européenne, y compris la compétence de pleine juridiction de la Cour de justice en ce qui concerne les sanctions en application de l'article 261 du traité sur le fonctionnement de l'Union européenne.

53. Règlement (UE) 2023/988 du Parlement européen et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits, modifiant le règlement (UE) no 1025/2012 du Parlement européen et du Conseil et la directive (UE) 2020/1828 du Parlement européen et du Conseil, et abrogeant la directive 2001/95/CE du Parlement européen et du Conseil et la directive 87/357/CEE du Conseil (JO L 135 du 23.5.2023, p. 1).

(170)Le droit de l'Union et le droit national prévoient déjà des voies de recours effectives pour les personnes physiques et morales qui subissent une atteinte à leurs droits et libertés en raison de l'utilisation de systèmes d'IA. Sans préjudice de ces recours, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement devrait avoir le droit d'introduire une réclamation auprès de l'autorité de surveillance du marché concernée.

(171)Les personnes concernées devraient avoir le droit d'obtenir une explication lorsque la décision d'un déployeur est principalement fondée sur les sorties de certains systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et lorsque cette décision produit des effets juridiques ou cause un préjudice important de façon similaire à ces personnes d'une manière qu'elles considèrent comme ayant une incidence négative sur leur santé, leur sécurité ou leurs droits fondamentaux. Cette explication devrait être claire et pertinente, et constituer une base à partir de laquelle les personnes concernées peuvent exercer leurs droits. Le droit d'obtenir une explication ne devrait pas s'appliquer à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions découlent du droit de l'Union ou du droit national et ne devrait s'appliquer que dans la mesure où ce droit n'est pas déjà prévu par le droit de l'Union.

cf. déployeurs

(172)Les personnes agissant en tant que lanceurs d'alerte eu égard à des infractions au présent règlement devraient être protégées en vertu du droit de l'Union. La directive (UE) 2019/1937 du Parlement européen et du Conseil[54] devrait donc s'appliquer aux signalements d'infractions au présent règlement et à la protection des personnes signalant ces infractions.

(173)Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission pour lui permettre de modifier les conditions dans lesquelles un système d'IA ne doit pas être considéré comme étant à haut risque, la liste des systèmes d'IA à haut risque, les dispositions relatives à la documentation technique, le contenu de la déclaration «UE» de conformité, les dispositions relatives aux procédures d'évaluation de la conformité, les dispositions établissant les systèmes d'IA à haut risque auxquels devrait s'appliquer la procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique, le seuil, les critères de référence et les indicateurs, y compris en complétant ces critères de référence et indicateurs, dans les règles de classification des modèles d'IA à usage général présentant un risque systémique, les critères de désignation des modèles d'IA à usage général présentant un risque systémique, la documentation technique destinée aux fournisseurs de modèles d'IA à usage général et les informations relatives à la transparence pour les fournisseurs de modèles d'IA à usage général. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer»[55]. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

(174)Compte tenu de l'évolution rapide des technologies et de l'expertise technique requise aux fins de la bonne application du présent règlement, la Commission devrait évaluer et réexaminer le présent règlement au plus tard le 2 août 2029 et tous les quatre ans par la suite, et faire rapport au Parlement européen et au Conseil. En outre, en tenant compte des conséquences sur le champ d'application du présent règlement, la Commission devrait procéder à une évaluation de la nécessité de modifier une fois par an la liste des systèmes d'IA à haut risque et la liste des pratiques interdites. En outre, au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission devrait

54. Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).
55. JO L 123 du 12.5.2016, p. 1.

évaluer la nécessité de modifier les rubriques de la liste des domaines à haut risque figurant à l'annexe du présent règlement, les systèmes d'IA relevant des obligations de transparence, l'efficacité du système de surveillance et de gouvernance ainsi que l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, y compris la nécessité de mesures ou d'actions supplémentaires, et faire rapport au Parlement européen et au Conseil. Enfin, au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission devrait évaluer l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées pour les systèmes d'IA à haut risque dans le cas des systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour de tels systèmes d'IA.

(175)Afin de garantir des conditions uniformes de mise en œuvre du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) no 182/2011 du Parlement européen et du Conseil[56].

(176)Étant donné que l'objectif du présent règlement, à savoir améliorer le fonctionnement du marché intérieur et promouvoir l'adoption d'une IA axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, y compris la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions et des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(177)Afin d'assurer la sécurité juridique, de veiller à ce que les opérateurs disposent d'une période d'adaptation appropriée et d'éviter toute perturbation du marché, y compris en assurant la continuité de l'utilisation des systèmes d'IA, il convient que le présent règlement s'applique aux systèmes d'IA à haut risque qui ont été mis sur le marché ou mis en service avant la date générale d'application de celui-ci, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leur conception ou de leur destination. Il convient de préciser qu'à cet égard, la notion d'importante modification devrait être comprise comme équivalente sur le fond à celle de modification substantielle, qui est utilisée uniquement en ce qui concerne les systèmes d'IA à haut risque au titre du présent règlement. À titre exceptionnel et compte tenu de l'obligation de rendre des comptes au public, les exploitants de systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe du présent règlement et les exploitants de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques devraient prendre les mesures nécessaires pour se conformer aux exigences du présent règlement, respectivement, d'ici à la fin de 2030 et au plus tard le 2 août 2030.

(178)Les fournisseurs de systèmes d'IA à haut risque sont encouragés à commencer à se conformer, sur une base volontaire, aux obligations pertinentes du présent règlement dès la période transitoire.

(179)Le présent règlement devrait s'appliquer à partir du 2 août 2026. Toutefois, compte tenu du risque inacceptable associé à certaines utilisations de l'IA, les interdictions ainsi que les dispositions générales du présent règlement devraient déjà s'appliquer à compter du 2 février 2025. Si le plein effet de ces interdictions découle de la mise en place de la gouvernance et du contrôle du respect du présent règlement, il importe d'anticiper l'application des interdictions afin de tenir compte des risques inacceptables et d'avoir un effet sur d'autres procédures, par exemple en droit civil. En outre, l'infrastructure liée à la gouvernance et au système d'évaluation de la conformité devrait être opérationnelle avant le 2 août 2026, et les dispositions relatives aux organismes notifiés et à la structure de gouvernance devraient donc s'appliquer à

56. Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

compter du 2 août 2025. Compte tenu du rythme rapide des avancées technologiques et de l'adoption des modèles d'IA à usage général, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer à compter du 2 août 2025. Les codes de bonne pratique devraient être prêts au plus tard le 2 mai 2025 afin de permettre aux fournisseurs de démontrer leur conformité à temps. Le Bureau de l'IA devrait veiller à ce que les règles et procédures de classification soient à jour des évolutions technologiques. En outre, les États membres devraient définir et notifier à la Commission les règles relatives aux sanctions, y compris les amendes administratives, et veiller à ce qu'elles soient correctement et efficacement mises en œuvre à la date d'application du présent règlement. Par conséquent, les dispositions relatives aux sanctions devraient s'appliquer à compter du 2 août 2025.

(180)Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis conjoint le 18 juin 2021,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Disposition générales

article premier
Objet

1. L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation.

2. Le présent règlement établit:

a) des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation de systèmes d'IA dans l'Union;

b) l'interdiction de certaines pratiques en matière d'IA;

c) des exigences spécifiques applicables aux systèmes d'IA à haut risque et des obligations imposées aux opérateurs de ces systèmes;

d) des règles harmonisées en matière de transparence applicables à certains systèmes d'IA;

e) des règles harmonisées pour la mise sur le marché de modèles d'IA à usage général;

f) des règles relatives au suivi du marché, à la surveillance du marché, à la gouvernance et à l'application des règles;

g) des mesures visant à soutenir l'innovation, en mettant particulièrement l'accent sur les PME, y compris les jeunes pousses.

article 2
Champ d'application

1. Le présent règlement s'applique:

Acteurs de l'IA :
- fournisseurs
- déployeurs
- importateurs
- distrubuteurs
- fabricants
- mandataires
- personnes concernées

a) aux fournisseurs établis ou situés dans l'Union ou dans un pays tiers qui mettent sur le marché ou mettent en service des systèmes d'IA ou qui mettent sur le marché des modèles d'IA à usage général dans l'Union;

b) aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans l'Union;

c) aux fournisseurs et aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans un pays tiers, lorsque les sorties produites par le système d'IA sont utilisées dans l'Union;

d) aux importateurs et aux distributeurs de systèmes d'IA;

e) aux fabricants de produits qui mettent sur le marché ou mettent en service un système d'IA en même temps que leur produit et sous leur propre nom ou leur propre marque;

f) aux mandataires des fournisseurs qui ne sont pas établis dans l'Union;

g) aux personnes concernées qui sont situées dans l'Union.

2. En ce qui concerne les systèmes d'IA classés à haut risque conformément à l'article 6, paragraphe 1, liés aux produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, seuls l'article 6, paragraphe 1, les articles 102 à 109 et l'article 112 s'appliquent. L'article 57 ne s'applique que dans la mesure où les exigences applicables aux systèmes d'IA à haut risque au titre du présent règlement ont été intégrées dans ladite législation d'harmonisation de l'Union.

3. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en matière de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétences.

Le présent règlement ne s'applique pas aux systèmes d'IA si et dans la mesure où ils sont mis sur le marché, mis en service ou utilisés avec ou sans modifications exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

Le présent règlement ne s'applique pas aux systèmes d'IA qui ne sont pas mis sur le marché ou mis en service dans l'Union, lorsque les sorties sont utilisées dans l'Union exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

4. Le présent règlement ne s'applique ni aux autorités publiques d'un pays tiers ni aux organisations internationales relevant du champ d'application du présent règlement en vertu du paragraphe 1, lorsque ces autorités ou organisations utilisent des systèmes d'IA dans le cadre de la coopération internationale ou d'accords internationaux de coopération des services répressifs et judiciaires avec l'Union ou avec un ou plusieurs États membres, à condition que ce pays tiers ou cette organisation internationale fournisse des garanties adéquates en ce qui concerne la protection des droits fondamentaux et des libertés des personnes.

5. Le présent règlement n'affecte pas l'application des dispositions relatives à la responsabilité des prestataires intermédiaires énoncées au chapitre II du règlement (UE) 2022/2065.

6. Le présent règlement ne s'applique pas aux systèmes d'IA ou aux modèles d'IA spécifiquement développés et mis en service uniquement à des fins de recherche et développement scientifiques, ni à leurs sorties.

7. Le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 ou le règlement (UE) 2018/1725, ni sur la directive 2002/58/CE ou la directive (UE) 2016/680, sans préjudice de l'article 10, paragraphe 5, et de l'article 59 du présent règlement.

cf. RGPD

8. Le présent règlement ne s'applique pas aux activités de recherche, d'essai et de développement relatives aux systèmes d'IA ou modèles d'IA avant leur mise sur le marché ou leur mise en service. Ces activités sont menées conformément au droit de l'Union applicable. Les essais en conditions réelles ne sont pas couverts par cette exclusion.

9. Le présent règlement s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union relatifs à la protection des consommateurs et à la sécurité des produits.

10. Le présent règlement ne s'applique pas aux obligations incombant aux déployeurs qui sont des personnes physiques utilisant des systèmes d'IA dans le cadre d'une activité strictement personnelle à caractère non professionnel.

cf. déployeurs

11. Le présent règlement n'empêche pas l'Union ou les États membres de maintenir ou d'introduire des dispositions législatives, réglementaires ou administratives plus favorables aux travailleurs quant à la protection de leurs droits en ce qui concerne l'utilisation de systèmes d'IA par les employeurs, ou d'encourager ou de permettre l'application de conventions collectives plus favorables aux travailleurs.

12. Le présent règlement ne s'applique pas aux systèmes d'IA publiés dans le cadre de licences libres et ouvertes, sauf s'ils sont mis sur le marché ou mis en service en tant que systèmes d'IA à haut risque ou en tant que systèmes d'IA qui relèvent de l'article 5 ou de l'article 50.

article 3
Définitions

Aux fins du présent règlement, on entend par:

1) «système d'IA», un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels;

2) «risque», la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci;

3) «fournisseur», une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;

4) «déployeur», une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel;

cf. déployeurs

5) «mandataire», une personne physique ou morale située ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou de modèle d'IA à usage général pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement;

6) «importateur», une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers;

7) «distributeur», une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union;

8) «opérateur», un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur;

9) «mise sur le marché», la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'Union;

10) «mise à disposition sur le marché», la fourniture d'un système d'IA ou d'un modèle d'IA à usage général destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

11) «mise en service», la fourniture d'un système d'IA en vue d'une première utilisation directement au déployeur ou pour usage propre dans l'Union, conformément à la destination du système d'IA;

12) «destination», l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique;

13) «mauvaise utilisation raisonnablement prévisible», l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA;

14) «composant de sécurité», un composant d'un produit ou d'un système d'IA qui remplit une fonction de sécurité pour ce produit ou ce système d'IA, ou dont la défaillance ou le dysfonctionnement met en danger la santé et la sécurité des personnes ou des biens;

15) «notice d'utilisation», les indications communiquées par le fournisseur pour informer le déployeur, en particulier, de la destination et de l'utilisation correcte d'un système d'IA;

cf. déployeurs

16) «rappel d'un système d'IA», toute mesure visant à assurer le retour au fournisseur d'un système d'IA mis à la disposition de déployeurs ou à le mettre hors service ou à désactiver son utilisation;

cf. déployeurs

17) «retrait d'un système d'IA», toute mesure visant à empêcher qu'un système d'IA se trouvant dans la chaîne d'approvisionnement ne soit mis à disposition sur le marché;

18) «performance d'un système d'IA», la capacité d'un système d'IA à remplir sa destination;

19) «autorité notifiante», l'autorité nationale chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle;

20) «évaluation de la conformité», la procédure permettant de démontrer que les exigences relatives à un système d'IA à haut risque énoncées au chapitre III, section 2, ont été respectées;

21) «organisme d'évaluation de la conformité», un organisme en charge des activités d'évaluation de la conformité par un tiers, y compris la mise à l'essai, la certification et l'inspection;

22) «organisme notifié», un organisme d'évaluation de la conformité notifié en application du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents;

23) «modification substantielle», une modification apportée à un système d'IA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le système d'IA a été évalué;

24) «marquage CE», un marquage par lequel le fournisseur indique qu'un système d'IA est conforme aux exigences du chapitre III, section 2, et d'autres actes législatifs d'harmonisation de l'Union applicables qui en prévoient l'apposition;

25) «système de surveillance après commercialisation», l'ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser les données issues de l'expérience d'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service de manière à repérer toute nécessité d'appliquer immédiatement une mesure préventive ou corrective;

26) «autorité de surveillance du marché», l'autorité nationale assurant la mission et prenant les mesures prévues par le règlement (UE) 2019/1020;

27) «norme harmonisée», une norme harmonisée au sens de l'article 2, paragraphe 1, point c), du règlement (UE) no 1025/2012;

28) «spécification commune», un ensemble de spécifications techniques au sens de l'article 2, point 4), du règlement (UE) no 1025/2012 qui permettent de satisfaire à certaines exigences établies en vertu du présent règlement;

29) «données d'entraînement», les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînables;

30) «données de validation», les données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement;

31) «jeu de données de validation», un jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe;

32) «données de test», les données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service;

33) «données d'entrée», les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit une sortie;

34) «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques;

35) «identification biométrique», la reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données;

36) «vérification biométrique», la vérification «un à un» automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies;

37) «catégories particulières de données à caractère personnel», les catégories de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679, à l'article 10 de la directive (UE) 2016/680 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725;

cf. RGPD art. 9.1

38) «données opérationnelles sensibles», les données opérationnelles relatives à des activités de prévention et de détection des infractions pénales, ainsi que d'enquête ou de poursuites en la matière, dont la divulgation pourrait compromettre l'intégrité des procédures pénales;

39) «système de reconnaissance des émotions», un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques;

40) «système de catégorisation biométrique», un système d'IA destiné à affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques, à moins que cela ne soit accessoire à un autre service commercial et strictement nécessaire pour des raisons techniques objectives;

41) «système d'identification biométrique à distance», un système d'IA destiné à identifier des personnes physiques sans leur participation active, généralement à distance, en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données;

42) «système d'identification biométrique à distance en temps réel», un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel important et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles;

43) «système d'identification biométrique à distance a posteriori», un système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel;

44) «espace accessible au public», tout espace physique de propriété publique ou privée, accessible à un nombre indéterminé de personnes physiques, indépendamment de l'existence de conditions d'accès à cet espace qui puissent s'appliquer, et indépendamment d'éventuelles restrictions de capacité;

45) «autorités répressives»,

a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

46) «activités répressives», des activités menées par les autorités répressives ou pour leur compte pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

47) «Bureau de l'IA», la fonction de la Commission consistant à contribuer à la mise en œuvre, au suivi et à la surveillance des systèmes d'IA et de modèles d'IA à usage général et de la gouvernance de l'IA, établi par la décision de la Commission du 24 janvier 2024; les références faites au Bureau de l'IA dans le présent règlement s'entendent comme faites à la Commission;

48) ««autorité nationale compétente», une autorité notifiante ou une autorité de surveillance du marché; en ce qui concerne les systèmes d'IA mis en service ou utilisés par les institutions, organes ou organismes de l'Union, les références aux autorités nationales compétentes ou aux autorités de surveillance du marché dans le présent règlement s'entendent comme une référence au Contrôleur européen de la protection des données;

Pour les organes de l'Union, c'est le CEPD/EDPS qui est l'autorité compétente

49) «incident grave», un incident ou dysfonctionnement d'un système d'IA entraînant directement ou indirectement:

a) le décès d'une personne ou une atteinte grave à la santé d'une personne;

b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques;

c) la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux;

d) un dommage grave à des biens ou à l'environnement;

50) «données à caractère personnel», les données à caractère personnel définies à l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD art. 4.1

51) «données à caractère non personnel», les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

cf. RGPD art. 4.1

52) «profilage», le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

cf. RGPD art. 4.4

53) «plan d'essais en conditions réelles», un document décrivant les objectifs, la méthode, la population et le champ d'application géographique et la portée dans le temps, le suivi, l'organisation et la conduite des essais en conditions réelles;

54) «plan du bac à sable», un document adopté conjointement entre le fournisseur participant et l'autorité compétente, qui décrit les objectifs, les conditions, les délais, la méthodologie et les exigences applicables aux activités réalisées au sein du bac à sable;

55) «bac à sable réglementaire de l'IA», un cadre contrôlé mis en place par une autorité compétente qui offre aux fournisseurs ou fournisseurs potentiels de systèmes d'IA la possibilité de développer, d'entraîner, de valider et de tester, lorsqu'il y a lieu en conditions réelles, un système d'IA innovant, selon un plan du bac à sable pour une durée limitée sous surveillance réglementaire;

56) «maîtrise de l'IA», les compétences, les connaissances et la compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte du présent règlement, de procéder à un déploiement des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques que comporte l'IA, ainsi que des préjudices potentiels qu'elle peut causer;

cf. déployeurs

57) «essais en conditions réelles», les essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la conformité du système d'IA aux exigences du présent règlement; les essais en conditions réelles ne remplissent pas les conditions pour constituer une mise sur le marché ni une mise en service du système d'IA au sens du présent règlement, pour autant que toutes les conditions prévues à l'article 57 ou à l'article 60 soient remplies;

58) «participant», aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles;

59) «consentement éclairé», l'expression libre, spécifique, univoque et volontaire, par un participant, de sa volonté de participer à un essai en conditions réelles particulier, après avoir été informé de tous les éléments de l'essai qui lui permettent de prendre sa décision concernant sa participation;

60) «hypertrucage», une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques;

61) «infraction de grande ampleur», tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui:

a) a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui:
   i) où l'acte ou l'omission en question a son origine ou a eu lieu;
   ii) où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi; ou
   iii) où le déployeur est établi, lorsque l'infraction est commise par le déployeur;

cf. déployeurs

b) a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres;

62) «infrastructure critique», une infrastructure critique au sens de l'article 2, point 4), de la directive (UE) 2022/2557;

63) «modèle d'IA à usage général», un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de

manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché;

64) «capacités à fort impact», des capacités égales ou supérieures aux capacités enregistrées dans les modèles d'IA à usage général les plus avancés;

65) «risque systémique», un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur;

66) «système d'IA à usage général», un système d'IA qui est fondé sur un modèle d'IA à usage général et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA;

67) «opération en virgule flottante», toute opération ou assignation mathématique impliquant des nombres en virgule flottante, qui constituent un sous-ensemble des nombres réels généralement représentés sur un ordinateur par un entier de précision fixe suivi d'un exposant entier d'une base fixe;

68) «fournisseur en aval», un fournisseur d'un système d'IA, y compris d'un système d'IA à usage général, qui intègre un modèle d'IA, que le modèle d'IA soit fourni par lui-même ou non, et verticalement intégré ou fourni par une autre entité sur la base de relations contractuelles.

article 4
Maîtrise de l'IA

cf. déployeurs

Les fournisseurs et les déployeurs de systèmes d'IA prennent des mesures pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés.

CHAPITRE II
PRATIQUES INTERDITES EN MATIÈRE D'IA

Pratiques interdites

article 5
Pratiques interdites en matière d'IA

1. Les pratiques en matière d'IA suivantes sont interdites:

a) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales, au-dessous du seuil de conscience d'une personne, ou à des techniques délibérément manipulatrices ou trompeuses, avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne ou d'un groupe de personnes en portant considérablement atteinte à leur capacité à prendre une décision éclairée, amenant ainsi la personne à prendre une décision qu'elle n'aurait pas prise autrement, d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne, à une autre personne ou à un groupe de personnes;

b) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne physique ou d'un groupe de personnes donné avec pour objectif ou effet d'altérer substantiellement le comportement de cette personne ou d'un membre de ce groupe d'une manière qui

cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à un tiers;

c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA pour l'évaluation ou la classification de personnes physiques ou de groupes de personnes au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, la note sociale conduisant à l'une ou l'autre des situations suivantes, ou aux deux:

   i) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes de personnes dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine;

   ii) le traitement préjudiciable ou défavorable de certaines personnes ou de groupes de personnes, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci;

d) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour mener des évaluations des risques des personnes physiques visant à évaluer ou à prédire le risque qu'une personne physique commette une infraction pénale, uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques; cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour étayer l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables, directement liés à une activité criminelle;

e) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance;

f) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement, sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité;

g) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes de catégorisation biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle; cette interdiction ne couvre pas l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif;

h) l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs suivants:

   i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues;

   ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste;

   iii) la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans.

Le premier alinéa, point h), est sans préjudice de l'article 9 du règlement (UE) 2016/679 pour le traitement des données biométriques à des fins autres que répressives.

cf. RGPD art. 9

2. L'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), n'est déployée aux fins énoncées audit point, que pour confirmer l'identité de la personne spécifiquement ciblée et tient compte des éléments suivants:

a) la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité et l'ampleur du préjudice qui serait causé si le système n'était pas utilisé;

b) les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences.

En outre, l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), du présent article respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, conformément au droit national qui l'autorise, notamment eu égard aux limitations temporelles, géographiques et relatives aux personnes. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public n'est autorisée que si l'autorité répressive a réalisé une analyse d'impact sur les droits fondamentaux conformément à l'article 27 et a enregistré le système dans la base de données de l'UE prévue par l'article 49. Toutefois, dans des cas d'urgence dûment justifiés, il est possible de commencer à utiliser ces systèmes sans enregistrement dans la base de données de l'UE, à condition que cet enregistrement soit effectué sans retard injustifié.

3. Aux fins du paragraphe 1, premier alinéa, point h), et du paragraphe 2, chaque utilisation à des fins répressives d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public est subordonnée à une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante dont la décision est contraignante de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux règles détaillées du droit national visées au paragraphe 5. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser ce système sans autorisation à condition que cette autorisation soit demandée sans retard injustifié, au plus tard dans les 24 heures. Si cette autorisation est rejetée, il est mis fin à l'utilisation avec effet immédiat, et toutes les données, ainsi que les résultats et sorties de cette utilisation, sont immédiatement mis au rebut et supprimés.

L'autorité judiciaire compétente ou une autorité administrative indépendante dont la décision est contraignante n'accorde l'autorisation que si elle estime, sur la base d'éléments objectifs ou d'indications claires qui lui sont présentés, que l'utilisation du système d'identification biométrique à distance en temps réel concerné est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), tels qu'indiqués dans la demande et, en particulier, que cette utilisation reste limitée au strict nécessaire dans le temps et du point de vue de la portée géographique et personnelle. Lorsqu'elle statue sur la demande, cette autorité tient compte des éléments visés au paragraphe 2. Aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne peut être prise sur la seule base de la sortie du système d'identification biométrique à distance «en temps réel».

4. Sans préjudice du paragraphe 3, toute utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est notifiée à l'autorité de surveillance du marché concernée et à l'autorité nationale chargée de la protection des données, conformément aux règles nationales visées au paragraphe 5. Cette notification contient, au minimum, les informations visées au paragraphe 6 et n'inclut pas de données opérationnelles sensibles.

cf. CNIL

5. Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, dans les limites et les conditions énumérées au paragraphe 1, premier alinéa, point h), et aux paragraphes 2 et 3. Les États membres concernés établissent dans leur droit national les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations visées au paragraphe 3, ainsi qu'à la surveillance et à l'établissement de rap-

ports y afférents. Ces règles précisent également pour quels objectifs énumérés au paragraphe 1, premier alinéa, point h), et notamment pour quelles infractions pénales visées au point h), iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives. Les États membres notifient ces règles à la Commission au plus tard 30 jours après leur adoption. Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance.

6. Les autorités nationales de surveillance du marché et les autorités nationales chargées de la protection des données des États membres qui ont été notifiées de l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, conformément au paragraphe 4, soumettent à la Commission des rapports annuels sur cette utilisation. À cette fin, la Commission fournit aux États membres et aux autorités nationales en matière de surveillance du marché et de protection des données un modèle comprenant des informations sur le nombre de décisions prises par les autorités judiciaires compétentes ou par une autorité administrative indépendante dont la décision est contraignante en ce qui concerne les demandes d'autorisation conformément au paragraphe 3, ainsi que sur leur résultat.

cf. CNIL

cf. CNIL

7. La Commission publie des rapports annuels sur l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, fondés sur des données agrégées dans les États membres sur la base des rapports annuels visés au paragraphe 6. Ces rapports annuels n'incluent pas de données opérationnelles sensibles sur les activités répressives connexes.

8. Le présent article ne porte pas atteinte aux interdictions qui s'appliquent lorsqu'une pratique en matière d'IA enfreint d'autres dispositions du droit de l'Union.

CHAPITRE III
SYSTÈMES D'IA À HAUT RISQUE

Systèmes à haut risque

SECTION 1
Classification de systèmes d'IA comme systèmes à haut risque

article 6
Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque

1. Un système d'IA mis sur le marché ou mis en service, qu'il soit ou non indépendant des produits visés aux points a) et b), est considéré comme étant à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou le système d'IA constitue lui-même un tel produit;

b) le produit dont le composant de sécurité visé au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément à la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

2. Outre les systèmes d'IA à haut risque visés au paragraphe 1, les systèmes d'IA visés à l'annexe III sont considérés comme étant à haut risque.

3. Par dérogation au paragraphe 2, un système d'IA visé à l'annexe III n'est pas considéré comme étant à haut risque lorsqu'il ne présente pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision.

Le premier alinéa s'applique lorsqu'une des conditions suivantes est remplie:

a) le système d'IA est destiné à accomplir un tâche procédurale étroite;

b) le système d'IA est destiné à améliorer le résultat d'une activité humaine préalablement réalisée;

c) le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures et n'est pas destiné à se substituer à l'évaluation humaine préalablement réalisée, ni à influencer celle-ci, sans examen humain approprié; ou

d) le système d'IA est destiné à exécuter une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'utilisation visés à l'annexe III.

Nonobstant le premier alinéa, un système d'IA visé à l'annexe III est toujours considéré comme étant à haut risque lorsqu'il effectue un profilage de personnes physiques.

4. Un fournisseur qui considère qu'un système d'IA visé à l'annexe III n'est pas à haut risque documente son évaluation avant que ce système ne soit mis sur le marché ou mis en service. Ce fournisseur est soumis à l'obligation d'enregistrement visée à l'article 49, paragraphe 2. À la demande des autorités nationales compétentes, le fournisseur fournit la documentation de l'évaluation.

5. Après consultation du Comité européen de l'intelligence artificielle (ci-après dénommé « Comité IA»), et au plus tard le 2 février 2026, la Commission fournit des lignes directrices précisant la mise en œuvre pratique du présent article, conformément à l'article 96, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier le paragraphe 3, deuxième alinéa, du présent article en ajoutant de nouvelles conditions à celles qui y sont énoncées, ou en les modifiant, lorsqu'il existe des preuves concrètes et fiables de l'existence de systèmes d'IA qui relèvent du champ d'application de l'annexe III, mais qui ne présentent pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques.

7. La Commission adopte des actes délégués conformément à l'article 97 afin de modifier le paragraphe 3, deuxième alinéa, du présent article en supprimant l'une des conditions qui y est établie, lorsqu'il existe des preuves concrètes et fiables attestant que cela est nécessaire pour maintenir le niveau de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement.

8. Toute modification des conditions établies au paragraphe 3, deuxième alinéa, adoptée conformément aux paragraphe 6 et 7 du présent article ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement et veille à la cohérence avec les actes délégués adoptés conformément à l'article 7, paragraphe 1, et tient compte des évolutions du marché et des technologies.

article 7
Modifications de l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe III en y ajoutant des cas d'utilisation de systèmes d'IA à haut risque, ou en les modifiant, lorsque les deux conditions suivantes sont remplies:

a) les systèmes d'IA sont destinés à être utilisés dans l'un des domaines énumérés à l'annexe III;

b) les systèmes d'IA présentent un risque de préjudice pour la santé et la sécurité, ou un risque d'incidence négative sur les droits fondamentaux, et ce risque est équivalent ou supérieur au risque de préjudice ou d'incidence négative que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III.

2. Lorsqu'elle évalue les conditions visées au paragraphe 1, point b), la Commission tient compte des critères suivants:

a) la destination du système d'IA;

b) la mesure dans laquelle un système d'IA a été utilisé ou est susceptible de l'être;

c) la nature et la quantité des données traitées et utilisées par le système d'IA, en particulier le traitement ou l'absence de traitement des catégories particulières de données à caractère personnel;

d) la mesure dans laquelle le système d'IA agit de manière autonome et la mesure dans laquelle l'homme peut intervenir pour annuler une décision ou des recommandations susceptibles de causer un préjudice potentiel;

e) la mesure dans laquelle l'utilisation d'un système d'IA a déjà causé un préjudice à la santé et à la sécurité, a eu une incidence négative sur les droits fondamentaux ou a suscité de graves préoccupations quant à la probabilité de ce préjudice ou de cette incidence négative, tel que cela ressort, par exemple, des rapports ou allégations documentées soumis aux autorités nationales compétentes ou d'autres rapports, le cas échéant;

f) l'ampleur potentielle d'un tel préjudice ou d'une telle incidence négative, notamment en ce qui concerne son intensité et sa capacité d'affecter plusieurs personnes ou d'affecter un groupe particulier de personnes de manière disproportionnée;

g) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative dépendent des résultats obtenus au moyen d'un système d'IA, notamment parce qu'il n'est pas raisonnablement possible, pour des raisons pratiques ou juridiques, de s'affranchir de ces résultats;

h) la mesure dans laquelle il existe un déséquilibre de pouvoir, ou les personnes ayant potentiellement subi un préjudice ou une incidence négative se trouvent dans une situation vulnérable par rapport au déployeur d'un système d'IA, notamment en raison du statut, de l'autorité, de connaissances, de circonstances économiques ou sociales ou de l'âge;

cf. déployeurs

i) la mesure dans laquelle les résultats obtenus en utilisant un système d'IA sont facilement corrigibles ou réversibles, compte tenu des solutions techniques disponibles pour les corriger ou les inverser, les résultats qui ont une incidence négative sur la santé, la sécurité ou les droits fondamentaux ne devant pas être considérés comme facilement corrigibles ou réversibles;

j) la probabilité que le déploiement du système d'IA présente des avantages pour certaines personnes, certains groupes de personnes ou la société dans son ensemble et la portée de ces avantages, y compris les améliorations éventuelles quant à la sécurité des produits;

k) la mesure dans laquelle le droit existant de l'Union prévoit:

   i) des mesures de réparation efficaces en ce qui concerne les risques posés par un système d'IA, à l'exclusion des réclamations en dommages-intérêts;

   ii) des mesures efficaces destinées à prévenir ou à réduire substantiellement ces risques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier la liste figurant à l'annexe III en supprimant des systèmes d'IA à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA à haut risque concerné ne présente plus de risques substantiels pour les droits fondamentaux, la santé ou la sécurité, compte tenu des critères énumérés au paragraphe 2;

b) la suppression ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux en vertu du droit de l'Union.

SECTION 2
Exigences applicables aux systèmes d'IA à haut risque

article 8
Respect des exigences

1. Les systèmes d'IA à haut risque respectent les exigences énoncées dans la présente section, en tenant compte de leur destination ainsi que de l'état de la technique généralement reconnu en matière d'IA et de technologies liées à l'IA. Pour garantir le respect de ces exigences, il est tenu compte du système de gestion des risques prévu à l'article 9.

2. Lorsqu'un produit contient un système d'IA auquel s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, les fournisseurs sont chargés de veiller à ce que leur produit soit pleinement conforme à toutes les exigences en vertu de la législation d'harmonisation de l'Union applicable. Pour garantir que les systèmes d'IA à haut risque visés au paragraphe 1 sont conformes aux exigences énoncées dans la présente section, et afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les processus d'essai et de déclaration nécessaires, les informations et la documentation qu'ils fournissent concernant leur produit dans la documentation et les procédures qui existent déjà et qui sont requises en vertu de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I.

article 9
Système de gestion des risques

1. Un système de gestion des risques est établi, mis en œuvre, documenté et tenu à jour en ce qui concerne les systèmes d'IA à haut risque.

2. Ce système de gestion des risques s'entend comme étant un processus itératif continu qui est planifié et se déroule sur l'ensemble du cycle de vie d'un système d'IA à haut risque et qui doit périodiquement faire l'objet d'un examen et d'une mise à jour méthodiques. Il comprend les étapes suivantes:

a) l'identification et l'analyse des risques connus et raisonnablement prévisibles que le système d'IA à haut risque peut poser pour la santé, la sécurité ou les droits fondamentaux lorsque le système d'IA à haut risque est utilisé conformément à sa destination;

b) l'estimation et l'évaluation des risques susceptibles d'apparaître lorsque le système d'IA à haut risque est utilisé conformément à sa destination et dans des conditions de mauvaise utilisation raisonnablement prévisible;

c) l'évaluation d'autres risques susceptibles d'apparaître, sur la base de l'analyse des données recueillies au moyen du système de surveillance après commercialisation visé à l'article 72;

d) l'adoption de mesures appropriées et ciblées de gestion des risques, conçues pour répondre aux risques identifiés en vertu du point a).

3. Les risques visés au présent article ne concernent que ceux qui peuvent être raisonnablement atténués ou éliminés dans le cadre du développement ou de la conception du système d'IA à haut risque, ou par la fourniture d'informations techniques appropriées.

4. Les mesures de gestion des risques visées au paragraphe 2, point d), tiennent dûment compte des effets et de l'interaction possibles résultant de l'application combinée des exigences énoncées dans la présente section, en vue de prévenir les risques plus efficacement tout en parvenant à un bon équilibre dans le cadre de la mise en œuvre des mesures visant à répondre à ces exigences.

5. Les mesures de gestion des risques visées au paragraphe 2, point d), sont telles que le risque résiduel pertinent associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables.

Pour déterminer les mesures de gestion des risques les plus adaptées, il convient de veiller à:

a) éliminer ou réduire les risques identifiés et évalués conformément au paragraphe 2 autant que la technologie le permet grâce à une conception et à un développement appropriés du système d'IA à haut risque;

b) mettre en œuvre, le cas échéant, des mesures adéquates d'atténuation et de contrôle répondant aux risques impossibles à éliminer;

c) fournir aux déployeurs les informations requises conformément à l'article 13 et, éventuellement, une formation.

cf. déployeurs

En vue de l'élimination ou de la réduction des risques liés à l'utilisation du système d'IA à haut risque, il est dûment tenu compte des connaissances techniques, de l'expérience, de l'éducation et de la formation pouvant être attendues du déployeur, ainsi que du contexte prévisible dans lequel le système est destiné à être utilisé.

cf. déployeurs

6. Les systèmes d'IA à haut risque sont soumis à des essais afin de déterminer les mesures de gestion des risques les plus appropriées et les plus ciblées. Les essais garantissent que les systèmes d'IA à haut risque fonctionnent de manière conforme à leur destination et qu'ils sont conformes aux exigences énoncées dans la présente section.

7. Les procédures d'essai peuvent comprendre des essais en conditions réelles conformément à l'article 60.

8. Les tests des systèmes d'IA à haut risque sont effectués, selon les besoins, à tout moment pendant le processus de développement et, en tout état de cause, avant leur mise sur le marché ou leur mise en service. Les tests sont effectués sur la base d'indicateurs et de seuils probabilistes préalablement définis, qui sont adaptés à la destination du système d'IA à haut risque.

9. Lors de la mise en œuvre du système de gestion des risques prévu aux paragraphes 1 à 7, les fournisseurs prennent en considération la probabilité que, compte tenu de sa destination, le système d'IA à haut risque puisse avoir une incidence négative sur des personnes âgées de moins de 18 ans et, le cas échéant, sur d'autres groupes vulnérables.

10. En ce qui concerne les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des exigences concernant les processus internes de gestion des risques en vertu d'autres dispositions pertinentes du droit de l'Union, les aspects présentés aux paragraphes 1 à 9 peuvent faire partie des procédures de gestion des risques établies conformément à ladite législation, ou être combinées à celles-ci.

article 10
Données et gouvernance des données

1. Les systèmes d'IA à haut risque faisant appel à des techniques qui impliquent l'entraînement de modèles d'IA au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité visés aux paragraphes 2 à 5 chaque fois que ces jeux de données sont utilisés.

2. Les jeux de données d'entraînement, de validation et de test sont soumis à des pratiques en matière de gouvernance et de gestion des données appropriées à la destination du systèmes d'IA à haut risque. Ces pratiques concernent en particulier:

a) les choix de conception pertinents;

b) les processus de collecte de données et l'origine des données, ainsi que, dans le cas des données à caractère personnel, la finalité initiale de la collecte de données;

c) les opérations de traitement pertinentes pour la préparation des données, telles que l'annotation, l'étiquetage, le nettoyage, la mise à jour, l'enrichissement et l'agrégation;

d) la formulation d'hypothèses, notamment en ce qui concerne les informations que les données sont censées mesurer et représenter;

e) une évaluation de la disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires;

f) un examen permettant de repérer d'éventuels biais qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées pour les opérations futures;

g) les mesures appropriées visant à détecter, prévenir et atténuer les éventuels biais repérés conformément au point f);

h) la détection de lacunes ou déficiences pertinentes dans les données qui empêchent l'application du présent règlement, et la manière dont ces lacunes ou déficiences peuvent être comblées.

3. Les jeux de données d'entraînement, de validation et de test sont pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination. Ils possèdent les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des jeux de données peuvent être remplies au niveau des jeux de données pris individuellement ou d'une combinaison de ceux-ci.

4. Les jeux de données tiennent compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé.

5. Dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, conformément au paragraphe 2, points f) et g), du présent article, les fournisseurs de ces systèmes peuvent exceptionnellement traiter des catégories particulières de données à caractère personnel, sous réserve de garanties appropriées pour les droits et libertés fondamentaux des personnes physiques. Outre les dispositions des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680, toutes les conditions suivantes doivent être réunies pour que ce traitement puisse avoir lieu:

cf. RGPD

a) la détection et la correction des biais ne peuvent être satisfaites de manière efficace en traitant d'autres données, y compris des données synthétiques ou anonymisées;

b) les catégories particulières de données à caractère personnel sont soumises à des limitations techniques relatives à la réutilisation des données à caractère personnel, ainsi qu'aux mesures les plus avancées en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation;

c) les catégories particulières de données à caractère personnel font l'objet de mesures visant à garantir que les données à caractère personnel traitées sont sécurisées, protégées et soumises à des garanties appropriées, y compris des contrôles stricts et une documentation de l'accès, afin d'éviter toute mauvaise utilisation et de veiller à ce que seules les personnes autorisées ayant des obligations de confidentialité appropriées aient accès à ces données à caractère personnel;

d) les catégories particulières de données à caractère personnel ne doivent pas être transmises, transférées ou consultées d'une autre manière par d'autres parties;

e) les catégories particulières de données à caractère personnel sont supprimées une fois que le biais a été corrigé ou que la période de conservation des données à caractère personnel a expiré, selon celle de ces deux échéances qui arrive en premier;

f) les registres des activités de traitement visés dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680 comprennent les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel était strictement nécessaire pour détecter et corriger les biais, ainsi que la raison pour laquelle cet objectif n'a pas pu être atteint par le traitement d'autres données.

cf. RGPD

6. En ce qui concerne le développement de systèmes d'IA à haut risque qui ne font pas appel à des techniques qui impliquent l'entraînement de modèles d'IA, les paragraphes 2 à 5 s'appliquent uniquement aux jeux de données de test.

article 11
Documentation technique

1. La documentation technique relative à un système d'IA à haut risque est établie avant que ce système ne soit mis sur le marché ou mis en service et est tenue à jour.

La documentation technique est établie de manière à démontrer que le système d'IA à haut risque satisfait aux exigences énoncées dans la présente section et à fournir aux

autorités nationales compétentes et aux organismes notifiés les informations nécessaires sous une forme claire et intelligible pour évaluer la conformité du système d'IA avec ces exigences. Elle contient, au minimum, les éléments énoncés à l'annexe IV. Les PME, y compris les jeunes pousses, peuvent fournir des éléments de la documentation technique spécifiée à l'annexe IV d'une manière simplifiée. À cette fin, la Commission établit un formulaire de documentation technique simplifié ciblant les besoins des petites entreprises et des microentreprises. Lorsqu'une PME, y compris une jeune pousse, choisit de fournir les informations requises à l'annexe IV de manière simplifiée, elle utilise le formulaire visé au présent paragraphe. Les organismes notifiés acceptent le formulaire aux fins de l'évaluation de la conformité.

2. Lorsqu'un système d'IA à haut risque lié à un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I est mis sur le marché ou mis en service, un seul ensemble de documentation technique est établi, contenant toutes les informations visées au paragraphe 1, ainsi que les informations requises en vertu de ces actes juridiques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe IV, lorsque cela est nécessaire, afin de garantir que, compte tenu du progrès technique, la documentation technique fournit toutes les informations requises pour évaluer la conformité du système avec les exigences énoncées dans la présente section.

article 12
Enregistrement

1. Les systèmes d'IA à haut risque permettent, techniquement, l'enregistrement automatique des événements (journaux) tout au long de la durée de vie du système.

2. Afin de garantir un degré de traçabilité du fonctionnement d'un système d'IA qui soit adapté à la destination du système, les fonctionnalités de journalisation permettent l'enregistrement des événements pertinents pour:

a) repérer les situations susceptibles d'avoir pour effet que le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, ou d'entraîner une modification substantielle;

b) faciliter la surveillance après commercialisation visée à l'article 72; et

c) surveiller le fonctionnement du système d'IA à haut risque comme prévu à l'article 26, paragraphe 5.

3. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les fonctionnalités de journalisation fournissent, au minimum:

a) l'enregistrement de la période de chaque utilisation du système (date et heure de début et de fin pour chaque utilisation);

b) la base de données de référence utilisée par le système pour vérifier les données d'entrée;

c) les données d'entrée pour lesquelles la recherche a abouti à une correspondance;

d) l'identification des personnes physiques participant à la vérification des résultats, visées à l'article 14, paragraphe 5.

article 13
Transparence et fourniture d'informations aux déployeurs

1. La conception et le développement des systèmes d'IA à haut risque sont tels que le fonctionnement de ces systèmes est suffisamment transparent pour permettre aux déployeurs d'interpréter les sorties d'un système et de les utiliser de manière appropriée. Un type et un niveau adéquats de transparence sont garantis afin de veiller au respect des obligations pertinentes incombant au fournisseur et au déployeur énoncées à la section 3.

cf. déployeurs

2. Les systèmes d'IA à haut risque sont accompagnés d'une notice d'utilisation dans un format numérique approprié ou autre, contenant des informations concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les déployeurs.

cf. déployeurs

3. La notice d'utilisation contient au moins les informations suivantes:

a) l'identité et les coordonnées du fournisseur et, le cas échéant, de son mandataire;

b) les caractéristiques, les capacités et les limites de performance du système d'IA à haut risque, notamment:

i) sa destination;

ii) le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité visé à l'article 15 qui a servi de référence pour les tests et la validation du système d'IA à haut risque et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité;

iii) toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé et la sécurité ou pour les droits fondamentaux visés à l'article 9, paragraphe 2;

iv) le cas échéant, les capacités et caractéristiques techniques du système d'IA à haut risque à fournir des informations pertinentes pour expliquer ses sorties;

v) le cas échéant, sa performance en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé;

vi) le cas échéant, les spécifications relatives aux données d'entrée, ou toute autre information pertinente concernant les jeux de données d'entraînement, de validation et de test utilisés, compte tenu de la destination du système d'IA à haut risque;

vii) le cas échéant, les informations permettant aux déployeurs d'interpréter les sorties du système d'IA à haut risque et de les utiliser de manière appropriée;

cf. déployeurs

c) les modifications du système d'IA à haut risque et de sa performance qui ont été prédéterminées par le fournisseur au moment de l'évaluation initiale de la conformité, le cas échéant;

d) les mesures de contrôle humain visées à l'article 14, notamment les mesures techniques mises en place pour faciliter l'interprétation des sorties des systèmes d'IA à haut risque par les déployeurs;

cf. déployeurs

e) les ressources informatiques et matérielles nécessaires, la durée de vie attendue du système d'IA à haut risque et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement de ce système d'IA, notamment en ce qui concerne les mises à jour logicielles;

f) le cas échéant, une description des mécanismes compris dans le système d'IA à haut risque qui permet aux déployeurs de collecter, stocker et interpréter correctement les journaux, conformément à l'article 12.

cf. déployeurs

article 14
Contrôle humain

1. La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant leur période d'utilisation.

2. Le contrôle humain vise à prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître lorsqu'un système d'IA à haut risque est utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, en particulier lorsque de tels risques persistent malgré l'application d'autres exigences énoncées dans la présente section.

3. Les mesures de contrôle sont proportionnées aux risques, au niveau d'autonomie et au contexte d'utilisation du système d'IA à haut risque, et sont assurées au moyen d'un ou des deux types de mesures suivants:

a) des mesures identifiées et, lorsque cela est techniquement possible, intégrées par le fournisseur dans le système d'IA à haut risque avant la mise sur le marché ou la mise en service de ce dernier;

b) des mesures identifiées par le fournisseur avant la mise sur le marché ou la mise en service du système d'IA à haut risque et qui se prêtent à une mise en œuvre par le déployeur.

cf. déployeurs

4. Aux fins de la mise en œuvre des dispositions des paragraphes 1, 2 et 3, le système d'IA à haut risque est fourni au déployeur de telle manière que les personnes physiques chargées d'effectuer un contrôle humain, dans la mesure où cela est approprié et proportionné, ont la possibilité:

a) de comprendre correctement les capacités et les limites pertinentes du système d'IA à haut risque et d'être en mesure de surveiller correctement son fonctionnement, y compris en vue de détecter et de traiter les anomalies, les dysfonctionnements et les performances inattendues;

b) d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux sorties produites par un système d'IA à haut risque (biais d'automatisation), en particulier pour les systèmes d'IA à haut risque utilisés pour fournir des informations ou des recommandations concernant les décisions à prendre par des personnes physiques;

c) d'interpréter correctement les sorties du système d'IA à haut risque, compte tenu par exemple des outils et méthodes d'interprétation disponibles;

d) de décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque ou d'ignorer, remplacer ou inverser la sortie du système d'IA à haut risque;

e) d'intervenir dans le fonctionnement du système d'IA à haut risque ou d'interrompre le système au moyen d'un bouton d'arrêt ou d'une procédure similaire permettant au système de s'arrêter de manière sécurisée.

5. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les mesures prévues au paragraphe 3 du présent article sont de nature à garantir que, en outre, aucune mesure ou décision n'est prise par le déployeur sur la base de l'identification résultant du système sans vérification et confirmation distinctes de cette identification par au moins deux personnes physiques disposant des compétences, de la formation et de l'autorité nécessaires.

cf. déployeurs

L'exigence d'une vérification distincte par au moins deux personnes physiques ne s'applique pas aux systèmes d'IA à haut risque utilisés à des fins répressives ou dans les domaines de la migration, des contrôles aux frontières ou de l'asile, lorsque le droit de l'Union ou le droit national considère que l'application de cette exigence est disproportionnée.

article 15
Exactitude, robustesse et cybersécurité

1. La conception et le développement des systèmes d'IA à haut risque sont tels qu'ils leur permettent d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie.

2. Pour examiner les aspects techniques de la manière de mesurer les niveaux appropriés d'exactitude et de robustesse visés au paragraphe 1 et tout autre indicateur de performance pertinent, la Commission, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, encourage, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure.

3. Les niveaux d'exactitude et les indicateurs de l'exactitude des systèmes d'IA à haut risque sont indiqués dans la notice d'utilisation jointe.

4. Les systèmes d'IA à haut risque font preuve d'autant de résilience que possible en cas d'erreurs, de défaillances ou d'incohérences pouvant survenir au sein des systèmes eux-mêmes ou de l'environnement dans lequel ils fonctionnent, notamment en raison

de leur interaction avec des personnes physiques ou d'autres systèmes. Des mesures techniques et organisationnelles sont prises à cet égard.

Des solutions techniques redondantes, telles que des plans de sauvegarde ou des mesures de sécurité après défaillance, peuvent permettre de garantir la robustesse des systèmes d'IA à haut risque.

Les systèmes d'IA à haut risque qui continuent leur apprentissage après leur mise sur le marché ou leur mise en service sont développés de manière à éliminer ou à réduire dans la mesure du possible le risque que des sorties éventuellement biaisées n'influencent les entrées pour les opérations futures (boucles de rétroaction) et à veiller à ce que ces boucles de rétroaction fassent l'objet d'un traitement adéquat au moyen de mesures d'atténuation appropriées.

5. Les systèmes d'IA à haut risque résistent aux tentatives de tiers non autorisés visant à modifier leur utilisation, leurs sorties ou leur performance en exploitant les vulnérabilités du système.

Les solutions techniques visant à garantir la cybersécurité des systèmes d'IA à haut risque sont adaptées aux circonstances pertinentes et aux risques.

Les solutions techniques destinées à remédier aux vulnérabilités spécifiques à l'IA comprennent, au besoin, des mesures ayant pour but de prévenir, de détecter, de contrer, de résoudre et de maîtriser les attaques visant à manipuler le jeu de données d'entraînement (empoisonnement des données) ou les composants préentraînés utilisés en entraînement (empoisonnement de modèle), les entrées destinées à induire le modèle d'IA en erreur (exemples contradictoires ou invasion de modèle), les attaques visant la confidentialité ou les défauts du modèle.

SECTION 3
Obligations incombant aux fournisseurs et aux déployeurs de systèmes d'IA à haut risque et à d'autres parties

article 16
Obligations incombant aux fournisseurs de systèmes d'IA à haut risque

Les fournisseurs de systèmes d'IA à haut risque:

a) veillent à ce que leurs systèmes d'IA à haut risque soient conformes aux exigences énoncées à la section 2;

b) indiquent sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, leur nom, raison sociale ou marque déposée, l'adresse à laquelle ils peuvent être contactés;

c) mettent en place un système de gestion de la qualité conforme à l'article 17;

d) assurent la conservation de la documentation visée à l'article 18;

e) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, lorsque ces journaux se trouvent sous leur contrôle, conformément à l'article 19;

f) veillent à ce que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité applicable visée à l'article 43, avant sa mise sur le marché ou sa mise en service;

g) élaborent une déclaration UE de conformité conformément à l'article 47;

h) apposent le marquage CE sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, afin d'indiquer la conformité avec le présent règlement, conformément à l'article 48;

i) respectent les obligations en matière d'enregistrement prévues à l'article 49, paragraphe 1;

j) prennent les mesures correctives nécessaires et fournissent les informations requises à l'article 20;

k) à la demande motivée d'une ««autorité nationale compétente, prouvent la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2;

l) veillent à ce que le système d'IA à haut risque soit conforme aux exigences en matière d'accessibilité conformément aux directives (UE) 2016/2102 et (UE) 2019/882.

article 17
Système de gestion de la qualité

1. Les fournisseurs de systèmes d'IA à haut risque mettent en place un système de gestion de la qualité garantissant le respect du présent règlement. Ce système est documenté de manière méthodique et ordonnée sous la forme de politiques, de procédures et d'instructions écrites, et comprend au moins les aspects suivants:

a) une stratégie de respect de la réglementation, notamment le respect des procédures d'évaluation de la conformité et des procédures de gestion des modifications apportées aux systèmes d'IA à haut risque;

b) des techniques, procédures et actions systématiques destinées à la conception des systèmes d'IA à haut risque ainsi qu'au contrôle et à la vérification de cette conception;

c) des techniques, procédures et actions systématiques destinées au développement des systèmes d'IA à haut risque ainsi qu'au contrôle et à l'assurance de leur qualité;

d) des procédures d'examen, de test et de validation à exécuter avant, pendant et après le développement du système d'IA à haut risque, ainsi que la fréquence à laquelle elles doivent être réalisées;

e) des spécifications techniques, notamment des normes, à appliquer et, lorsque les normes harmonisées pertinentes ne sont pas appliquées intégralement, ou ne couvrent pas toutes les exigences pertinentes énoncées à la section 2, les moyens à utiliser pour faire en sorte que le système d'IA à haut risque satisfasse auxdites exigences;

f) les systèmes et procédures de gestion des données, notamment l'acquisition, la collecte, l'analyse, l'étiquetage, le stockage, la filtration, l'exploration, l'agrégation, la conservation des données et toute autre opération concernant les données qui est effectuée avant la mise sur le marché ou la mise en service de systèmes d'IA à haut risque et aux fins de celles-ci;

g) le système de gestion des risques prévu à l'article 9;

h) l'élaboration, la mise en œuvre et le fonctionnement d'un système de surveillance après commercialisation conformément à l'article 72;

i) les procédures relatives au signalement d'un incident grave conformément à l'article 73;

j) la gestion des communications avec les autorités nationales compétentes, les autres autorités compétentes, y compris celles fournissant ou facilitant l'accès aux données, les organismes notifiés, les autres opérateurs, les clients ou d'autres parties intéressées;

k) les systèmes et procédures de conservation de tous les documents et informations pertinents;

l) la gestion des ressources, y compris les mesures liées à la sécurité d'approvisionnement;

m) un cadre de responsabilisation définissant les responsabilités de l'encadrement et des autres membres du personnel en ce qui concerne tous les aspects énumérés dans le présent paragraphe.

2. La mise en œuvre des aspects visés au paragraphe 1 est proportionnée à la taille de l'organisation du fournisseur. Les fournisseurs respectent, en tout état de cause, le degré de rigueur et le niveau de protection requis afin de garantir que leurs systèmes d'IA à haut risque sont conformes au présent règlement.

3. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations relatives aux systèmes de gestion de la qualité, ou liées à l'exercice d'une fonction équivalente en vertu de la législation sectorielle pertinente de l'Union peuvent inclure

les aspects énumérés au paragraphe 1 dans les systèmes de gestion de la qualité conformément à ladite législation.

4. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues dans la législation pertinente de l'Union sur les services financiers vaut respect de l'obligation de mettre en place un système de gestion de la qualité, à l'exception du paragraphe 1, points g), h) et i) du présent article. À cette fin, toute norme harmonisée visée à l'article 40 est prise en considération.

article 18
Conservation des documents

1. Pendant une période prenant fin 10 ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, le fournisseur tient à la disposition des autorités nationales compétentes:

a) la documentation technique visée à l'article 11;

b) la documentation concernant le système de gestion de la qualité visé à l'article 17;

c) la documentation concernant les modifications approuvées par les organismes notifiés, le cas échéant;

d) les décisions et autres documents émis par les organismes notifiés, le cas échéant;

e) la déclaration UE de conformité visée à l'article 47.

2. Chaque État membre détermine les conditions dans lesquelles la documentation visée au paragraphe 1 reste à la disposition des autorités nationales compétentes pendant la période indiquée audit paragraphe dans le cas où un fournisseur ou son mandataire établi sur son territoire fait faillite ou met un terme à ses activités avant la fin de cette période.

3. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour la documentation technique dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

article 19
Journaux générés automatiquement

1. Les fournisseurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous leur contrôle. Sans préjudice du droit de l'Union ou du droit national applicable, les journaux sont conservés pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

2. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux générés automatiquement par leurs systèmes d'IA à haut risque dans le cadre de la documentation conservée en vertu de la législation pertinente sur les services financiers.

article 20
Mesures corrective et devoir d'information

1. Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité, le retirer, le désactiver ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque

concerné et, le cas échéant, les déployeurs, le mandataire et les importateurs en conséquence.

cf. déployeurs

2. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, et que le fournisseur prend conscience de ce risque, celui-ci recherche immédiatement les causes, en collaboration avec le déployeur à l'origine du signalement, le cas échéant, et informe les autorités de surveillance du marché compétentes pour le système d'IA à haut risque concerné et, le cas échéant, l'organisme notifié qui a délivré un certificat pour ce système d'IA à haut risque, conformément à l'article 44, en précisant en particulier la nature du cas de non-conformité et les éventuelles mesures correctives pertinentes prises.

cf. déployeurs

article 21
Coopération avec les autorités compétentes

1. À la demande motivée d'une autorité compétente, les fournisseurs de systèmes d'IA à haut risque fournissent à ladite autorité toutes les informations et tous les documents nécessaires pour démontrer la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par l'autorité dans l'une des langues officielles des institutions de l'Union, telle qu'indiquée par l'État membre concerné.

2. À la demande motivée d'une autorité compétente, les fournisseurs accordent également à l'autorité compétente à l'origine de la demande, le cas échéant, l'accès aux journaux générés automatiquement par le système d'IA à haut risque visés à l'article 12, paragraphe 1, dans la mesure où ces journaux sont sous leur contrôle.

3. Les informations obtenues par une autorité compétente en application du présent article sont traitées conformément aux obligations de confidentialité énoncées à l'article 78.

article 22
Mandataires des fournisseurs de systèmes d'IA à haut risque

1. Avant de mettre leurs systèmes d'IA à haut risque à disposition sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.

3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat aux autorités de surveillance du marché à leur demande, dans l'une des langues officielles des institutions de l'Union, indiquée par l'autorité compétente. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:

a) vérifier que la déclaration UE de conformité visée à l'article 47 et la documentation technique visée à l'article 11 ont été établies et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité;

b) tenir à la disposition des autorités compétentes et des autorités ou organismes nationaux visés à l'article 74, paragraphe 10, pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les coordonnées du fournisseur ayant désigné le mandataire, une copie de la déclaration UE de conformité visée à l'article 47, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié;

c) à la demande motivée d'une autorité compétente, communiquer à cette dernière toutes les informations et tous les documents, y compris ceux visés au point b) du présent alinéa, nécessaires pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, et notamment lui donner accès aux journaux générés automatiquement par le système d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous le contrôle du fournisseur;

d) à la demande motivée des autorités compétentes, coopérer avec elles à toute mesure prise par ces dernières à l'égard du système d'IA à haut risque, en particulier pour réduire et atténuer les risques posés par le système d'IA à haut risque;

e) le cas échéant, respecter les obligations en matière d'enregistrement visées à l'article 49, paragraphe 1, ou, si l'enregistrement est effectué par le fournisseur lui-même, vérifier que les informations visées à l'annexe VIII, section A, point 3, sont correctes.

Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

4. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe immédiatement l'autorité de surveillance du marché concernée et, selon le cas, l'organisme notifié pertinent de la cessation du mandat et des motifs qui la sous-tendent.

article 23
Obligations des importateurs

1. Avant de mettre sur le marché un système d'IA à haut risque, les importateurs s'assurent que le système est conforme au présent règlement en vérifiant que:

a) le fournisseur du système d'IA à haut risque a suivi la procédure pertinente d'évaluation de la conformité visée à l'article 43;

b) le fournisseur a établi la documentation technique conformément à l'article 11 et à l'annexe IV;

c) le système porte le marquage CE requis et est accompagné de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation;

d) le fournisseur a désigné un mandataire conformément à l'article 22, paragraphe 1.

2. Lorsqu'un importateur a des raisons suffisantes de considérer qu'un système d'IA à haut risque n'est pas conforme au présent règlement, ou a été falsifié ou s'accompagne de documents falsifiés, il ne met le système sur le marché qu'après sa mise en conformité. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, l'importateur en informe le fournisseur du système, les mandataires et les autorités de surveillance du marché.

3. Les importateurs indiquent leur nom, raison sociale ou marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés, sur le système d'IA à haut risque et sur son emballage ou dans la documentation l'accompagnant, selon le cas.

4. Les importateurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.

5. Pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les importateurs conservent une copie du certificat délivré par l'organisme notifié, selon le cas, de la notice d'utilisation et de la déclaration UE de conformité visée à l'article 47.

6. À la demande motivée des autorités compétentes concernées, les importateurs communiquent à ces dernières toutes les informations et tous les documents nécessaires, y compris ceux visés au paragraphe 5, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par les autorités nationales compétentes. À cette fin, ils veillent également à ce que la documentation technique puisse être mise à la disposition de ces autorités.

7. Les importateurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis sur le marché par les importateurs, en particulier pour réduire et atténuer les risques qu'il présente.

article 24
Obligations des distributeurs

1. Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs vérifient qu'il porte le marquage CE requis, qu'il est accompagné d'une copie de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation, et que le fournisseur et l'importateur dudit système, selon le cas, ont respecté leurs obligations respectives en vertu de l'article 16, points b) et c), et de l'article 23, paragraphe 3.

2. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque n'est pas conforme aux exigences énoncées à la section 2, il ne met le système à disposition sur le marché qu'après la mise en conformité de celui-ci avec lesdites exigences. De plus, lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe le fournisseur ou l'importateur du système, selon le cas.

3. Les distributeurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.

4. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque qu'il a mis à disposition sur le marché n'est pas conforme aux exigences énoncées à la section 2, il prend les mesures correctives nécessaires pour mettre ce système en conformité avec lesdites exigences, le retirer ou le rappeler ou veille à ce que le fournisseur, l'importateur ou tout opérateur concerné, selon le cas, prenne ces mesures correctives. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe immédiatement le fournisseur ou l'importateur du système ainsi que les autorités compétentes pour le système d'IA à haut risque concerné et précise, notamment, le cas de non-conformité et les éventuelles mesures correctives prises.

5. À la demande motivée d'une autorité compétente concernée, les distributeurs d'un système d'IA à haut risque communiquent à cette autorité toutes les informations et tous les documents concernant les mesures qu'ils ont prises en vertu des paragraphes 1 à 4, nécessaires pour démontrer la conformité de ce système avec les exigences énoncées à la section 2.

6. Les distributeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis à disposition sur le marché par les distributeurs, en particulier pour réduire et atténuer les risques qu'il présente.

article 25
Responsabilités tout au long de la chaîne de valeur de l'IA

cf. déployeurs

1. Tout distributeur, importateur, déployeur ou autre tiers est considéré comme un fournisseur d'un système d'IA à haut risque aux fins du présent règlement et est soumis aux obligations incombant au fournisseur au titre de l'article 16 dans toutes les circonstances suivantes:

a) il commercialise sous son propre nom ou sa propre marque un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles prévoyant une autre répartition des obligations;

b) il apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service de telle manière qu'il reste un système d'IA à haut risque en application de l'article 6;

c) il modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé à haut risque et a déjà été mis sur le marché ou mis en service de telle manière que le système d'IA concerné devient un système d'IA à haut risque conformément l'article 6.

2. Lorsque les circonstances visées au paragraphe 1, se produisent, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA n'est plus considéré comme un fournisseur de ce système d'IA spécifique aux fins du présent règlement. Ce fournisseur initial coopère étroitement avec les nouveaux fournisseurs et met à dis-

position les informations nécessaires et fournit l'accès technique raisonnablement attendu et toute autre assistance nécessaire au respect des obligations énoncées dans le présent règlement, en particulier en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque. Le présent paragraphe ne s'applique pas dans les cas où le fournisseur initial a clairement précisé que son système d'IA ne doit pas être transformé en un système d'IA à haut risque et ne relève donc pas de l'obligation relative à la remise de la documentation.

3. Lorsque des systèmes d'IA à haut risque constituent des composants de sécurité de produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fabricant de ces produits est considéré comme étant le fournisseur du système d'IA à haut risque et est soumis aux obligations visées à l'article 16 dans l'un des deux cas suivants:

a) le système d'IA à haut risque est mis sur le marché avec le produit sous le nom ou la marque du fabricant du produit;

b) le système d'IA à haut risque est mis en service sous le nom ou la marque du fabricant du produit après que le produit a été mis sur le marché.

4. Le fournisseur d'un système d'IA à haut risque et le tiers qui fournit un système d'IA, des outils, services, composants ou processus qui sont utilisés ou intégrés dans un système d'IA à haut risque précisent, par accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaire, sur la base de l'état de la technique généralement reconnu, pour permettre au fournisseur du système d'IA à haut risque de se conformer pleinement aux obligations prévues dans le présent règlement. Le présent paragraphe ne s'applique pas aux tiers qui rendent accessibles au public des outils, services, processus ou composants, autres que des modèles d'IA à usage général, dans le cadre d'une licence libre et ouverte.

Le Bureau de l'IA peut élaborer et recommander des clauses types volontaires pour les contrats entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque. Lorsqu'il élabore des clauses types volontaires, le Bureau de l'IA tient compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques. Les clauses types volontaires sont publiées et mises à disposition gratuitement dans un format électronique facile d'utilisation.

5. Les paragraphes 2 et 3 sont sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle, les informations confidentielles de nature commerciale et les secrets d'affaires conformément au droit de l'Union et au droit national.

article 26
Obligations incombant aux déployeurs de systèmes d'IA à haut risque

1. Les déployeurs de systèmes d'IA à haut risque prennent des mesures techniques et organisationnelles appropriées afin de garantir qu'ils utilisent ces systèmes conformément aux notices d'utilisation accompagnant les systèmes, conformément aux paragraphes 3 et 6.

cf. déployeurs

2. Les déployeurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire.

cf. déployeurs

3. Les obligations énoncées aux paragraphes 1 et 2 sont sans préjudice des autres obligations du déployeur prévues par le droit de l'Union ou le droit national et de la faculté du déployeur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de contrôle humain indiquées par le fournisseur.

cf. déployeurs

4. Sans préjudice des paragraphes 1 et 2, pour autant que le déployeur exerce un contrôle sur les données d'entrée, il veille à ce que ces dernières soient pertinentes et suffisamment représentatives au regard de la destination du système d'IA à haut risque.

cf. déployeurs

5. Les déployeurs surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation et, le cas échéant, informent les fournisseurs conformément à l'article 72. Lorsque les déployeurs ont des raisons de considérer que l'utilisation du système d'IA à haut risque conformément à la notice d'utilisation pourrait conduire à ce que le système d'IA présente un risque au sens de l'article 79, paragraphe 1, ils en informent, sans retard injustifié, le fournisseur ou le distributeur ainsi que l'autorité de surveillance du marché concernée, et suspendent l'utilisation de ce système. Lorsque les déployeurs ont détecté un incident grave, ils informent également immédiatement d'abord le fournisseur, puis l'importateur ou le distributeur et les autorités de surveillance du marché concernées de cet incident. Si le déployeur n'est pas en mesure de joindre le fournisseur, l'article 73 s'applique mutatis mutandis. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs de systèmes d'IA qui sont des autorités répressives.

cf. déployeurs

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à la gouvernance, aux dispositifs, aux processus et aux mécanismes internes prévues dans la législation sur les services financiers vaut respect de l'obligation de surveillance énoncée au premier alinéa.

cf. déployeurs

6. Les déployeurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque dans la mesure où ces journaux se trouvent sous leur contrôle, pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

cf. déployeurs

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

cf. déployeurs

7. Avant de mettre en service ou d'utiliser un système d'IA à haut risque sur le lieu de travail, les déployeurs qui sont des employeurs informent les représentants des travailleurs et les travailleurs concernés qu'ils seront soumis à l'utilisation du système d'IA à haut risque. Ces informations sont fournies, le cas échéant, conformément aux règles et procédures prévues par le droit de l'Union et le droit national et aux pratiques en matière d'information des travailleurs et de leurs représentants.

cf. déployeurs

8. Les déployeurs de systèmes d'IA à haut risque qui sont des autorités publiques ou des institutions, organes ou organismes de l'Union, respectent les obligations en matière d'enregistrement prévues à l'article 49. Dans le cas où ces déployeurs constatent que le système d'IA à haut risque qu'ils envisagent d'utiliser n'a pas été enregistré dans la base de données de l'UE visée à l'article 71, ils n'utilisent pas ce système et informent le fournisseur ou le distributeur.

cf. déployeurs

9. Le cas échéant, les déployeurs de systèmes d'IA à haut risque utilisent les informations fournies en application de l'article 13 du présent règlement pour se conformer à leur obligation de procéder à une analyse d'impact relative à la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680.

cf. RGPD art. 35

10. Sans préjudice de la directive (UE) 2016/680, dans le cadre d'une enquête en vue de la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale, le déployeur d'un système d'IA à haut risque pour l'identification biométrique à distance a posteriori demande l'autorisation, ex ante ou sans retard injustifié et au plus tard dans les 48 heures, d'une autorité judiciaire ou administrative dont la décision est contraignante et soumise à un contrôle juridictionnel, pour l'utilisation de ce système, sauf lorsqu'il est utilisé pour l'identification initiale d'un suspect potentiel sur la base de faits objectifs et vérifiables directement liés à l'infraction. Chaque utilisation est limitée à ce qui est strictement nécessaire pour enquêter sur une infraction pénale spécifique.

cf. déployeurs

Si l'autorisation demandée en application du premier alinéa est rejetée, l'utilisation du système d'identification biométrique à distance a posteriori lié à l'autorisation demandée est interrompue avec effet immédiat et les données à caractère personnel liées à l'utilisation du système d'IA à haut risque pour lequel l'autorisation a été demandée sont supprimées.

En aucun cas, ce système d'IA à haut risque pour l'identification biométrique à distance a posteriori ne peut être utilisé à des fins répressives de manière non ciblée, sans aucun lien avec une infraction pénale, une procédure pénale, une menace réelle et actuelle ou réelle et prévisible d'une infraction pénale, ou la recherche d'une personne disparue spécifique. Il convient d'assurer qu'aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne puisse être prise par les autorités répressives sur la seule base des sorties de tels systèmes d'identification biométrique à distance a posteriori.

Le présent paragraphe est sans préjudice de l'article 9 du règlement (UE) 2016/679 et de l'article 10 de la directive (UE) 2016/680 pour le traitement des données biométriques.

cf. RGPD art. 9

Indépendamment de la finalité ou du déployeur, chaque utilisation de ces systèmes d'IA à haut risque est documentée dans le dossier de police pertinent et est mise à la disposition de l'autorité de surveillance du marché concernée et de l'autorité nationale chargée de la protection des données sur demande, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Le présent alinéa est sans préjudice des pouvoirs conférés par la directive (UE) 2016/680 aux autorités de contrôle.

cf. déployeurs

cf. CNIL

Les déployeurs soumettent aux autorités de surveillance du marché concernées et aux autorités nationales chargées de la protection des données des rapports annuels sur leur utilisation de systèmes d'identification biométrique à distance a posteriori, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Les rapports peuvent être agrégés pour couvrir plus d'un déploiement.

cf. CNIL

Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance a posteriori.

11. Sans préjudice de l'article 50 du présent règlement, les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, qui prennent des décisions ou facilitent les prises de décision concernant des personnes physiques, informent lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Pour les systèmes d'IA à haut risque utilisés à des fins répressives, l'article 13 de la directive (UE) 2016/680 s'applique.

cf. déployeurs

12. Les déployeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard du système d'IA à haut risque en vue de mettre en œuvre le présent règlement.

cf. déployeurs

article 27
Analyse d'impact des systèmes d'IA à haut risque sur les droits fondamentaux

1. Avant le déploiement d'un système d'IA à haut risque visé à l'article 6, paragraphe 2, à l'exception des systèmes d'IA à haut risque destinés à être utilisés dans le domaine visé à l'annexe III, point 2, les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, points 5), b) et c), effectuent une analyse de l'impact sur les droits fondamentaux que l'utilisation de ce système peut produire. À cette fin, les déployeurs effectuent une analyse comprenant:

cf. déployeurs

a) une description des processus du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination;

b) une description de la période pendant laquelle et de la fréquence à laquelle chaque système d'IA à haut risque est destiné à être utilisé;

c) les catégories de personnes physiques et les groupes susceptibles d'être concernés par son utilisation dans le contexte spécifique;

d) les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les catégories de personnes physiques ou groupes de personnes identifiés en vertu du point c) du présent paragraphe, compte tenu des informations fournies par le fournisseur conformément à l'article 13;

e) une description de la mise en œuvre des mesures de contrôle humain, conformément à la notice d'utilisation;

f) les mesures à prendre en cas de matérialisation de ces risques, y compris les dispositifs relatifs à la gouvernance interne et aux mécanismes de plainte internes.

2. L'obligation établie au paragraphe 1 s'applique à la première utilisation du système d'IA à haut risque. Le déployeur peut, dans des cas similaires, s'appuyer sur des analyses d'impact sur les droits fondamentaux effectuées précédemment ou sur des analyses d'impact existantes réalisées par le fournisseur. Si, au cours de l'utilisation du système d'IA à haut risque, le déployeur estime qu'un des éléments énumérés au paragraphe 1 a changé ou n'est plus à jour, il prend les mesures nécessaires pour mettre à jour les informations.

cf. déployeurs

3. Une fois l'analyse visée au paragraphe 1 du présent article effectuée, le déployeur en notifie les résultats à l'autorité de surveillance du marché, et soumet le modèle visé au paragraphe 5 du présent article, rempli, dans le cadre de la notification. Dans le cas visé à l'article 46, paragraphe 1, les déployeurs peuvent être exemptés de cette obligation de notification.

4. Si l'une des obligations prévues au présent article est déjà remplie au moyen de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, l'analyse d'impact sur les droits fondamentaux visée au paragraphe 1 du présent article complète ladite analyse d'impact relative à la protection des données.

cf. RGPD

5. Le Bureau de l'IA élabore un modèle de questionnaire, y compris au moyen d'un outil automatisé, afin d'aider les déployeurs à se conformer de manière simplifiée aux obligations qui leur incombent en vertu du présent article.

SECTION 4
Autorités notifiantes et organismes notifiés

article 28
Autorités notifiantes

1. Chaque État membre désigne ou établit au moins une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle. Ces procédures sont élaborées en coopération entre les autorités notifiantes de tous les États membres.

2. Les États membres peuvent décider que l'évaluation et le contrôle visés au paragraphe 1 doivent être effectués par un organisme national d'accréditation au sens du règlement (CE) no 765/2008 et conformément à ses dispositions.

3. Les autorités notifiantes sont établies, organisées et gérées de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité et à garantir l'objectivité et l'impartialité de leurs activités.

4. Les autorités notifiantes sont organisées de telle sorte que les décisions concernant la notification des organismes d'évaluation de la conformité soient prises par des personnes compétentes différentes de celles qui ont réalisé l'évaluation de ces organismes.

5. Les autorités notifiantes ne proposent ni ne fournissent aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle.

6. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.

7. Les autorités notifiantes disposent d'un personnel compétent en nombre suffisant pour la bonne exécution de leurs tâches. Le personnel compétent possède l'expertise nécessaire, le cas échéant, pour sa fonction, dans des domaines tels que les technologies de l'information, l'IA et le droit, y compris le contrôle du respect des droits fondamentaux.

article 29
Demande de notification d'un organisme d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité soumettent une demande de notification à l'autorité notifiante de l'État membre dans lequel ils sont établis.

2. La demande de notification est accompagnée d'une description des activités d'évaluation de la conformité, du ou des modules d'évaluation de la conformité et des types de systèmes d'IA pour lesquels l'organisme d'évaluation de la conformité se déclare compétent, ainsi que d'un certificat d'accréditation, lorsqu'il existe, délivré par un organisme national d'accréditation qui atteste que l'organisme d'évaluation de la conformité remplit les exigences énoncées à l'article 31.

Tout document en cours de validité relatif à des désignations existantes de l'organisme notifié demandeur en vertu de toute autre législation d'harmonisation de l'Union est ajouté.

3. Lorsque l'organisme d'évaluation de la conformité ne peut pas produire de certificat d'accréditation, il présente à l'autorité notifiante toutes les preuves documentaires nécessaires à la vérification, à la reconnaissance et au contrôle régulier de sa conformité avec les exigences définies à l'article 31.

4. Quant aux organismes notifiés désignés en vertu de toute autre législation d'harmonisation de l'Union, tous les documents et certificats liés à ces désignations peuvent être utilisés à l'appui de leur procédure de désignation au titre du présent règlement, le cas échéant. L'organisme notifié met à jour la documentation visée aux paragraphes 2 et 3 du présent article dès que des changements pertinents interviennent afin de permettre à l'autorité responsable des organismes notifiés de contrôler et de vérifier que toutes les exigences énoncées à l'article 31 demeurent observées.

article 30
Procédure de notification

1. Les autorités notifiantes ne peuvent notifier que les organismes d'évaluation de la conformité qui ont satisfait aux exigences énoncées à l'article 31.

2. Les autorités notifiantes informent la Commission et les autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission quant à chaque organisme d'évaluation de la conformité visé au paragraphe 1.

3. La notification visée au paragraphe 2 du présent article comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les types de systèmes d'IA concernés, ainsi que l'attestation de compétence correspondante. Lorsqu'une notification n'est pas fondée sur le certificat d'accréditation visé à l'article 29, paragraphe 2, l'autorité notifiante fournit à la Commission et aux autres États membres les preuves documentaires attestant de la compétence de l'organisme d'évaluation de la conformité et des dispositions prises pour faire en sorte que cet organisme soit régulièrement contrôlé et continue à satisfaire aux exigences énoncées à l'article 31.

4. L'organisme d'évaluation de la conformité concerné ne peut effectuer les activités propres à un organisme notifié que si aucune objection n'est émise par la Commission ou les autres États membres dans les deux semaines suivant la notification par une autorité notifiante, si cette notification comprend le certificat d'accréditation visé à l'article 29, paragraphe 2, ou dans les deux mois suivant la notification par une autorité notifiante si cette notification comprend les preuves documentaires visées à l'article 29, paragraphe 3.

5. En cas d'objections, la Commission entame sans tarder des consultations avec les États membres et l'organisme d'évaluation de la conformité concernés. Au vu de ces consultations, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre et à l'organisme d'évaluation de la conformité concernés.

article 31
Exigences concernant les organismes notifiés

1. Un organisme notifié est constitué en vertu du droit national d'un État membre et a la personnalité juridique.

2. Les organismes notifiés se conforment aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de procédures qui sont nécessaires à l'exécution de leurs tâches, ainsi qu'aux exigences appropriées en matière de cybersécurité.

3. La structure organisationnelle, la répartition des responsabilités, les liens hiérarchiques et le fonctionnement des organismes notifiés garantissent la confiance dans leurs activités et la fiabilité des résultats des activités d'évaluation de la conformité menées par les organismes notifiés.

4. Les organismes notifiés sont indépendants du fournisseur du système d'IA à haut risque pour lequel ils mènent les activités d'évaluation de la conformité. Les organismes notifiés sont également indépendants de tout autre opérateur ayant un intérêt économique dans les systèmes d'IA à haut risque qui font l'objet de l'évaluation, ainsi que de tout concurrent du fournisseur. Cela n'exclut pas l'utilisation de systèmes d'IA à haut risque évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces systèmes d'IA à haut risque à des fins personnelles.

5. L'organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter ses tâches d'évaluation de la conformité ne participent pas directement à la conception, au développement, à la commercialisation ou à l'utilisation de systèmes d'IA à haut risque, pas plus qu'ils ne représentent les parties engagées dans ces activités. Ils n'exercent aucune activité susceptible d'entrer en conflit avec leur indépendance de jugement ou leur intégrité en ce qui concerne les activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela s'applique en particulier aux services de conseil.

6. Les organismes notifiés sont organisés et fonctionnent de façon à garantir l'indépendance, l'objectivité et l'impartialité de leurs activités. Les organismes notifiés documentent et appliquent une structure et des procédures visant à garantir l'impartialité et à encourager et appliquer les principes d'impartialité dans l'ensemble de leur organisation, du personnel et des activités d'évaluation.

7. Les organismes notifiés disposent de procédures documentées pour veiller à ce que leur personnel, leurs comités, leurs filiales, leurs sous-traitants et tout organisme associé ou le personnel d'organismes externes préservent, conformément à l'article 78, la confidentialité des informations auxquelles ils accèdent durant l'exercice de leurs activités d'évaluation de la conformité, sauf lorsque leur divulgation est requise par la loi. Le personnel des organismes notifiés est lié par le secret professionnel pour toutes les informations dont il a connaissance dans l'exercice de ses fonctions au titre du présent règlement, sauf à l'égard des autorités notifiantes de l'État membre où il exerce ses activités.

8. Les organismes notifiés disposent de procédures pour accomplir leurs activités qui tiennent dûment compte de la taille des fournisseurs, du secteur dans lequel ils exercent leurs activités, de leur structure et du degré de complexité du système d'IA concerné.

9. Les organismes notifiés souscrivent, pour leurs activités d'évaluation de la conformité, une assurance de responsabilité civile appropriée à moins que cette responsabilité ne soit couverte par l'État membre dans lequel ils sont établis sur la base du droit national ou que l'État membre soit lui-même responsable de l'évaluation de la conformité.

10. Les organismes notifiés sont en mesure d'accomplir toutes leurs tâches au titre du présent règlement avec la plus haute intégrité professionnelle et la compétence requise dans le domaine spécifique, qu'ils exécutent eux-mêmes ces tâches ou que celles-ci soient exécutées pour leur compte et sous leur responsabilité.

11. Les organismes notifiés disposent de compétences internes suffisantes pour pouvoir évaluer efficacement les tâches effectuées pour leur compte par des parties extérieures. L'organisme notifié dispose en permanence d'un personnel administratif, technique, juridique et scientifique en nombre suffisant et doté d'une expérience et de connaissances liées aux données, au traitement des données et aux types de systèmes d'IA en cause et aux exigences énoncées à la section 2.

12. Les organismes notifiés prennent part aux activités de coordination visées à l'article 38. Ils participent également, directement ou par l'intermédiaire d'un représentant, aux activités des organisations européennes de normalisation, ou font en sorte de se tenir informés des normes applicables et de leur état.

article 32
Présomption de conformité avec les exigences concernant les organismes notifiés

Lorsqu'un organisme d'évaluation de la conformité démontre sa conformité avec les critères énoncés dans les normes harmonisées concernées, ou dans des parties de ces normes, dont les références ont été publiées au Journal officiel de l'Union européenne, il est présumé répondre aux exigences énoncées à l'article 31 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

article 33
Filiales des organismes notifiés et sous-traitance

1. Lorsqu'un organisme notifié sous-traite des tâches spécifiques dans le cadre de l'évaluation de la conformité ou a recours à une filiale, il s'assure que le sous-traitant ou la filiale répond aux exigences fixées à l'article 31 et en informe l'autorité notifiante.

2. Les organismes notifiés assument l'entière responsabilité des tâches effectuées par tout sous-traitants ou toute filiale.

3. Des activités ne peuvent être sous-traitées ou réalisées par une filiale qu'avec l'accord du fournisseur. Les organismes notifiés rendent publique une liste de leurs filiales.

4. Les documents pertinents concernant l'évaluation des qualifications du sous-traitant ou de la filiale et le travail exécuté par celui-ci ou celle-ci en vertu du présent règlement sont tenus à la disposition de l'autorité notifiante pendant une période de cinq ans à compter de la date de cessation de la sous-traitance.

article 34
Obligations opérationnelles des organismes notifiés

1. Les organismes notifiés vérifient la conformité du système d'IA à haut risque conformément aux procédures d'évaluation de la conformité visées à l'article 43.

2. Les organismes notifiés évitent les charges inutiles pour les fournisseurs dans l'exercice de leurs activités et tiennent dûment compte de la taille du fournisseur, du secteur dans lequel il exerce ses activités, de sa structure et du degré de complexité du système d'IA à haut risque concerné, en particulier en vue de réduire au minimum les charges administratives et les coûts de mise en conformité pour les microentreprises et les petites entreprises au sens de la recommandation 2003/361/CE. L'organisme notifié respecte néanmoins le degré de rigueur et le niveau de protection requis afin de garantir la conformité du système d'IA à haut risque avec les exigences du présent règlement.

3. Les organismes notifiés mettent à la disposition de l'autorité notifiante visée à l'article 28 et lui soumettent sur demande toute la documentation pertinente, y compris

celle des fournisseurs, afin de permettre à cette autorité de réaliser ses activités d'évaluation, de désignation, de notification et de surveillance et pour faciliter les évaluations décrites à la présente section.

article 35
Numéros d'identification et listes des organismes notifiés

1. La Commission attribue un numéro d'identification unique à chaque organisme notifié, même lorsqu'un organisme est notifié au titre de plus d'un acte de l'Union.

2. La Commission rend publique la liste des organismes notifiés au titre du présent règlement et y mentionne leurs numéros d'identification et les activités pour lesquelles ils ont été notifiés. La Commission veille à ce que cette liste soit tenue à jour.

article 36
Modifications apportées aux notifications

1. L'autorité notifiante notifie à la Commission et aux autres États membres toute modification pertinente apportée à la notification d'un organisme notifié au moyen de l'outil de notification électronique visé à l'article 30, paragraphe 2.

2. Les procédures établies aux articles 29 et 30 s'appliquent en cas d'extension de la portée de la notification.

En cas de modification de la notification autre qu'une extension de sa portée, les procédures prévues aux paragraphes 3 à 9 s'appliquent.

3. Lorsqu'un organisme notifié décide de cesser ses activités d'évaluation de la conformité, il informe l'autorité notifiante et les fournisseurs concernés dès que possible et, dans le cas d'un arrêt prévu de ses activités, au moins un an avant de mettre un terme à ses activités. Les certificats de l'organisme notifié peuvent rester valables pendant une période de neuf mois après l'arrêt des activités de l'organisme notifié, à condition qu'un autre organisme notifié confirme par écrit qu'il assumera la responsabilité des systèmes d'IA à haut risque concernés par ces certificats. Cet autre organisme notifié procède à une évaluation complète des systèmes d'IA à haut risque concernés avant la fin de cette période de neuf mois, avant de délivrer de nouveaux certificats pour les systèmes en question. Lorsque l'organisme notifié a mis un terme à ses activités, l'autorité notifiante retire la désignation.

4. Lorsqu'une autorité notifiante a des raisons suffisantes de considérer qu'un organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, l'autorité notifiante procède sans retard à une enquête avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des objections soulevées et lui donne la possibilité de faire connaître son point de vue. Si l'autorité notifiante conclut que l'organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la désignation à des restrictions, la suspend ou la retire, selon le cas, en fonction de la gravité du manquement. Elle en informe immédiatement la Commission et les autres États membres.

5. Lorsque sa désignation a été suspendue, restreinte ou révoquée en tout ou en partie, l'organisme notifié en informe les fournisseurs concernés dans un délai de dix jours.

6. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante prend les mesures nécessaires pour que les dossiers de l'organisme notifié en question soient conservés et pour qu'ils soient mis à la disposition des autorités notifiantes d'autres États membres et des autorités de surveillance du marché, à leur demande.

7. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante:

a) évalue l'incidence sur les certificats délivrés par l'organisme notifié;

b) transmet un rapport sur ses conclusions à la Commission et aux autres États membres dans un délai de trois mois après avoir signalé les modifications apportées à la désignation;

c) exige de l'organisme notifié qu'il suspende ou retire, dans un délai raisonnable qu'elle détermine, tous les certificats délivrés à tort afin d'assurer la conformité constante des systèmes d'IA à haut risque sur le marché;

d) informe la Commission et les États membres des certificats dont elle a demandé la suspension ou le retrait;

e) fournit aux autorités nationales compétentes de l'État membre dans lequel le fournisseur a son siège social toutes les informations pertinentes sur les certificats dont elle a demandé la suspension ou le retrait; cette autorité prend les mesures appropriées si cela est nécessaire pour éviter un risque potentiel pour la santé, la sécurité ou les droits fondamentaux.

8. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été suspendue ou restreinte, les certificats restent valables dans l'un des cas suivants:

a) l'autorité notifiante a confirmé, dans un délai d'un mois suivant la suspension ou la restriction, qu'il n'y a pas de risque pour la santé, la sécurité ou les droits fondamentaux en lien avec les certificats concernés par la suspension ou la restriction, et l'autorité notifiante a défini un calendrier de mesures pour remédier à la suspension ou à la restriction; ou

b) l'autorité notifiante a confirmé qu'aucun certificat ayant trait à la suspension ne sera délivré, modifié ou délivré à nouveau pendant la période de suspension ou de restriction et elle indique si l'organisme notifié est en mesure de continuer à contrôler les certificats existants délivrés et à en être responsable pour la durée de la suspension ou de la restriction. Si l'autorité notifiante considère que l'organisme notifié n'est pas en mesure de se charger des certificats existants délivrés, le fournisseur du système faisant l'objet du certificat confirme par écrit aux autorités nationales compétentes de l'État membre dans lequel il a son siège social, dans un délai de trois mois suivant la suspension ou la restriction, qu'un autre organisme notifié qualifié assume temporairement les fonctions de surveillance de l'organisme notifié et continue d'assumer la responsabilité des certificats pour la durée de la suspension ou de la restriction.

9. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été retirée, les certificats restent valables pendant une durée de neuf mois dans les cas suivants:

a) l'««autorité nationale compétente de l'État membre dans lequel le fournisseur du système d'IA à haut risque faisant l'objet du certificat a son siège social a confirmé que les systèmes d'IA à haut risque en question ne présentent pas de risque pour la santé, la sécurité ou les droits fondamentaux; et

b) un autre organisme notifié a confirmé par écrit qu'il assumera la responsabilité immédiate de ces systèmes d'IA et achèvera son évaluation dans un délai de douze mois à compter du retrait de la désignation.

Dans le cas visé au premier alinéa, l'««autorité nationale compétente de l'État membre dans lequel le fournisseur du système faisant l'objet du certificat a son siège peut prolonger à plusieurs reprises la durée de validité provisoire des certificats de trois mois supplémentaires, pour une durée totale maximale de douze mois.

L'««autorité nationale compétente ou l'organisme notifié assumant les fonctions de l'organisme notifié concerné par la modification de la désignation en informe immédiatement la Commission, les autres États membres et les autres organismes notifiés.

article 37
Contestation de la compétence des organismes notifiés

1. La Commission enquête, s'il y a lieu, sur tous les cas où il existe des raisons de douter de la compétence d'un organisme notifié ou du respect continu, par un organisme notifié, des exigences établies à l'article 31 et de ses responsabilités applicables.

2. L'autorité notifiante fournit à la Commission, sur demande, toutes les informations utiles relatives à la notification ou au maintien de la compétence de l'organisme notifié concerné.

3. La Commission veille à ce que toutes les informations sensibles obtenues au cours des enquêtes qu'elle mène au titre du présent article soient traitées de manière confidentielle conformément à l'article 78.

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences relatives à sa notification, elle informe l'État membre notifiant en conséquence et lui demande de prendre les mesures correctives qui s'imposent, y compris la suspension ou le retrait de la notification si nécessaire. Si l'État membre ne prend pas les mesures correctives qui s'imposent, la Commission peut, au moyen d'un acte d'exécution, suspendre, restreindre ou retirer la désignation. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

article 38
Coordination des organismes notifiés

1. La Commission veille à ce que, en ce qui concerne les systèmes d'IA à haut risque, une coordination et une coopération appropriées entre les organismes notifiés intervenant dans les procédures d'évaluation de la conformité conformément au présent règlement soient mises en place et gérées de manière adéquate dans le cadre d'un groupe sectoriel d'organismes notifiés.

2. Chaque autorité notifiante veille à ce que les organismes qu'elle a notifiés participent aux travaux d'un groupe visé au paragraphe 1, directement ou par l'intermédiaire de représentants désignés.

3. La Commission veille à l'échange des connaissances et des bonnes pratiques entre les autorités notifiantes.

article 39
Organismes d'évaluation de la conformité de pays tiers

Les organismes d'évaluation de la conformité établis conformément à la législation d'un pays tiers avec lequel l'Union a conclu un accord peuvent être autorisés à exercer les activités d'organismes notifiés au titre du présent règlement, pour autant qu'ils répondent aux exigences prévues à l'article 31 ou qu'ils veillent à un niveau équivalent de respect.

SECTION 5
Normes, évaluation de la conformité, certificats, enregistrement

article 40
Normes harmonisées et travaux de normalisation

1. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au Journal officiel de l'Union européenne conformément au règlement (UE) no 1025/2012 sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, du présent règlement, dans la mesure où ces exigences ou obligations sont couvertes par ces normes.

2. Conformément à l'article 10 du règlement (UE) no 1025/2012, la Commission présente sans retard injustifié des demandes de normalisation couvrant toutes les exigences énoncées à la section 2 du présent chapitre et, le cas échéant, les demandes de normalisation couvrant les obligations énoncées au chapitre V, sections 2 et 3, du présent règlement. La demande de normalisation inclut également une demande de livrables sur les processus de déclaration et de documentation afin d'améliorer les performances des systèmes d'IA en matière de ressources, telles que la réduction de la consommation d'énergie et d'autres ressources par le système d'IA à haut risque au cours de son cycle de vie, et sur le développement économe en énergie de modèles d'IA à usage général. Lors de la préparation d'une demande de normalisation, la Commission consulte le Comité IA et les parties prenantes concernées, y compris le forum consultatif.

Lorsqu'elle présente une demande de normalisation aux organisations européennes de normalisation, la Commission précise que les normes doivent être claires, cohérentes, y compris avec les normes développées dans les différents secteurs pour les produits relevant de la législation d'harmonisation de l'Union existante dont la liste figure à l'annexe I, et visant à veiller à ce que les systèmes d'IA à haut risque ou les modèles d'IA à usage général mis sur le marché ou mis en service dans l'Union satisfont aux exigences ou obligations pertinentes énoncées dans le présent règlement.

La Commission demande aux organisations européennes de normalisation de fournir la preuve qu'elles mettent tout en œuvre pour atteindre les objectifs visés aux premier et deuxième alinéas du présent paragraphe, conformément à l'article 24 du règlement (UE) no 1025/2012.

3. Les participants au processus de normalisation s'efforcent de favoriser les investissements et l'innovation dans le domaine de l'IA, y compris en renforçant la sécurité juridique, ainsi que la compétitivité et la croissance du marché de l'Union, de contribuer à renforcer la coopération mondiale en faveur d'une normalisation en tenant compte des normes internationales existantes dans le domaine de l'IA qui sont conformes aux valeurs et aux intérêts de l'Union et aux droits fondamentaux, et de renforcer la gouvernance multipartite en veillant à une représentation équilibrée des intérêts et à la participation effective de toutes les parties prenantes concernées conformément aux articles 5, 6 et 7 du règlement (UE) no 1025/2012.

article 41
Spécifications communes

1. La Commission peut adopter des actes d'exécution établissant des spécifications communes pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre V, sections 2 et 3, lorsque les conditions suivantes sont remplies:

a) la Commission, en vertu de l'article 10, paragraphe 1, du règlement (UE) no 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre V, sections 2 et 3, et:
   i) la demande n'a été acceptée par aucune des organisations européennes de normalisation; ou
   ii) les normes harmonisées faisant l'objet de cette demande n'ont pas été présentées dans le délai fixé conformément à l'article 10, paragraphe 1, du règlement (UE) no 1025/2012; ou
   iii) les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux; ou
   iv) les normes harmonisées ne sont pas conformes à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences visées à la section 2 du chapitre ou, le cas échéant, les obligations énoncées au chapitre V, sections 2 et 3, n'a été publiée au Journal officiel de l'Union européenne conformément au règlement (UE) no 1025/2012, et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Lors de la rédaction des spécifications communes, la Commission consulte le forum consultatif visé à l'article 67.

Les actes d'exécution visés au premier alinéa du présent paragraphe sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Avant d'élaborer un projet d'acte d'exécution, la Commission informe le comité visé à l'article 22 du règlement (UE) no 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 1 du présent article sont remplies.

3. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes aux spécifications communes visées au paragraphe 1, ou à des parties de ces spécifications, sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant pour se conformer aux obligations visées au chapitre V, sections 2 et

3, dans la mesure où ces exigences ou obligations sont couvertes par ces spécifications communes.

4. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au Journal officiel de l'Union européenne, la Commission procède à l'évaluation de cette norme harmonisée conformément au règlement (UE) no 1025/2012. Lorsque la référence à une norme harmonisée est publiée au Journal officiel de l'Union européenne, la Commission abroge les actes d'exécution visés au paragraphe 1, ou les parties de ces actes qui couvrent les mêmes exigences que celles énoncées à la section 2 du présent chapitre ou, le cas échéant les mêmes obligations que celles énoncées au chapitre V, sections 2 et 3.

5. Lorsque les fournisseurs de systèmes d'IA à haut risque ou de modèles d'IA à usage général ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment avoir adopté des solutions techniques qui satisfont aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, à un niveau au moins équivalent auxdites spécifications.

6. Lorsqu'un État membre considère qu'une spécification commune ne satisfait pas entièrement aux exigences énoncées à la section 2 ou, le cas échéant aux obligations énoncées au chapitre V, sections 2 et 3, il en informe la Commission au moyen d'une explication détaillée. La Commission évalue ces informations et, le cas échéant, modifie l'acte d'exécution établissant la spécification commune concernée.

article 42
Présomption de conformité avec certaines exigences

1. Les systèmes d'IA à haut risque qui ont été entraînés et testés avec des données tenant compte du cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes aux exigences pertinentes établies à l'article 10, paragraphe 4.

2. Les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 et dont les références ont été publiées au Journal officiel de l'Union européenne sont présumés conformes aux exigences de cybersécurité énoncées à l'article 15 du présent règlement, dans la mesure où ces dernières sont couvertes par tout ou partie du certificat de cybersécurité ou de la déclaration de conformité.

article 43
Évaluation de la conformité

1. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, lorsque, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur a appliqué les normes harmonisées visées à l'article 40 ou, le cas échéant, les spécifications communes visées à l'article 41, il choisit l'une des procédures d'évaluation de la conformité suivantes sur la base:

a) du contrôle interne visé à l'annexe VI; ou

b) de l'évaluation du système de gestion de la qualité et de l'évaluation de la documentation technique, avec l'intervention d'un organisme notifié, visée à l'annexe VII.

Pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur suit la procédure d'évaluation de la conformité prévue à l'annexe VII dans les cas suivants:

a) les normes harmonisées visées à l'article 40 n'existent pas et les spécifications communes visées à l'article 41 font défaut;

b) le fournisseur n'a pas appliqué la norme harmonisée ou ne l'a appliquée que partiellement;

c) les spécifications communes visées au point a) existent, mais le fournisseur ne les a pas appliquées;

d) une ou plusieurs des normes harmonisées visées au point a), ont été publiées assorties d'une restriction et seulement sur la partie de la norme qui a été soumise à une restriction.

Aux fins de la procédure d'évaluation de la conformité visée à l'annexe VII, le fournisseur peut choisir n'importe lequel des organismes notifiés. Toutefois, lorsque le système d'IA à haut risque est destiné à être mis en service par les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile ou par les institutions, organes ou organismes de l'UE, l'autorité de surveillance du marché visée à l'article 74, paragraphe 8 ou 9, selon le cas, agit en tant qu'organisme notifié.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas d'intervention d'un organisme notifié.

3. Pour les systèmes d'IA à haut risque couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fournisseur suit la procédure d'évaluation de la conformité pertinente selon les modalités requises par ces actes juridiques. Les exigences énoncées à la section 2 du présent chapitre s'appliquent à ces systèmes d'IA à haut risque et font partie de cette évaluation. Les points 4.3, 4.4 et 4.5 de l'annexe VII ainsi que le point 4.6, cinquième alinéa, de ladite annexe s'appliquent également.

Aux fins de ces évaluations, les organismes notifiés qui ont été notifiés en vertu de ces actes juridiques sont habilités à contrôler la conformité des systèmes d'IA à haut risque avec les exigences énoncées à la section 2, à condition que le respect, par ces organismes notifiés, des exigences énoncées à l'article 31, paragraphes 4, 5, 10 et 11, ait été évalué dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsqu'un acte juridique énuméré à l'annexe I, section A, confère au fabricant du produit la faculté de ne pas faire procéder à une évaluation de la conformité par un tiers, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant ne peut faire usage de cette faculté que s'il a également appliqué les normes harmonisées ou, le cas échéant, les spécifications communes visées à l'article 41 couvrant toutes les exigences énoncées à la section 2 du présent chapitre.

4. Les systèmes d'IA à haut risque qui ont déjà été soumis à une procédure d'évaluation de la conformité sont soumis à une nouvelle procédure d'évaluation de la conformité lorsqu'ils font l'objet de modifications substantielles, que le système modifié soit destiné à être distribué plus largement ou reste utilisé par le déployeur actuel.

cf. déployeurs

Pour les systèmes d'IA à haut risque qui continuent leur apprentissage après avoir été mis sur le marché ou mis en service, les modifications apportées au système d'IA à haut risque et à sa performance qui ont été déterminées au préalable par le fournisseur au moment de l'évaluation initiale de la conformité et font partie des informations contenues dans la documentation technique visée à l'annexe IV, point 2), f), ne constituent pas une modification substantielle.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les annexes VI et VII afin de les mettre à jour compte tenu du progrès technique.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les paragraphes 1 et 2 du présent article afin de soumettre les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, à tout ou partie de la procédure d'évaluation de la conformité visée à l'annexe VII. La Commission adopte ces actes délégués en tenant compte de l'efficacité de la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI pour prévenir ou réduire au minimum les risques que ces systèmes font peser sur la santé et la sécurité et sur la protection des droits fondamentaux, ainsi que de la disponibilité de capacités et de ressources suffisantes au sein des organismes notifiés.

article 44
Certificats

1. Les certificats délivrés par les organismes notifiés conformément à l'annexe VII sont établis dans une langue aisément compréhensible par les autorités compétentes de l'État membre dans lequel l'organisme notifié est établi.

2. Les certificats sont valables pendant la période indiquée sur ceux-ci, qui n'excède pas cinq ans pour les systèmes d'IA relevant de l'annexe I, et quatre ans pour les systèmes d'IA relevant de l'annexe III. À la demande du fournisseur, la durée de validité d'un certificat peut être prolongée d'une durée maximale de cinq ans à chaque fois pour les systèmes d'IA relevant de l'annexe I, et de quatre ans pour les systèmes d'IA relevant de l'annexe III, sur la base d'une nouvelle évaluation suivant les procédures d'évaluation de la conformité applicables. Tout document complémentaire à un certificat reste valable, à condition que le certificat qu'il complète le soit.

3. Lorsqu'un organisme notifié constate qu'un système d'IA ne répond plus aux exigences énoncées à la section 2, il suspend ou retire le certificat délivré ou l'assortit de restrictions, en tenant compte du principe de proportionnalité, sauf si le fournisseur applique, en vue du respect de ces exigences, des mesures correctives appropriées dans le délai imparti à cet effet par l'organisme notifié. L'organisme notifié motive sa décision.

Une procédure de recours contre les décisions des organismes notifiés, y compris concernant des certificats de conformité délivrés, est disponible.

article 45
Obligations d'information des organismes notifiés

1. Les organismes notifiés communiquent à l'autorité notifiante:

a) tout certificat d'évaluation UE de la documentation technique, tout document complémentaire afférent à ce certificat, et toute approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;

b) tout refus, restriction, suspension ou retrait d'un certificat d'évaluation UE de la documentation technique ou d'une approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;

c) toute circonstance ayant une incidence sur la portée ou les conditions de la notification;

d) toute demande d'information reçue des autorités de surveillance du marché concernant les activités d'évaluation de la conformité;

e) sur demande, les activités d'évaluation de la conformité réalisées dans le cadre de leur notification et toute autre activité réalisée, y compris les activités transfrontières et sous-traitées.

2. Chaque organisme notifié porte à la connaissance des autres organismes notifiés:

a) les approbations de systèmes de gestion de la qualité qu'il a refusées, suspendues ou retirées et, sur demande, les approbations qu'il a délivrées;

b) les certificats d'évaluation UE de la documentation technique ou les documents complémentaires y afférents qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions et, sur demande, les certificats et/ou documents complémentaires y afférents qu'il a délivrés.

3. Chaque organisme notifié fournit aux autres organismes notifiés qui accomplissent des activités similaires d'évaluation de la conformité portant sur les mêmes types de systèmes d'IA des informations pertinentes sur les aspects liés à des résultats négatifs et, sur demande, à des résultats positifs d'évaluation de la conformité.

4. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.

article 46
Dérogation à la procédure d'évaluation de la conformité

1. Par dérogation à l'article 43 et sur demande dûment justifiée, toute autorité de surveillance du marché peut, pour des raisons exceptionnelles de sécurité publique ou pour assurer la protection de la vie et de la santé humaines, la protection de l'environnement ou la protection d'actifs industriels et d'infrastructures d'importance majeure, autoriser la mise sur le marché ou la mise en service de systèmes d'IA à haut risque spécifiques sur le territoire de l'État membre concerné. Cette autorisation est accordée pour une période limitée pendant la durée des procédures d'évaluation de la conformité nécessaires, en tenant compte des raisons exceptionnelles justifiant la dérogation. Ces procédures sont menées à bien sans retard injustifié.

2. Dans une situation d'urgence dûment justifiée pour des raisons exceptionnelles de sécurité publique ou en cas de menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques, les autorités répressives ou les autorités de protection civile peuvent mettre en service un service d'IA à haut risque spécifique sans avoir obtenu l'autorisation visée au paragraphe 1, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation. Si l'autorisation visée au paragraphe 1 est refusée, l'utilisation du système d'IA à haut risque cesse immédiatement et tous les résultats et sorties de cette utilisation sont immédiatement mis au rebut.

3. L'autorisation visée au paragraphe 1 n'est délivrée que si l'autorité de surveillance du marché conclut que le système d'IA à haut risque satisfait aux exigences de la section 2. L'autorité de surveillance du marché informe la Commission et les autres États membres de toute autorisation délivrée conformément aux paragraphes 1 et 2. Cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives.

4. Si aucune objection n'est émise, dans un délai de quinze jours civils suivant la réception des informations visées au paragraphe 3, par un État membre ou par la Commission à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un État membre conformément au paragraphe 1, cette autorisation est réputée justifiée.

5. Si, dans un délai de quinze jours civils suivant la réception de la notification visée au paragraphe 3, un État membre soulève des objections à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un autre État membre, ou si la Commission estime que l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres quant à la conformité du système visée au paragraphe 3 n'est pas fondée, la Commission entame sans retard des consultations avec l'État membre concerné. Les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Sur cette base, la Commission décide si l'autorisation est justifiée ou non. La Commission communique sa décision à l'État membre concerné ainsi qu'aux opérateurs concernés.

6. Si la Commission estime que l'autorisation est injustifiée, elle est retirée par l'autorité de surveillance du marché de l'État membre concerné.

7. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, seules les dérogations à l'évaluation de la conformité établies dans ladite législation d'harmonisation de l'Union s'appliquent.

article 47
Déclaration UE de conformité

1. Le fournisseur établit une déclaration UE de conformité écrite, lisible par machine, signée à la main ou électroniquement concernant chaque système d'IA à haut risque et la tient à la disposition des autorités nationales compétentes pendant une durée de dix ans à partir du moment où le système d'IA à haut risque a été mis sur le marché ou mis en service. La déclaration UE de conformité identifie le système d'IA à haut risque pour lequel elle a été établie. Une copie de la déclaration UE de conformité est communiquée, sur demande, aux autorités nationales compétentes concernées.

2. La déclaration UE de conformité atteste que le système d'IA à haut risque concerné satisfait aux exigences énoncées à la section 2. La déclaration UE de conformité contient les informations qui figurent à l'annexe V et est traduite dans une langue aisément compréhensible par les autorités nationales compétentes des États membres dans lesquels le système d'IA à haut risque est mis sur le marché ou mis à disposition.

3. Si des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs d'harmonisation de l'Union qui exigent également une déclaration UE de conformité, une seule déclaration UE de conformité est établie au titre de tous les actes législatifs de l'Union applicables au système d'IA à haut risque. La déclaration contient toutes les informations nécessaires à l'identification de la législation d'harmonisation de l'Union à laquelle la déclaration se rapporte.

4. Lors de l'établissement de la déclaration UE de conformité, le fournisseur assume la responsabilité du respect des exigences énoncées à la section 2. Le fournisseur tient à jour la déclaration UE de conformité, le cas échéant.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe V en mettant à jour le contenu de la déclaration UE de conformité prévu à ladite annexe afin d'y introduire les éléments devenus nécessaires compte tenu du progrès technique.

article 48
Marquage CE

1. Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) no 765/2008.

2. Pour les systèmes d'IA à haut risque fournis numériquement, un marquage CE numérique n'est utilisé que s'il est facile d'y accéder par l'interface à partir de laquelle l'accès à ce système s'effectue ou au moyen d'un code facilement accessible lisible par machine ou d'autres moyens électroniques.

3. Le marquage CE est apposé de façon visible, lisible et indélébile sur les systèmes d'IA à haut risque. Si cela est impossible ou injustifié étant donné la nature du système d'IA à haut risque, il est apposé sur l'emballage ou sur les documents d'accompagnement, selon le cas.

4. Le cas échéant, le marquage CE est suivi du numéro d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité prévues à l'article 43. Le numéro d'identification de l'organisme notifié est apposé par l'organisme lui-même ou, sur instruction de celui-ci, par le fournisseur ou par le mandataire du fournisseur. Le numéro d'identification est également indiqué dans tous les documents publicitaires mentionnant que le système d'IA à haut risque est conforme aux exigences applicables au marquage CE.

5. Lorsque des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, ce marquage indique que les systèmes d'IA à haut risque satisfont également aux exigences de ces autres actes législatifs.

article 49
Enregistrement

1. Avant de mettre sur le marché ou de mettre en service un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque visés à l'annexe III, point 2, le fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi son système.

2. Avant de mettre sur le marché ou de mettre en service un système d'IA à propos duquel le fournisseur a conclu qu'il ne s'agissait pas d'un système à haut risque au titre de l'article 6, paragraphe 3, ce fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi ce système.

3. Avant de mettre en service ou d'utiliser un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque énumérés à l'annexe III, point 2, les déployeurs qui sont des autorités publiques, des institutions organes ou organismes de l'Union ou des personnes agissant en leur nom s'enregistrent, sélectionnent le système et enregistrent son utilisation dans la base de données de l'UE visée à l'article 71.

cf. déployeurs

4. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, l'enregistrement visé aux paragraphes 1, 2 et 3 du présent article figure dans une section sécurisée non publique de la base de données de l'UE visée à l'article 71 et comprend uniquement les informations suivantes, selon le cas, visées:

a) à l'annexe VIII, section A, points 1 à 10, à l'exception des points 6, 8 et 9;

b) à l'annexe VIII, section B, points 1 à 5, et points 8 et 9;

c) à l'annexe VIII, section C, points 1 à 3;

d) à l'annexe IX, points 1, 2, 3 et 5.

Seules la Commission et les autorités nationales visées à l'article 74, paragraphe 8, ont accès aux différentes sections restreintes de la base de données de l'UE énumérées au premier alinéa du présent paragraphe.

5. Les systèmes d'IA à haut risque visés à l'annexe III, point 2, sont enregistrés au niveau national.

CHAPITRE IV
OBLIGATIONS DE TRANSPARENCE POUR LES FOURNISSEURS ET LES DÉPLOYEURS DE CERTAINS SYSTÈMES D'IA

Obligations de transparence

article 50
Obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA

1. Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir directement avec des personnes physiques soient conçus et développés de manière que les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Cette obligation ne s'applique pas aux systèmes d'IA dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers, sauf si ces systèmes sont mis à la disposition du public pour permettre le signalement d'une infraction pénale.

2. Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. Cette obligation ne s'applique pas dans la mesure où les systèmes d'IA remplissent une fonction d'assistance pour la mise en forme standard ou ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière.

cf. déployeurs

3. Les déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément

au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la catégorisation biométrique et la reconnaissance des émotions dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales ou d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers et conformément au droit de l'Union.

cf. RGPD

4. Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage indiquent que les contenus ont été générés ou manipulés par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre.

cf. déployeurs

Les déployeurs d'un système d'IA qui génère ou manipule des textes publiés dans le but d'informer le public sur des questions d'intérêt public indiquent que le texte a été généré ou manipulé par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, ou lorsque le contenu généré par l'IA a fait l'objet d'un processus d'examen humain ou de contrôle éditorial et lorsqu'une personne physique ou morale assume la responsabilité éditoriale de la publication du contenu.

cf. déployeurs

5. Les informations visées aux paragraphes 1 à 4 sont fournies aux personnes physiques concernées de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition. Les informations sont conformes aux exigences applicables en matière d'accessibilité.

6. Les paragraphes 1 à 4 n'ont pas d'incidence sur les exigences et obligations énoncées au chapitre III et sont sans préjudice des autres obligations de transparence prévues par le droit de l'Union ou le droit national pour les déployeurs de systèmes d'IA.

cf. déployeurs

7. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA. La Commission peut adopter des actes d'exécution pour approuver ces codes de bonne pratique conformément à la procédure prévue à l'article 56, paragraphe 6. Si elle estime que le code n'est pas approprié, la Commission peut adopter un acte d'exécution précisant des règles communes pour la mise en œuvre de ces obligations conformément à la procédure d'examen prévue à l'article 98, paragraphe 2.

CHAPITRE V
MODÈLES D'IA À USAGE GÉNÉRAL

Modèles d'IA à usage général

SECTION 1
Règles de classification

article 51
Classification de modèles d'IA à usage général en tant que modèles d'IA à usage général présentant un risque systémique

1. Un modèle d'IA à usage général est classé comme modèle d'IA à usage général présentant un risque systémique s'il remplit l'une des conditions suivantes:

a) il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence;

b) sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique, il possède des capacités ou un impact équivalents à ceux énoncés au point a), compte tenu des critères définis à l'annexe XIII.

2. Un modèle d'IA à usage général est présumé avoir des capacités à fort impact conformément au paragraphe 1, point a), lorsque la quantité cumulée de calcul utilisée pour son entraînement mesurée en opérations en virgule flottante est supérieure à 1025.

3. La Commission adopte des actes délégués conformément à l'article 97 pour modifier les seuils énumérés aux paragraphes 1 et 2 du présent article, ainsi que pour compléter les critères de référence et les indicateurs à la lumière des évolutions technologiques, telles que les améliorations algorithmiques ou l'efficacité accrue du matériel informatique, si nécessaire, afin que ces seuils reflètent l'état de la technique.

article 52
Procédure

1. Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51, paragraphe 1, point a), le fournisseur concerné en informe la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou après qu'il a été établi qu'il le sera. Cette notification comprend les informations nécessaires pour démontrer que le critère pertinent a été rempli. Si la Commission apprend l'existence d'un modèle d'IA à usage général présentant un risque systémique dont elle n'a pas été informée, elle peut décider de le désigner comme modèle présentant un risque systémique.

2. Le fournisseur d'un modèle d'IA à usage général qui remplit la condition visée à l'article 51, paragraphe 1, point a), peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'il remplisse ce critère, le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique et ne devrait donc pas être classé comme modèle d'IA à usage général présentant un risque systémique.

3. Lorsque la Commission conclut que les arguments présentés conformément au paragraphe 2 ne sont pas suffisamment étayés et que le fournisseur concerné n'a pas été en mesure de démontrer que le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique, elle rejette ces arguments, et le modèle d'IA à usage général est considéré comme un modèle d'IA à usage général présentant un risque systémique.

4. La Commission peut désigner un modèle d'IA à usage général comme présentant un risque systémique, d'office ou à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a), sur la base des critères énoncés à l'annexe XIII.

La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe XIII en précisant et mettant à jour les critères énoncés à ladite annexe.

5. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique en vertu du paragraphe 4, la Commission tient compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique sur la base des critères énoncés à l'annexe XIII. Une telle demande contient les éléments objectifs, détaillés et nouveaux qui sont apparus depuis la décision de désignation. Les fournisseurs peuvent demander une réévaluation au plus tôt six mois après la décision de désignation. Lorsque la Commission, à la suite de sa réévaluation, décide de maintenir la désignation en tant que modèle d'IA à usage général présentant un risque systémique, les fournisseurs peuvent demander une réévaluation au plus tôt six mois après cette décision.

6. La Commission veille à ce qu'une liste des modèles d'IA à usage général présentant un risque systémique soit publiée et tient cette liste à jour, sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national.

SECTION 2
Obligations incombant aux fournisseurs de modèles d'IA à usage général

article 53
Obligations incombant aux fournisseurs de modèles d'IA à usage général

1. Les fournisseurs de modèles d'IA à usage général:

a) élaborent et tiennent à jour la documentation technique du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, qui contient, au minimum, les informations énoncées à l'annexe XI aux fins de la fournir, sur demande, au Bureau de l'IA et aux autorités nationales compétentes;

b) élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation:

   i) permettent aux fournisseurs de systèmes d'IA d'avoir une bonne compréhension des capacités et des limites du modèle d'IA à usage général et de se conformer aux obligations qui leur incombent en vertu du présent règlement; et

   ii) contiennent, au minimum, les éléments énoncés à l'annexe XII;

c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790;

d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA.

2. Les obligations énoncées au paragraphe 1, points a) et b), ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. Cette exception ne s'applique pas aux modèles d'IA à usage général présentant un risque systémique.

3. Les fournisseurs de modèles d'IA à usage général coopèrent, en tant que de besoin, avec la Commission et les autorités nationales compétentes dans l'exercice de leurs compétences et pouvoirs en vertu du présent règlement.

4. Les fournisseurs de modèles d'IA à usage général peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.

5. Afin de faciliter le respect de l'annexe XI, et notamment du point 2, points d) et e), la Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour préciser les méthodes de mesure et de calcul en vue de permettre l'élaboration d'une documentation comparable et vérifiable.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97, paragraphe 2, pour modifier les annexes XI et XII à la lumière des évolutions technologiques.

7. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

article 54
Mandataires des fournisseurs de modèles d'IA à usage général

1. Avant de mettre un modèle d'IA à usage général sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.

3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat au Bureau de l'IA à la demande de ce dernier, dans l'une des langues officielles des institutions de l'Union. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:

a) vérifier que la documentation technique prévue à l'annexe XI a été rédigée et que toutes les obligations visées à l'article 53 et, le cas échéant, à l'article 55 ont été remplies par le fournisseur;

b) tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise sur le marché du modèle d'IA à usage général, et les coordonnées du fournisseur ayant désigné le mandataire;

c) communiquer au Bureau de l'IA, sur demande motivée de sa part, toutes les informations et tous les documents, y compris ceux visés au point b), nécessaires pour démontrer qu'il respecte les obligations du présent chapitre;

d) coopérer avec le Bureau de l'IA et les autorités compétentes, sur demande motivée de leur part, à toute mesure qu'ils prennent à l'égard d'un modèle d'IA à usage général, y compris lorsque le modèle est intégré dans des systèmes d'IA mis sur le marché ou mis en service dans l'Union.

4. Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, au Bureau de l'IA ou aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

5. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe en outre immédiatement le Bureau de l'IA de la cessation du mandat et des motifs qui la sous-tendent.

6. L'obligation énoncée au présent article ne s'applique pas aux fournisseurs de modèles d'IA à usage général qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics, à moins que les modèles d'IA à usage général présentent un risque systémique.

SECTION 3
Obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique

article 55
Obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique

1. Outre les obligations énumérées aux articles 53 et 54, les fournisseurs de modèles d'IA à usage général présentant un risque systémique:

a) effectuent une évaluation des modèles sur la base de protocoles et d'outils normalisés reflétant l'état de la technique, y compris en réalisant et en documentant

des essais contradictoires des modèles en vue d'identifier et d'atténuer les risques systémiques;

b) évaluent et atténuent les risques systémiques éventuels au niveau de l'Union, y compris leurs origines, qui peuvent découler du développement, de la mise sur le marché ou de l'utilisation de modèles d'IA à usage général présentant un risque systémique;

c) suivent, documentent et communiquent sans retard injustifié au Bureau de l'IA et, le cas échéant, aux autorités nationales compétentes les informations pertinentes concernant les incidents graves ainsi que les éventuelles mesures correctives pour y remédier;

d) garantissent un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.

2. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.

3. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

SECTION 4
Codes de bonnes pratiques

article 56
Codes de bonne pratique

1. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de contribuer à la bonne application du présent règlement, en tenant compte des approches internationales.

2. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique couvrent au moins les obligations prévues aux articles 53 et 55, y compris les questions suivantes:

a) les moyens de s'assurer que les informations visées à l'article 53, paragraphe 1, points a) et b), sont mises à jour à la lumière des évolutions du marché et des technologies;

b) le niveau approprié de détail pour le résumé du contenu utilisé pour l'entraînement;

c) l'identification du type et de la nature des risques systémiques au niveau de l'Union, y compris leurs origines, le cas échéant;

d) les mesures, procédures et modalités d'évaluation et de gestion des risques systémiques au niveau de l'Union, y compris la documentation y afférente, qui sont proportionnées aux risques, prennent en considération leur gravité et leur probabilité et tiennent compte des défis spécifiques que pose la maîtrise de ces risques à la lumière des différentes façons dont ils peuvent apparaître ou se concrétiser tout au long de la chaîne de valeur de l'IA.

3. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général, ainsi que les autorités nationales compétentes concernées, à participer à l'élaboration de codes de bonne pratique. Les organisations de la société civile, l'industrie, le monde universitaire et d'autres parties prenantes concernées, telles que les fournisseurs en aval et les experts indépendants, peuvent apporter leur soutien au processus.

4. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique définissent clairement leurs objectifs spécifiques et contiennent des engagements ou des mesures, y compris, le cas échéant, des indicateurs de performance clés, afin de garantir la réalisation de ces objectifs, et à ce qu'ils tiennent dûment compte des besoins et des intérêts de l'ensemble des parties intéressées, y compris les personnes concernées, au niveau de l'Union.

5. Le Bureau de l'IA veille à ce que les participants aux codes de bonne pratique fassent régulièrement rapport au Bureau de l'IA sur la mise en œuvre des engagements ainsi que sur les mesures qu'ils adoptent et leurs résultats, y compris mesurés par rapport aux indicateurs de performance clés, le cas échéant. Les indicateurs de performance clés et l'obligation de présenter des rapports reflètent les différences de taille et de capacité entre les différents participants.

6. Le Bureau de l'IA et le Comité IA contrôlent et évaluent régulièrement la réalisation des objectifs des codes de bonne pratique par les participants et leur contribution à la bonne application du présent règlement. Le Bureau de l'IA et le Comité IA évaluent si les codes de bonne pratique couvrent les obligations prévues aux articles 53 et 55, et contrôlent et évaluent régulièrement la réalisation de leurs objectifs. Ils publient leur évaluation de l'adéquation des codes de bonne pratique.

La Commission peut, au moyen d'un acte d'exécution, approuver un code de bonnes pratiques et lui conférer une validité générale au sein de l'Union. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général à adhérer aux codes de bonne pratique. Pour les fournisseurs de modèles d'IA à usage général ne présentant pas de risque systémique, cette adhésion peut se limiter aux obligations prévues à l'article 53, à moins qu'ils ne déclarent explicitement leur intérêt à respecter le code complet.

8. Le Bureau de l'IA encourage et facilite également, le cas échéant, le réexamen et l'adaptation des codes de bonne pratique, en particulier à la lumière des normes émergentes. Le Bureau de l'IA participe à l'évaluation des normes disponibles.

9. Les codes de bonne pratique sont prêts au plus tard le 2 mai 2025. Le Bureau de l'IA prend les mesures nécessaires, y compris inviter les fournisseurs en vertu du paragraphe 7.

Si, à la date du 2 août 2025, un code de bonnes pratiques n'a pas pu être mis au point, ou si le Bureau de l'IA estime qu'il n'est pas approprié à la suite de son évaluation au titre du paragraphe 6 du présent article, la Commission peut prévoir, au moyen d'actes d'exécution, des règles communes pour la mise en œuvre des obligations prévues aux articles 53 et 55, y compris les questions énoncées au paragraphe 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

CHAPITRE VI
MESURES DE SOUTIEN À L'INNOVATION

Soutien à l'innovation

article 57
Bacs à sable réglementaires de l'IA

1. Les États membres veillent à ce que leurs autorités compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national, qui est opérationnel au plus tard le 2 août 2026. Ce bac à sable peut également être établi conjointement avec les autorités compétentes d'autres États membres. La Commission peut fournir un soutien technique, des conseils et des outils pour la mise en place et l'exploitation de bacs à sable réglementaires de l'IA.

L'obligation visée au premier alinéa peut également être remplie en participant à un bac à sable existant, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants.

2. Des bacs à sable réglementaires de l'IA supplémentaires au niveau régional ou au niveau local, ou établis conjointement avec les autorités compétentes d'autres États membres peuvent également être mis en place.

3. Le Contrôleur européen de la protection des données peut également créer un bac à sable réglementaire de l'IA pour les institutions, organes et organismes de l'Union, et peut exercer les rôles et les tâches des autorités nationales compétentes conformément au présent chapitre.

4. Les États membres veillent à ce que les autorités compétentes visées aux paragraphes 1 et 2 allouent des ressources suffisantes pour se conformer au présent article de manière efficace et en temps utile. Lorsqu'il y a lieu, les autorités nationales compétentes coopèrent avec d'autres autorités concernées et peuvent permettre la participation d'autres acteurs de l'écosystème de l'IA. Le présent article n'a pas d'incidence sur d'autres bacs à sable réglementaires établis en vertu du droit de l'Union ou du droit national. Les États membres assurent un niveau approprié de coopération entre les autorités chargées de la surveillance de ces autres bacs à sable et les autorités nationales compétentes.

5. Les bacs à sable réglementaires de l'IA établis en vertu du paragraphe 1 offrent un environnement contrôlé qui favorise l'innovation et facilite le développement, l'entraînement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique de bac à sable convenu entre les fournisseurs ou fournisseurs potentiels et l'autorité compétente. Ces bacs à sable peuvent comprendre des essais en conditions réelles qui y sont supervisés.

6. Les autorités compétentes fournissent, s'il y a lieu, des orientations, une surveillance et un soutien dans le cadre du bac à sable réglementaire de l'IA en ce qui concerne l'identification des risques, en particulier pour les droits fondamentaux, la santé et la sécurité, les essais, les mesures d'atténuation et leur efficacité par rapport aux obligations et exigences du présent règlement et, le cas échéant, d'autres dispositions du droit de l'Union et du droit national dont le respect est suivi dans le cadre du bac à sable.

7. Les autorités compétentes donnent aux fournisseurs et aux fournisseurs potentiels participant au bac à sable réglementaire de l'IA des orientations sur les attentes réglementaires et la manière de satisfaire aux exigences et obligations énoncées dans le présent règlement.

À la demande du fournisseur ou du fournisseur potentiel du système d'IA, l'autorité compétente fournit une preuve écrite des activités menées avec succès dans le bac à sable. L'autorité compétente fournit également un rapport de sortie détaillant les activités menées dans le bac à sable ainsi que les résultats et acquis d'apprentissage correspondants. Les fournisseurs peuvent utiliser ces documents pour démontrer leur conformité avec le présent règlement au moyen de la procédure d'évaluation de la conformité ou d'activités pertinentes de surveillance du marché. À cet égard, les rapports de sortie et la preuve écrite fournie par l'««autorité nationale compétente sont évalués de manière positive par les autorités de surveillance du marché et les organismes notifiés, en vue d'accélérer les procédures d'évaluation de la conformité dans une mesure raisonnable.

8. Sous réserve des dispositions relatives à la confidentialité énoncées à l'article 78 et avec l'accord du fournisseur ou du fournisseur potentiel, la Commission et le Comité IA sont autorisés à accéder aux rapports de sortie et en tiennent compte, le cas échéant, dans l'exercice des tâches qui leur incombent en vertu du présent règlement. Si le fournisseur ou le fournisseur potentiel et l'«autorité nationale compétente y consentent explicitement, le rapport de sortie peut être mis à la disposition du public par l'intermédiaire de la plateforme d'information unique visée au présent article.

9. La mise en place de bacs à sable réglementaires de l'IA vise à contribuer aux objectifs suivants:

a) améliorer la sécurité juridique afin d'assurer le respect réglementaire du présent règlement ou, le cas échéant, d'autres dispositions applicables du droit de l'Union et du droit national;

b) soutenir le partage des bonnes pratiques par la coopération avec les autorités participant au bac à sable réglementaire de l'IA;

c) favoriser l'innovation et la compétitivité et faciliter la mise en place d'un écosystème d'IA;

d) contribuer à l'apprentissage réglementaire fondé sur des données probantes;

e) faciliter et accélérer l'accès au marché de l'Union pour les systèmes d'IA, en particulier lorsqu'ils sont fournis par des PME, y compris des jeunes pousses.

10. Les autorités nationales compétentes veillent à ce que, dans la mesure où les systèmes d'IA innovants impliquent le traitement de données à caractère personnel ou relèvent à d'autres titres de la surveillance d'autres autorités nationales ou autorités compétentes assurant ou encadrant l'accès aux données, les autorités nationales chargées de la protection des données et ces autres autorités nationales ou autorités compétentes soient associées à l'exploitation du bac à sable réglementaire de l'IA et participent au contrôle des aspects qui relèvent de leurs tâches et pouvoirs respectifs.

11. Les bacs à sable réglementaires de l'IA n'ont pas d'incidence sur les pouvoirs en matière de contrôle ou de mesures correctives des autorités compétentes chargées de la surveillance des bacs à sable, y compris au niveau régional ou local. Tout risque substantiel pour la santé, la sécurité et les droits fondamentaux constaté lors du développement et des tests de ces systèmes d'IA donne lieu à des mesures d'atténuation appropriées. Les autorités nationales compétentes sont habilitées à suspendre temporairement ou définitivement le processus d'essai ou la participation au bac à sable si aucune atténuation efficace n'est possible, et elles informent le Bureau de l'IA de cette décision. Les autorités nationales compétentes exercent leurs pouvoirs de surveillance, dans les limites de la législation applicable, en faisant usage de leurs pouvoirs discrétionnaires lorsqu'elles mettent en œuvre des dispositions juridiques relatives à un projet spécifique de bac à sable réglementaire de l'IA, dans le but de soutenir l'innovation dans le domaine de l'IA au sein de l'Union.

12. Les fournisseurs et les fournisseurs potentiels participant au bac à sable réglementaire de l'IA demeurent responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice infligé à des tiers en raison de l'expérimentation menée dans le bac à sable. Toutefois, sous réserve du respect par les fournisseurs potentiels du plan spécifique ainsi que des modalités de leur participation et de leur disposition à suivre de bonne foi les orientations fournies par l'«autorité nationale compétente, aucune amende administrative n'est infligée par les autorités en cas de violation du présent règlement. Lorsque d'autres autorités compétentes chargées d'autres dispositions du droit de l'Union et du droit national ont participé activement à la surveillance du système d'IA dans le bac à sable et ont fourni des orientations en matière de conformité, aucune amende administrative n'est infligée en ce qui concerne ces dispositions.

13. Les bacs à sable réglementaires de l'IA sont conçus et mis en œuvre de manière à faciliter, le cas échéant, la coopération transfrontière entre les autorités nationales compétentes.

14. Les autorités nationales compétentes coordonnent leurs activités et coopèrent dans le cadre du Comité IA.

15. Les autorités nationales compétentes informent le Bureau de l'IA et le Comité IA de la mise en place d'un bac à sable et peuvent leur demander un soutien et des orientations. Le Bureau de l'IA publie une liste des bacs à sable prévus et existants et la tient à jour afin d'encourager une plus grande interaction dans les bacs à sable réglementaires de l'IA et la coopération transfrontière.

16. Les autorités nationales compétentes présentent des rapports annuels au Bureau de l'IA et au Comité IA, dont le premier est élaboré dans un délai d'un an à compter de la mise en place du bac à sable réglementaire de l'IA, puis tous les ans jusqu'à son terme, et un rapport final. Ces rapports fournissent des informations sur les progrès et les résultats de la mise en œuvre de ces bacs à sable, y compris les bonnes pratiques,

les incidents, les enseignements et les recommandations concernant leur mise en place et, le cas échéant, sur l'application et la révision éventuelle du présent règlement, y compris ses actes délégués et actes d'exécution, et sur l'application d'autres dispositions législatives de l'Union contrôlés par les autorités compétentes dans le cadre du bac à sable. Les autorités nationales compétentes publient ces rapports annuels ou des résumés de ceux-ci en ligne. La Commission tient compte, s'il y a lieu, des rapports annuels dans l'exercice de ses tâches au titre du présent règlement.

17. La Commission développe une interface unique et spécifique contenant toutes les informations pertinentes relatives aux bacs à sable réglementaires de l'IA pour permettre aux parties prenantes d'interagir avec les bacs à sable réglementaires de l'IA et de s'informer auprès des autorités compétentes, ainsi que de demander des orientations non contraignantes sur la conformité de produits, services et modèles commerciaux innovants intégrant les technologies de l'IA, conformément à l'article 62, paragraphe 1, point c). La Commission assure une coordination proactive avec les autorités nationales compétentes, le cas échéant.

article 58
Modalités détaillées pour les bacs à sable réglementaires de l'IA et fonctionnement de ceux-ci

1. Afin d'éviter une fragmentation à travers l'Union, la Commission adopte des actes d'exécution précisant les modalités détaillées de mise en place, de développement, de mise en œuvre, d'exploitation et de surveillance des bacs à sable réglementaires de l'IA. Les actes d'exécution contiennent des principes communs sur les questions suivantes:

a) les critères d'éligibilité et de sélection pour la participation au bac à sable réglementaire de l'IA;

b) les procédures de demande, de surveillance, de sortie et d'expiration du bac à sable réglementaire de l'IA, ainsi que de participation à celui-ci, y compris le plan du bac à sable et le rapport de sortie;

c) les conditions applicables aux participants.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Les actes d'exécution visés au paragraphe 1 garantissent que:

a) les bacs à sable réglementaires de l'IA sont ouverts à tout fournisseur ou fournisseur potentiel d'un système d'IA qui remplit les critères d'éligibilité et de sélection, lesquels sont transparents et équitables, et que les autorités nationales compétentes informent les demandeurs de leur décision dans un délai de trois mois à compter de la demande;

b) que les bacs à sable réglementaires de l'IA permettent un accès étendu et égal et suivent la demande de participation; les fournisseurs et fournisseurs potentiels peuvent également soumettre des demandes en partenariat avec des déployeurs et d'autre tiers concernés;

cf. déployeurs

c) que les modalités détaillées pour les bacs à sable réglementaires de l'IA et les conditions relatives à ces derniers favorisent, dans toute la mesure du possible, la flexibilité permettant aux autorités nationales compétentes de mettre en place et d'exploiter leurs bacs à sable réglementaires de l'IA;

d) que l'accès aux bacs à sable réglementaires de l'IA est gratuit pour les PME, y compris les jeunes pousses, sans préjudice des coûts exceptionnels que les autorités nationales compétentes peuvent recouvrer de manière équitable et proportionnée;

e) qu'ils aident les fournisseurs et les fournisseurs potentiels, au moyen des acquis d'apprentissage des bacs à sable réglementaires de l'IA, à se conformer aux obligations d'évaluation de la conformité prévues par le présent règlement et à l'application volontaire des codes de conduite visés à l'article 95;

f) que les bacs à sable réglementaires de l'IA facilitent la participation d'autres acteurs pertinents au sein de l'écosystème de l'IA, tels que les organismes notifiés et les organisations de normalisation, les PME, y compris les jeunes pousses, les entreprises, les innovateurs, les installations d'expérimentation et d'essai, les laboratoires de recherche et d'expérimentation et les pôles européens d'innova-

tion numérique, les centres d'excellence, les chercheurs individuels, afin de permettre et de faciliter la coopération avec les secteurs public et privé;

g) que les procédures, processus et exigences administratives applicables en matière de demande, de sélection, de participation et de sortie dans le cadre du bac à sable réglementaires de l'IA sont simples, facilement compréhensibles et clairement communiqués afin de faciliter la participation des PME, y compris des jeunes pousses, disposant de capacités juridiques et administratives limitées, et sont rationalisés dans toute l'Union, afin d'éviter la fragmentation et de permettre que la participation à un bac à sable réglementaire de l'IA mis en place par un État membre ou par le Contrôleur européen de la protection des données soit mutuellement et uniformément reconnue et produise les mêmes effets juridiques dans l'ensemble de l'Union;

h) que la participation au bac à sable réglementaire de l'IA est limitée à une période adaptée à la complexité et à l'envergure du projet, qui peut être prolongée par l'«autorité nationale compétente;

i) que les bacs à sable réglementaire de l'IA facilitent le développement d'outils et d'infrastructures pour la mise à l'essai, l'étalonnage des performances, l'évaluation et l'explication des aspects des systèmes d'IA pertinents pour l'apprentissage réglementaire, tels que la précision, la solidité et la cybersécurité, ainsi que les mesures d'atténuation des risques d'atteinte aux droits fondamentaux et à la société au sens large.

3. Les fournisseurs potentiels dans les bacs à sable réglementaires de l'IA, en particulier les PME et les jeunes pousses, sont dirigés, le cas échéant, vers des services préalables au déploiement, tels que des orientations sur la mise en œuvre du présent règlement, et vers d'autres services à valeur ajoutée, tels que l'aide avec les documents de normalisation et la certification, les installations d'essai et d'expérimentation, les pôles européens d'innovation numérique et les centres d'excellence.

4. Lorsque les autorités nationales compétentes envisagent d'autoriser des essais en conditions réelles supervisés dans le cadre d'un bac à sable réglementaire de l'IA établi en vertu du présent article, elles conviennent spécifiquement des conditions de ces essais et, en particulier, des garanties appropriées avec les participants en vue de protéger les droits fondamentaux, la santé et la sécurité. Le cas échéant, elles coopèrent avec d'autres autorités nationales compétentes en vue d'assurer la cohérence des pratiques dans l'ensemble de l'Union.

article 59
Traitement ultérieur de données à caractère personnel en vue du développement de certains systèmes d'IA dans l'intérêt public dans le cadre du bac à sable réglementaire de l'IA

1. Dans le bac à sable réglementaire de l'IA, les données à caractère personnel collectées légalement à d'autres fins peuvent être traitées uniquement aux fins du développement, de l'entraînement et de la mise à l'essai de certains systèmes d'IA dans le bac à sable, lorsque l'ensemble des conditions suivantes sont remplies:

a) les systèmes d'IA sont développés pour préserver des intérêts publics importants par une autorité publique ou une autre personne physique ou morale et dans un ou plusieurs des domaines suivants:

   i) la sécurité publique et la santé publique, y compris la détection, le diagnostic, la prévention, le contrôle et le traitement des maladies ainsi que l'amélioration des systèmes de soins de santé;

   ii) un niveau élevé de protection et d'amélioration de la qualité de l'environnement, la protection de la biodiversité, la protection contre la pollution, les mesures de transition écologique et les mesures d'atténuation du changement climatique et d'adaptation à celui-ci;

   iii) la durabilité énergétique;

   iv) la sécurité et la résilience des systèmes de transport et de la mobilité, des infrastructures critiques et des réseaux de transport;

   v) l'efficacité et la qualité de l'administration publique et des services publics;

b) les données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au chapitre III, section 2, lorsque ces exigences ne peuvent être

satisfaites de manière efficace en traitant des données anonymisées, synthétiques ou autres à caractère non personnel;

c) il existe des mécanismes de suivi efficaces pour déterminer si des risques élevés pour les droits et les libertés des personnes concernées, visés à l'article 35 du règlement (UE) 2016/679 et à l'article 39 du règlement (UE) 2018/1725, sont susceptibles de survenir lors de l'expérimentation menée dans le cadre du bac à sable, ainsi que des mécanismes de réponse permettant d'atténuer rapidement ces risques et, au besoin, de faire cesser le traitement des données;

cf. RGPD art. 35

d) les données à caractère personnel à traiter dans le cadre du bac à sable se trouvent dans un environnement de traitement des données séparé, isolé et protégé sur le plan fonctionnel, placé sous le contrôle du fournisseur potentiel, et seules les personnes autorisées ont accès à ces données;

e) les fournisseurs ne peuvent en outre partager les données initialement collectées que conformément au droit de l'Union en matière de protection des données; aucune données à caractère personnel créée dans le bac à sable ne peut être partagée en dehors du bac à sable;

f) aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable ne débouche sur des mesures ou des décisions affectant les personnes concernées ni n'a d'incidence sur l'application des droits que leur confère le droit de l'Union en matière de protection des données à caractère personnel;

g) les données à caractère personnel traitées dans le cadre du bac à sable sont protégées par des mesures techniques et organisationnelles appropriées et supprimées une fois que la participation au bac à sable a cessé ou que la période de conservation de ces données à caractère personnel a expiré;

h) les registres du traitement des données à caractère personnel dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac à sable, sauf disposition contraire du droit de l'Union ou du droit national;

i) une description complète et détaillée du processus et de la justification de l'entraînement, de la mise à l'essai et de la validation du système d'IA est conservée avec les résultats des essais, et fait partie de la documentation technique visée à l'annexe IV;

j) un résumé succinct du projet d'IA développé dans le cadre du bac à sable, de ses objectifs et des résultats escomptés est publié sur le site web des autorités compétentes; cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

2. Aux fins de la prévention et de la détection d'infractions pénales, ainsi que des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sous le contrôle et la responsabilité des autorités répressives, le traitement des données à caractère personnel dans les bacs à sable réglementaires de l'IA est fondé sur une disposition spécifique du droit de l'Union ou du droit national et soumis aux mêmes conditions cumulatives que celles visées au paragraphe 1.

3. Le paragraphe 1 est sans préjudice du droit de l'Union ou du droit national excluant le traitement des données à caractère personnel à des fins autres que celles expressément mentionnées dans ce droit, ainsi que sans préjudice du droit de l'Union ou du droit national établissant le fondement du traitement des données à caractère personnel qui est nécessaire aux fins du développement, de la mise à l'essai et de l'entraînement de systèmes d'IA innovants, ou de toute autre base juridique, dans le respect du droit de l'Union relatif à la protection des données à caractère personnel.

article 60
Essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Les essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA peuvent être effectués par les fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque énumérés à l'annexe III, conformément au présent article et au plan d'essais en conditions réelles visé au présent article, sans préjudice des interdictions prévues à l'article 5.

La Commission précise, par voie d'actes d'exécution, les éléments détaillés du plan d'essais en conditions réelles. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Le présent paragraphe est sans préjudice du droit de l'Union ou du droit national relatif aux essais en conditions réelles de systèmes d'IA à haut risque liés aux produits qui relèvent de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

2. Les fournisseurs ou fournisseurs potentiels peuvent effectuer, seuls ou en partenariat avec un ou plusieurs déployeurs ou déployeurs potentiels, des essais des systèmes d'IA à haut risque visés à l'annexe III, en conditions réelles, à tout moment avant la mise sur le marché ou la mise en service du système d'IA concerné.

cf. déployeurs

3. Les essais de systèmes d'IA à haut risque en conditions réelles au titre du présent article sont sans préjudice de tout examen éthique exigé par le droit de l'Union ou le droit national.

4. Les fournisseurs ou fournisseurs potentiels ne peuvent effectuer les essais en conditions réelles que si toutes les conditions suivantes sont remplies:

a) le fournisseur ou le fournisseur potentiel a établi un plan d'essais en conditions réelles et l'a soumis à l'autorité de surveillance du marché dans l'État membre où les essais en conditions réelles doivent être réalisés;

b) l'autorité de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés a approuvé les essais en conditions réelles et le plan d'essais en conditions réelles; lorsque l'autorité de surveillance du marché n'a pas fourni de réponse dans un délai de 30 jours, les essais en conditions réelles et le plan d'essais en conditions réelles sont réputés approuvés; lorsque le droit national ne prévoit pas d'approbation tacite, les essais en conditions réelles restent soumis à autorisation;

c) le fournisseur ou fournisseur potentiel, à l'exception des fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, ainsi que des systèmes d'IA à haut risque visés à l'annexe III, point 2, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 71, paragraphe 4, avec un numéro d'identification unique à l'échelle de l'Union et les informations indiquées à l'annexe IX; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 49, paragraphe 4, point d), avec un numéro d'identification unique à l'échelle de l'Union et les informations y indiquées; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, point 2, a enregistré les essais en conditions réelles conformément à l'article 49, paragraphe 5.

d) le fournisseur ou fournisseur potentiel effectuant les essais en conditions réelles est établi dans l'Union ou a désigné un représentant légal établi dans l'Union;

e) les données collectées et traitées aux fins des essais en conditions réelles ne sont transférées vers des pays tiers qu'à condition que des garanties appropriées et applicables en vertu du droit de l'Union soient en place;

f) les essais en conditions réelles ne durent pas plus longtemps que nécessaire pour atteindre leurs objectifs et, en tout état de cause, pas plus de six mois, qui peuvent être prolongés pour une période supplémentaire de six mois, sous réserve d'une notification préalable par le fournisseur ou fournisseur potentiel à l'autorité de surveillance du marché, accompagnée d'une explication des raisons qui motivent une telle prolongation;

g) les participants aux essais en conditions réelles qui sont des personnes appartenant à des groupes vulnérables en raison de leur âge ou de leur handicap sont dûment protégées;

h) lorsqu'un fournisseur ou un fournisseur potentiel organise les essais en conditions réelles en coopération avec un ou plusieurs déployeurs ou déployeurs potentiels, ces derniers ont été préalablement informés de tous les aspects des

cf. déployeurs

essais qui sont pertinents pour leur décision de participer et ont reçu les instructions d'utilisation adéquates pour le système d'IA visé à l'article 13; le fournisseur ou fournisseur potentiel et le déployeur ou déployeur potentiel concluent un accord précisant leurs rôles et responsabilités en vue d'assurer le respect des dispositions relatives aux essais en conditions réelles prévues par le présent règlement et en vertu d'autres dispositions applicables du droit de l'Union et du droit national;

cf. déployeurs

i) les participants aux essais en conditions réelles ont donné leur consentement éclairé conformément à l'article 61 ou, dans le cas des services répressifs, lorsque la recherche d'un consentement éclairé empêcherait de réaliser les essais du système d'IA, les essais proprement dits et les résultats des essais en conditions réelles n'ont pas d'effet négatif sur les participants, et leurs données à caractère personnel sont supprimées une fois les essais réalisés;

j) le fournisseur ou le fournisseur potentiel ainsi que les déployeurs ou les déployeurs potentiels effectuent un contrôle effectif des essais en conditions réelles, par des personnes dûment qualifiées dans le domaine concerné et disposant des capacités, de la formation et de l'autorité nécessaires pour accomplir leurs tâches;

cf. déployeurs

k) les prévisions, recommandations ou décisions du système d'IA peuvent effectivement être infirmées et ignorées.

5. Tout participant aux essais en conditions réelles, ou son représentant légal, selon le cas, peut, sans encourir de préjudice et sans devoir se justifier, se retirer des essais à tout moment, en révoquant son consentement éclairé et peut demander la suppression immédiate et définitive de ses données à caractère personnel. Le retrait du consentement éclairé n'affecte pas les activités déjà menées.

6. Conformément à l'article 75, les États membres confèrent à leurs autorités de surveillance du marché le pouvoir d'exiger des fournisseurs et des fournisseurs potentiels qu'ils fournissent des informations, de procéder à des inspections inopinées à distance ou sur place et d'effectuer des vérifications concernant la réalisation des essais en conditions réelles et des systèmes d'IA à haut risque connexes. Les autorités de surveillance du marché utilisent ces pouvoirs pour veiller au développement sûr des essais en conditions réelles.

7. Tout incident grave constaté au cours des essais en conditions réelles est signalé à l'autorité nationale de surveillance du marché, conformément à l'article 73. Le fournisseur ou fournisseur potentiel adopte des mesures d'atténuation immédiates ou, à défaut, suspend les essais en conditions réelles jusqu'à ce que cette atténuation soit effective ou y met fin en l'absence d'atténuation. Le fournisseur ou fournisseur potentiel établit une procédure pour le rappel rapide du système d'IA lors de la cessation des essais en conditions réelles.

8. Les fournisseurs ou fournisseurs potentiels informent l'autorité nationale de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés de la suspension ou de la cessation des essais en conditions réelles et des résultats finaux.

9. Le fournisseur ou le fournisseur potentiel sont responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice causé durant les essais en conditions réelles.

article 61
Consentement éclairé à participer aux essais en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Aux fins des essais en conditions réelles visés à l'article 60, le consentement éclairé donné librement est obtenu des participants aux essais avant que ceux-ci ne prennent part à ces essais et après qu'ils ont été dûment informés au moyen d'informations concises, claires, pertinentes et compréhensibles concernant:

a) la nature et les objectifs des essais en conditions réelles ainsi que les désagréments éventuels pouvant être liés à sa participation;

b) les conditions dans lesquelles les essais en conditions réelles doivent être réalisés, y compris la durée prévue de la participation;

c) les droits et garanties concernant leur participation, en particulier leur droit de refuser de participer aux essais en conditions réelles et leur droit de s'en retirer à tout moment sans encourir de préjudice et sans devoir se justifier;

d) les modalités selon lesquelles il peut être demandé que des prévisions, recommandations ou décisions du système d'IA soient infirmées ou ignorées;

e) le numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles conformément à l'article 60, paragraphe 4, point c), et les coordonnées du fournisseur ou de son représentant légal auprès duquel des informations complémentaires peuvent être obtenues.

2. Le consentement éclairé est daté et documenté et une copie en est remise aux participants aux essais ou à leur représentant légal.

article 62
Mesures en faveur des fournisseurs et déployeurs, en particulier les PME, y compris les jeunes pousses

1. Les États membres:

a) accordent aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union, un accès prioritaire aux bacs à sable réglementaires de l'IA, dans la mesure où elles remplissent les conditions d'éligibilité et les critères de sélection; l'accès prioritaire n'empêche pas d'autres PME, y compris les jeunes pousses, autres que celles visées au présent alinéa, d'accéder au bac à sable réglementaire de l'IA, pour autant qu'elles remplissent également les conditions d'éligibilité et les critères de sélection;

b) organisent des activités spécifiques de sensibilisation et de formation à l'application du présent règlement, adaptées aux besoins des PME, y compris les jeunes pousses, les déployeurs et, si nécessaire, les pouvoirs publics locaux;

cf. déployeurs

c) utilisent des canaux privilégiés existants et, s'il y a lieu, en établissent de nouveaux avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, si nécessaire, les pouvoirs publics locaux, afin de fournir des conseils et de répondre aux questions relatives à la mise en œuvre du présent règlement, y compris en ce qui concerne la participation à des bacs à sable réglementaires de l'IA;

d) facilitent la participation des PME et d'autres parties concernées au processus d'élaboration de la normalisation.

2. Les intérêts et les besoins spécifiques des PME fournisseuses, y compris les jeunes pousses, sont pris en considération lors de la fixation des frais liés à l'évaluation de la conformité visée à l'article 43, ces frais étant réduits proportionnellement à leur taille, à la taille de leur marché et à d'autres indicateurs pertinents.

3. Le Bureau de l'IA:

a) fournit des modèles normalisés pour les domaines qui relèvent du présent règlement, comme précisé par le Comité IA dans sa demande;

b) met au point et tient à jour une plateforme d'information unique fournissant des informations faciles à utiliser en rapport avec le présent règlement pour tous les opérateurs dans l'ensemble de l'Union;

c) organise des campagnes de communication appropriées pour sensibiliser aux obligations découlant du présent règlement;

d) évalue et promeut la convergence des bonnes pratiques en matière de procédures de passation de marchés publics en ce qui concerne les systèmes d'IA.

article 63
Dérogations pour des opérateurs spécifiques

1. Les microentreprises au sens de la recommandation 2003/361/CE peuvent se conformer de manière simplifiée à certains éléments du système de gestion de la qualité requis par l'article 17 du présent règlement, pour autant qu'elles n'aient pas d'entreprises partenaires ou d'entreprises liées au sens de ladite recommandation. À cette fin, la Commission élabore des lignes directrices sur les éléments du système de gestion de la qualité qui peuvent être respectés de manière simplifiée en tenant compte

des besoins des microentreprises, sans affecter le niveau de protection ni la nécessité de se conformer aux exigences relatives aux systèmes d'IA à haut risque.

2. Le paragraphe 1 du présent article ne peut être interprété comme dispensant ces opérateurs de satisfaire à d'autres exigences ou obligations prévues par le présent règlement, y compris celles établies aux articles 9, 10, 11, 12, 13, 14, 15, 72 et 73.

CHAPITRE VII
GOUVERNANCE

Gouvernance

SECTION 1
Gouvernance au niveau de l'Union

article 64
Bureau de l'IA

1. La Commission développe l'expertise et les capacités de l'Union dans le domaine de l'IA par l'intermédiaire du Bureau de l'IA.

2. Les États membres facilitent l'accomplissement des tâches confiées au Bureau de l'IA, telles qu'elles sont définies dans le présent règlement.

article 65
Création et structure du Comité européen de l'intelligence artificielle

1. Un Comité européen de l'intelligence artificielle (ci-après dénommé « Comité IA») est créé.

2. Le Comité IA est composé d'un représentant par État membre. Le Contrôleur européen de la protection des données participe en qualité d'observateur. Le Bureau de l'IA assiste également aux réunions du Comité IA sans toutefois prendre part aux votes. D'autres autorités, organes ou experts nationaux et de l'Union peuvent être invités aux réunions par le Comité IA au cas par cas, lorsque les questions examinées relèvent de leurs compétences.

3. Chaque représentant est désigné par son État membre pour une période de trois ans, renouvelable une fois.

4. Les États membres veillent à ce que leurs représentants au sein du Comité IA:

a) disposent des compétences et pouvoirs pertinents dans leur État membre afin de contribuer activement à l'accomplissement des tâches du Comité IA visées à l'article 66;

b) soient désignés comme point de contact unique vis-à-vis du Comité IA et, lorsqu'il y a lieu, compte tenu des besoins des États membres, comme point de contact unique pour les parties prenantes;

c) soient habilités à faciliter la cohérence et la coordination entre les autorités nationales compétentes de leur État membre en ce qui concerne la mise en œuvre du présent règlement, y compris par la collecte de données et d'informations pertinentes aux fins de l'accomplissement de leurs tâches au sein du Comité IA.

5. Les représentants désignés des États membres adoptent le règlement intérieur du Comité IA à la majorité des deux tiers. Le règlement intérieur établit, en particulier, les procédures de sélection, la durée du mandat et les spécifications des missions du président, les modalités de vote détaillées et l'organisation des activités du Comité IA et de celles de ses sous-groupes.

6. Le Comité IA établit deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes au sujet des questions liées à la surveillance du marché et aux organismes notifiés respectivement.

Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020.

Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le cas échéant, des représentants du forum consultatif visé à l'article 67 peuvent être invités à ces sous-groupes ou à des réunions spécifiques de ces sous-groupes en qualité d'observateurs.

7. Le Comité IA est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités.

8. Le Comité IA est présidé par l'un des représentants des États membres. Le Bureau de l'IA assure le secrétariat du Comité IA, convoque les réunions à la demande du président et prépare l'ordre du jour conformément aux tâches du Comité IA au titre du présent règlement et à son règlement intérieur.

article 66
Tâches du Comité IA

Le Comité IA conseille et assiste la Commission et les États membres afin de faciliter l'application cohérente et efficace du présent règlement. À cette fin, le Comité IA peut notamment:

a) contribuer à la coordination entre les autorités nationales compétentes chargées de l'application du présent règlement et, en coopération avec les autorités de surveillance du marché concernées et sous réserve de leur accord, soutenir les activités conjointes des autorités de surveillance du marché visées à l'article 74, paragraphe 11;

b) recueillir l'expertise technique et réglementaire ainsi que les bonnes pratiques et les partager entre les États membres;

c) fournir des conseils sur la mise en œuvre du présent règlement, en particulier en ce qui concerne le contrôle de l'application des règles relatives aux modèles d'IA à usage général;

d) contribuer à l'harmonisation des pratiques administratives dans les États membres, y compris en ce qui concerne la dérogation à la procédure d'évaluation de la conformité visée à l'article 46, le fonctionnement des bacs à sable réglementaires de l'IA et les essais en conditions réelles visés aux articles 57, 59 et 60;

e) à la demande de la Commission ou de sa propre initiative, émettre des recommandations et des avis écrits sur toute question pertinente liée à la mise en œuvre du présent règlement et à son application cohérente et efficace, y compris:

   i) sur l'élaboration et l'application de codes de conduite et de codes de bonne pratique conformément au présent règlement, ainsi que des lignes directrices de la Commission;

   ii) sur l'évaluation et le réexamen du présent règlement conformément à l'article 112, y compris en ce qui concerne les signalements d'incidents graves visés à l'article 73, le fonctionnement de la base de données de l'UE visée à l'article 71, l'élaboration des actes délégués ou des actes d'exécution, ainsi que les alignements éventuels du présent règlement sur les dispositions d'harmonisation de la législation de l'Union figurant à l'annexe I;

   iii) sur les spécifications techniques ou les normes existantes se rapportant aux exigences énoncées au chapitre III, section 2;

   iv) sur l'utilisation des normes harmonisées ou des spécifications communes visées aux articles 40 et 41;

   v) sur les tendances, telles que la compétitivité mondiale de l'Europe dans le domaine de l'IA, l'adoption de l'IA dans l'Union et le développement des compétences numériques;

   vi) sur les tendances concernant l'évolution de la typologie des chaînes de valeur de l'IA, en particulier en ce qui concerne les conséquences qui en découlent en termes de responsabilité;

   vii) sur la nécessité éventuelle de modifier l'annexe III conformément à l'article 7, et sur la nécessité éventuelle d'une révision de l'article 5 confor-

mément à l'article 112, en tenant compte des éléments probants pertinents disponibles et des dernières évolutions technologiques;

f) soutenir la Commission afin de promouvoir la maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA;

g) faciliter l'élaboration de critères communs et d'une interprétation commune, entre les opérateurs du marché et les autorités compétentes, des concepts pertinents prévus par le présent règlement, y compris en contribuant au développement de critères de référence;

h) coopérer, lorsqu'il y a lieu, avec d'autres institutions, organes et organismes de l'Union, ainsi que des groupes d'experts et réseaux compétents de l'Union, en particulier dans les domaines de la sécurité des produits, de la cybersécurité, de la concurrence, des services numériques et des services de médias, des services financiers, de la protection des consommateurs, de la protection des données et des droits fondamentaux;

i) contribuer à une coopération efficace avec les autorités compétentes de pays tiers et des organisations internationales;

j) aider les autorités nationales compétentes et la Commission à développer l'expertise organisationnelle et technique nécessaire à la mise en œuvre du présent règlement, y compris en contribuant à l'évaluation des besoins de formation du personnel des États membres participant à la mise en œuvre du présent règlement;

k) aider le Bureau de l'IA à soutenir les autorités nationales compétentes dans la mise en place et le développement de bacs à sable réglementaires de l'IA, et faciliter la coopération et le partage d'informations entre les bacs à sable réglementaires de l'IA;

l) contribuer à l'élaboration de documents d'orientation et fournir des conseils pertinents en la matière;

m) conseiller la Commission sur les questions internationales en matière d'IA;

n) fournir des avis à la Commission sur les alertes qualifiées concernant les modèles d'IA à usage général;

o) recevoir des avis des États membres sur les alertes qualifiées concernant les modèles d'IA à usage général, ainsi que sur les expériences et pratiques nationales en matière de suivi et de contrôle de l'application des systèmes d'IA, en particulier des systèmes intégrant les modèles d'IA à usage général.

article 67
Forum consultatif

1. Un forum consultatif est créé pour fournir une expertise technique et conseiller le Comité IA et la Commission, ainsi que pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

2. La composition du forum consultatif est équilibrée en ce qui concerne la représentation des parties prenantes, y compris l'industrie, les jeunes pousses, les PME, la société civile et le monde universitaire. La composition du forum consultatif est équilibrée sur le plan des intérêts commerciaux et non commerciaux et, dans la catégorie des intérêts commerciaux, en ce qui concerne les PME et les autres entreprises.

3. La Commission nomme les membres du forum consultatif, conformément aux critères énoncés au paragraphe 2, parmi les parties prenantes possédant une expertise reconnue dans le domaine de l'IA.

4. La durée du mandat des membres du forum consultatif est de deux ans et peut être prolongée au maximum de quatre ans.

5. L'Agence des droits fondamentaux, l'ENISA, le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen de normalisation des télécommunications (ETSI) sont membres permanents du forum consultatif.

6. Le forum consultatif établit son règlement intérieur. Il élit parmi ses membres deux coprésidents, conformément aux critères énoncés au paragraphe 2. Leur mandat est d'une durée de deux ans, renouvelable une fois.

7. Le forum consultatif tient des réunions régulières au moins deux fois par an. Il peut inviter des experts et d'autres parties prenantes à ses réunions.

8. Le forum consultatif peut préparer des avis, des recommandations et des contributions écrites à la demande du Comité IA ou de la Commission.

9. Le forum consultatif peut créer des sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques liées aux objectifs du présent règlement.

10. Le forum consultatif prépare un rapport annuel sur ses activités. Ce rapport est rendu public.

article 68
Groupe scientifique d'experts indépendants

1. La Commission adopte, au moyen d'un acte d'exécution, des dispositions relatives à la constitution d'un groupe scientifique d'experts indépendants (ci-après dénommé «groupe scientifique») destiné à soutenir les activités de contrôle de l'application du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Le groupe scientifique est composé d'experts sélectionnés par la Commission en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA, nécessaire pour s'acquitter des tâches énoncées au paragraphe 3, et est en mesure de démontrer qu'ils remplissent toutes les conditions suivantes:

a) disposer d'une expertise et d'une compétence particulières ainsi que d'une expertise scientifique ou technique dans le domaine de l'IA;

b) être indépendant vis-à-vis de tout fournisseur de systèmes d'IA ou de modèles d'IA à usage général;

c) être capable de mener des activités avec diligence, précision et objectivité.

La Commission, en consultation avec le Comité IA, détermine le nombre d'experts au sein du groupe scientifique en fonction des besoins et veille à une représentation équitable entre les hommes et les femmes ainsi que sur le plan géographique.

3. Le groupe scientifique conseille et soutient le Bureau de l'IA, notamment en ce qui concerne les tâches suivantes:

a) soutenir la mise en œuvre et le contrôle de l'application du présent règlement en ce qui concerne les modèles et systèmes d'IA à usage général, en particulier:

   i) en alertant le Bureau de l'IA au sujet d'éventuels risques systémiques posés au niveau de l'Union par des modèles d'IA à usage général, conformément à l'article 90;

   ii) en contribuant à la mise au point d'outils et de méthodologies destinés à évaluer les capacités des modèles et systèmes d'IA à usage général, y compris au moyen de critères de référence;

   iii) en fournissant des conseils quant à la classification des modèles d'IA à usage général présentant un risque systémique;

   iv) en fournissant des conseils quant à la classification de différents modèles et systèmes d'IA à usage général;

   v) en contribuant à la mise au point d'outils et de modèles;

b) soutenir, à leur demande, les autorités de surveillance du marché dans leur travail;

c) soutenir les activités transfrontières de surveillance du marché visées à l'article 74, paragraphe 11, sans préjudice des pouvoirs des autorités de surveillance du marché;

d) soutenir le Bureau de l'IA dans l'exercice de ses fonctions dans le cadre de la procédure de sauvegarde de l'Union prévue à l'article 81.

4. Les experts du groupe scientifique s'acquittent de leurs tâches avec impartialité et objectivité, et garantissent la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Ils ne sollicitent ni n'acceptent d'instructions de quiconque dans l'exercice des tâches qui leur incombent en vertu du paragraphe 3. Chaque expert établit une déclaration d'intérêts qui est rendue publique. Le Bureau de l'IA met en place des systèmes et des procédures visant à prévenir et gérer efficacement les conflits d'intérêts potentiels.

5. L'acte d'exécution visé au paragraphe 1 comprend des dispositions sur les conditions, les procédures et les modalités détaillées permettant au groupe scientifique et à ses membres d'émettre des alertes et de demander l'assistance du Bureau de l'IA pour l'exécution des tâches du groupe scientifique.

article 69
Accès des États membres au groupe scientifique

1. Les États membres peuvent faire appel à des experts du groupe scientifique pour soutenir leurs activités de contrôle de l'application du présent règlement.

2. Les États membres peuvent être tenus de payer des honoraires pour les conseils et le soutien fournis par les experts. La structure et le niveau des honoraires ainsi que le barème et la structure des dépens récupérables sont définis dans l'acte d'exécution visé à l'article 68, paragraphe 1, en tenant compte des objectifs consistant à mettre en œuvre le présent règlement de façon appropriée, à assurer un bon rapport coût-efficacité et à garantir que tous les États membres aient un accès effectif à des experts.

3. La Commission facilite l'accès en temps utile des États membres aux experts, en fonction des besoins, et veille à ce que la combinaison des activités de soutien menées par les structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 84 et par les experts au titre du présent article soit organisée de manière efficace et apporte la meilleure valeur ajoutée possible.

SECTION 2
Autorités nationales compétentes

Autorités nationales compétentes

article 70
Désignation des autorités nationales compétentes et des points de contact uniques

1. Chaque État membre établit ou désigne en tant qu'autorités nationales compétentes au moins une autorité notifiante et au moins une autorité de surveillance du marché aux fins du présent règlement. Ces autorités nationales compétentes exercent leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver l'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités s'abstiennent de tout acte incompatible avec leurs fonctions. Pour autant que ces principes soient respectés, les activités et tâches précitées peuvent être exécutées par une ou plusieurs autorités désignées, en fonction des besoins organisationnels de l'État membre.

Les autorités compétentes sont, au moins :
- une autorité notifiante
- une autorité de surveillance du marché

2. Les États membres communiquent à la Commission les autorités notifiantes et les autorités de surveillance du marché désignées et les tâches incombant à ces autorités, ainsi que toute modification ultérieure y afférente. Les États membres rendent publiques des informations sur la manière dont les autorités compétentes et les points de contact uniques peuvent être contactés, par voie électronique, au plus tard le 2 août 2025. Les États membres désignent une autorité de surveillance du marché pour faire office de point de contact unique pour le présent règlement et communiquent à la Commission l'identité du point de contact unique. La Commission publie une liste des points de contact uniques.

3. Les États membres veillent à ce que leurs autorités nationales compétentes disposent de ressources techniques, financières et humaines suffisantes, ainsi que

d'infrastructures pour mener à bien efficacement les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'IA, des données et du traitement de données, de la protection des données à caractère personnel, de la cybersécurité, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en vigueur. Chaque année, les États membres évaluent et, si nécessaire, mettent à jour les exigences portant sur les compétences et les ressources visées au présent paragraphe.

4. Les autorités nationales compétentes prennent des mesures appropriées pour garantir un niveau adapté de cybersécurité.

5. Dans le cadre de l'accomplissement de leurs tâches, les autorités nationales compétentes agissent conformément aux obligations de confidentialité énoncées à l'article 78.

6. Au plus tard le 2 août 2025, et tous les deux ans par la suite, les États membres font rapport à la Commission sur l'état des ressources financières et humaines des autorités nationales compétentes, et lui présentent une évaluation de l'adéquation de ces ressources. La Commission transmet ces informations au Comité IA pour discussion et recommandations éventuelles.

7. La Commission facilite les échanges d'expériences entre les autorités nationales compétentes.

8. Les autorités nationales compétentes peuvent fournir des orientations et des conseils sur la mise en œuvre du présent règlement, en particulier aux PME, y compris les jeunes pousses, en tenant compte des orientations et conseils du Comité IA et de la Commission, selon le cas. Chaque fois que les autorités nationales compétentes envisagent de fournir des orientations et des conseils concernant un système d'IA dans des domaines relevant d'autres actes législatifs de l'Union, les autorités compétentes nationales en vertu de ces actes législatifs de l'Union sont consultées, le cas échéant.

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données agit en tant qu'autorité compétente responsable de leur surveillance.

CHAPITRE VIII
BASE DE DONNÉES DE L'UE POUR LES SYSTÈMES D'IA À HAUT RISQUE

Base de données des systèmes d'IA à haut risque

article 71
Base de données de l'UE pour les systèmes d'IA à haut risque énumérés à l'annexe III

1. La Commission, en collaboration avec les États membres, crée et tient à jour une base de données de l'UE contenant les informations visées aux paragraphes 2 et 3 du présent article en ce qui concerne les systèmes d'IA à haut risque visés à l'article 6, paragraphe 2, qui sont enregistrés conformément aux articles 49 et 60 et les systèmes d'IA qui ne sont pas considérés à haut risque en vertu de l'article 6, paragraphe 3, et qui sont enregistrés conformément à l'article 6, paragraphe 4, et à l'article 49. Lorsqu'elle définit les spécifications fonctionnelles de cette base de données, la Commission consulte les experts compétents et, lorsqu'elle les met à jour, elle consulte le Comité IA.

2. Les données énumérées à l'annexe VIII, sections A et B, sont introduites dans la base de données de l'UE par le fournisseur ou, le cas échéant, par le mandataire.

3. Les données énumérées à la section C de l'annexe VIII sont introduites dans la base de données de l'UE par le déployeur qui est ou agit pour le compte d'une autorité, d'une agence ou d'un organisme public, conformément à l'article 49, paragraphes 3 et 4.

4. À l'exception de la section visée à l'article 49, paragraphe 4, et à l'article 60, paragraphe 4, point c), les informations contenues dans la base de données de l'UE enregistrées conformément à l'article 49 sont accessibles et mises à la disposition du public d'une manière conviviale. Ces informations devraient être consultables grâce à une navigation aisée et lisibles par machine. Les informations enregistrées conformément à l'article 60 ne sont accessibles qu'aux autorités de surveillance du marché et à la Commission, sauf si le fournisseur ou fournisseur potentiel a donné son consentement pour que ces informations soient également accessibles au public.

5. La base de données de l'UE ne contient des données à caractère personnel que dans la mesure où celles-ci sont nécessaires à la collecte et au traitement d'informations conformément au présent règlement. Ces informations incluent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et légalement autorisées à représenter le fournisseur ou le déployeur, selon le cas.

cf. déployeurs

6. La Commission est la responsable du traitement pour la base de données de l'UE. Elle met à la disposition des fournisseurs, des fournisseurs potentiels et des déployeurs un soutien technique et administratif approprié. La base de données de l'UE est conforme aux exigences applicables en matière d'accessibilité.

CHAPITRE IX
SURVEILLANCE APRÈS COMMERCIALISATION, PARTAGE D'INFORMATIONS ET SURVEILLANCE DU MARCHÉ

Surveillance du marché

SECTION 1
Surveillance après commercialisation

article 72
Surveillance après commercialisation par les fournisseurs et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque

1. Les fournisseurs établissent et documentent un système de surveillance après commercialisation d'une manière qui soit proportionnée à la nature des technologies d'IA et des risques du système d'IA à haut risque.

2. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes qui peuvent être fournies par les déployeurs ou qui peuvent être collectées via d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur cycle de vie, et qui permettent au fournisseur d'évaluer si les systèmes d'IA respectent en permanence les exigences énoncées au chapitre III, section 2. Le cas échéant, la surveillance après commercialisation comprend une analyse de l'interaction avec d'autres systèmes d'IA. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs qui sont des autorités répressives.

cf. déployeurs

3. Le système de surveillance après commercialisation repose sur un plan de surveillance après commercialisation. Le plan de surveillance après commercialisation fait partie de la documentation technique visée à l'annexe IV. La Commission adopte un acte d'exécution fixant des dispositions détaillées établissant un modèle pour le plan de surveillance après commercialisation et la liste des éléments à inclure dans le plan au plus tard le 2 février 2026. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

4. Pour les systèmes d'IA à haut risque relevant de la législation d'harmonisation de l'Union énumérés à la section A de l'annexe I, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de ces actes, afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les éléments nécessaires décrits aux paragraphes 1, 2 et 3 en utilisant le modèle visé au paragraphe

3 dans les systèmes et plans existants au titre desdits actes, pour autant que cela donne lieu à un niveau de protection équivalent.

Le premier alinéa du présent paragraphe s'applique également aux systèmes d'IA à haut risque visés à l'annexe III, point 5, mis sur le marché ou mis en service par des établissements financiers qui sont soumis à des exigences en vertu de la législation de l'Union sur les services financiers concernant leur gouvernance, leurs dispositifs ou leurs processus internes.

SECTION 2
Partage d'informations sur les incidents graves

article 73
Signalement d'incidents graves

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave aux autorités de surveillance du marché des États membres dans lesquels cet incident s'est produit.

2. Le signalement visé au paragraphe 1 est effectué immédiatement après que le fournisseur a établi un lien de causalité, ou la probabilité raisonnable qu'un tel lien existe, entre le système d'IA et l'incident grave et, en tout état de cause, au plus tard 15 jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

cf. déployeurs

Le délai pour le signalement visé au premier alinéa tient compte de l'ampleur de l'incident grave.

3. Nonobstant le paragraphe 2 du présent article, en cas d'infraction de grande ampleur ou d'incident grave au sens de l'article 3, point 49), b), le signalement visé au paragraphe 1 du présent article est effectué immédiatement, et au plus tard deux jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de cet incident.

4. Nonobstant le paragraphe 2, en cas de décès d'une personne, le signalement est effectué immédiatement après que le fournisseur ou le déployeur a établi un lien de causalité entre le système d'IA à haut risque et l'incident grave ou dès qu'il soupçonne un tel lien, mais au plus tard 10 jours après la date à laquelle le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

cf. déployeurs

5. Si cela est nécessaire pour assurer un signalement en temps utile, le fournisseur ou, le cas échéant, le déployeur peut soumettre un signalement initial incomplet, suivi d'un signalement complet.

6. À la suite du signalement d'un incident grave en application du paragraphe 1, le fournisseur mène sans tarder les investigations nécessaires liées à l'incident grave et au système d'IA concerné. Ces investigations comprennent notamment une évaluation des risques résultant de l'incident, ainsi que des mesures correctives.

Le fournisseur coopère avec les autorités compétentes et, le cas échéant, avec l'organisme notifié concerné, au cours des investigations visées au premier alinéa, et ne mène aucune investigation nécessitant de modifier le système d'IA concerné d'une manière susceptible d'avoir une incidence sur toute évaluation ultérieure des causes de l'incident, avant d'informer les autorités compétentes de telles mesures.

7. Dès réception d'une notification relative à un incident grave visé à l'article 3, point 49) c), l'autorité de surveillance du marché compétente informe les autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1 du présent article. Ces orientations sont publiées au plus tard le 2 août 2025, et font l'objet d'une évaluation régulière.

8. L'autorité de surveillance du marché prend les mesures qui s'imposent, conformément à l'article 19 du règlement (UE) 2019/1020, dans un délai de sept jours à comp-

ter de la date à laquelle elle a reçu la notification visée au paragraphe 1 du présent article, et suit les procédures de notification prévues par ledit règlement.

9. Pour les systèmes d'IA à haut risque visés à l'annexe III qui sont mis sur le marché ou mis en service par des fournisseurs qui sont soumis à des instruments législatifs de l'Union établissant des obligations de signalement équivalentes à celles énoncées dans le présent règlement, la notification des incidents graves est limitée à ceux visés à l'article 3, point 49) c).

10. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, relevant des règlements (UE) 2017/745 et (UE) 2017/746, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 49) c), du présent règlement, et est adressée à l'«autorité nationale compétente choisie à cette fin par les États membres dans lesquels l'incident s'est produit.

11. Les autorités nationales compétentes notifient immédiatement à la Commission tout incident grave, qu'elles aient ou non pris des mesures à cet égard, conformément à l'article 20 du règlement (UE) 2019/1020.

SECTION 3
Contrôle de l'application

article 74
Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union

1. Le règlement (UE) 2019/1020 s'applique aux systèmes d'IA relevant du présent règlement. Aux fins du contrôle effectif de l'application du présent règlement:

a) toute référence à un opérateur économique en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les opérateurs identifiés à l'article 2, paragraphe 1, du présent règlement;

b) toute référence à un produit en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA relevant du champ d'application du présent règlement.

2. Dans le cadre des obligations d'information qui leur incombent en vertu de l'article 34, paragraphe 4, du règlement (UE) 2019/1020, les autorités de surveillance du marché communiquent chaque année à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence. Elles font également rapport chaque année à la Commission sur les recours aux pratiques interdites intervenus au cours de l'année concernée et sur les mesures prises.

3. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité responsable des activités de surveillance du marché désignée en vertu de ces actes juridiques.

Par dérogation au premier alinéa, et dans des circonstances appropriées, les États membres peuvent désigner une autre autorité compétente pour faire office d'autorité de surveillance du marché, à condition d'assurer la coordination avec les autorités sectorielles de surveillance du marché compétentes chargées du contrôle de l'application des actes juridiques énumérés à l'annexe I.

4. Les procédures visées aux articles 79 à 83 du présent règlement ne s'appliquent pas aux systèmes d'IA liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure la section A de l'annexe I, lorsque ces actes juridiques prévoient déjà des procédures assurant un niveau de protection équivalent et ayant le même objectif. En pareils cas, ce sont les procédures sectorielles pertinentes qui s'appliquent.

5. Sans préjudice des pouvoirs conférés aux autorités de surveillance du marché par l'article 14 du règlement (UE) 2019/1020, afin d'assurer le contrôle effectif de l'application du présent règlement, les autorités de surveillance du marché peuvent exercer les pouvoirs visés à l'article 14, paragraphe 4, points d) et j), dudit règlement à distance, le cas échéant.

6. Pour les systèmes d'IA à haut risque mis sur le marché, mis en service ou utilisés par des établissements financiers régis par la législation de l'Union sur les services financiers, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité nationale responsable de la surveillance financière de ces établissements en vertu de cette législation dans la mesure où la mise sur le marché, la mise en service ou l'utilisation du système d'IA est directement liée à la fourniture de ces services financiers.

7. Par dérogation au paragraphe 6, dans des circonstances appropriées, et pour autant que la coordination soit assurée, l'État membre peut désigner une autre autorité compétente comme autorité de surveillance du marché aux fins du présent règlement.

Les autorités nationales de surveillance du marché surveillant les établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) no 1024/2013, devraient communiquer sans tarder à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour les missions de surveillance prudentielle de la Banque centrale européenne définies dans ledit règlement.

8. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, du présent règlement, dans la mesure où ils sont utilisés à des fins répressives, de gestion des frontières et de justice et démocratie, et pour les systèmes d'IA à haut risque énumérés à l'annexe III, points 6, 7 et 8, du présent règlement, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes en matière de contrôle de la protection des données en vertu du règlement (UE) 2016/679 ou de la directive (UE) 2016/680, soit toute autre autorité désignée en application des mêmes conditions énoncées aux articles 41 à 44 de la directive (UE) 2016/680. Les activités de surveillance du marché ne portent en aucune manière atteinte à l'indépendance des autorités judiciaires ni n'interfèrent d'une autre manière avec leurs activités lorsque ces autorités agissent dans l'exercice de leurs fonctions judiciaires.

cf. RGPD

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données est leur autorité de surveillance du marché, sauf en ce qui concerne la Cour de justice de l'Union européenne agissant dans l'exercice de ses fonctions judiciaires.

10. Les États membres facilitent la coordination entre les autorités de surveillance du marché désignées en vertu du présent règlement et les autres autorités ou organismes nationaux compétents pour surveiller l'application de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou dans d'autres législations de l'Union, qui sont susceptibles d'être pertinents pour les systèmes d'IA à haut risque visés à l'annexe III.

11. Les autorités de surveillance du marché et la Commission sont en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener soit par les autorités de surveillance du marché, soit par les autorités de surveillance du marché conjointement avec la Commission, qui ont pour objectif de promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser ou de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont identifiés comme présentant un risque grave dans deux États membres ou plus conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA fournit une aide à la coordination des enquêtes conjointes.

12. Sans préjudice des pouvoirs prévus par le règlement (UE) 2019/1020, et lorsque cela est pertinent et limité à ce qui est nécessaire à l'accomplissement de leurs tâches, les fournisseurs accordent aux autorités de surveillance du marché un accès complet à la documentation ainsi qu'aux jeux de données d'entraînement, de validation et de test utilisés pour le développement des systèmes d'IA à haut risque, y compris, lorsque

cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'interfaces de programmation d'application (API) ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

13. Les autorités de surveillance du marché se voient accorder l'accès au code source du système d'IA à haut risque sur demande motivée et uniquement lorsque les deux conditions suivantes sont réunies:

a) l'accès au code source est nécessaire pour évaluer la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2; et

b) les procédures d'essai ou d'audit et les vérifications fondées sur les données et la documentation communiquées par le fournisseur ont été entièrement accomplies ou se sont révélées insuffisantes.

14. Toute information ou documentation obtenue par les autorités de surveillance du marché est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

article 75
Assistance mutuelle, surveillance du marché et contrôle des systèmes d'IA à usage général

1. Lorsqu'un système d'IA repose sur un modèle d'IA à usage général, et que le modèle et le système sont mis au point par le même fournisseur, le Bureau de l'IA est habilité à contrôler et surveiller la conformité de ce système d'IA avec les obligations prévues par le présent règlement. Pour s'acquitter de ses tâches de contrôle et de surveillance, le Bureau de l'IA dispose de tous les pouvoirs d'une autorité de surveillance du marché prévus dans la présente section et dans le règlement (UE) 2019/1020.

2. Lorsqu'elles ont des raisons suffisantes de considérer que des systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque en vertu du présent règlement ne sont pas conformes aux exigences énoncées dans le présent règlement, les autorités de surveillance du marché concernées coopèrent avec le Bureau de l'IA pour procéder à des évaluations de la conformité, et en informent le Comité IA et les autres autorités de surveillance du marché.

cf. déployeurs

3. Lorsqu'une autorité de surveillance du marché n'est pas en mesure de conclure son enquête sur le système d'IA à haut risque en raison de son incapacité à accéder à certaines informations relatives au modèle d'IA à usage général bien qu'elle ait déployé tous les efforts appropriés pour obtenir ces informations, elle peut présenter une demande motivée au Bureau de l'IA, par laquelle l'accès à ces informations est mis en œuvre. Dans ce cas, le Bureau de l'IA fournit sans tarder à l'autorité requérante, et en tout état de cause dans un délai de 30 jours, toute information qu'il juge pertinente pour déterminer si un système d'IA à haut risque est non conforme. Les autorités de surveillance du marché garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78 du présent règlement. La procédure prévue au chapitre VI du règlement (UE) 2019/1020 s'applique mutatis mutandis.

article 76
Supervision des essais en conditions réelles par les autorités de surveillance du marché

1. Les autorités de surveillance du marché ont les compétences et les pouvoirs nécessaires pour veiller à ce que les essais en conditions réelles soient conformes au présent règlement.

2. Lorsque des essais en conditions réelles sont effectués pour des systèmes d'IA supervisés dans un bac à sable réglementaire de l'IA en vertu de l'article 58, les autorités de surveillance du marché vérifient le respect de l'article 60 dans le cadre de leur rôle de surveillance du bac à sable réglementaire de l'IA. Ces autorités peuvent, lorsqu'il y a lieu, autoriser le fournisseur ou le fournisseur potentiel à effectuer les essais en conditions réelles, par dérogation aux conditions énoncées à l'article 60, paragraphe 4, points f) et g).

3. Lorsqu'une autorité de surveillance du marché a été informée d'un incident grave par le fournisseur potentiel, le fournisseur ou tout tiers, ou qu'elle a d'autres raisons de penser que les conditions énoncées aux articles 60 et 61 ne sont pas remplies, elle peut prendre l'une ou l'autre des décisions suivantes sur son territoire, selon le cas:

a) suspendre ou faire cesser les essais en conditions réelles;

b) exiger du fournisseur ou du fournisseur potentiel et du déployeur ou futur déployeur qu'ils modifient tout aspect des essais en conditions réelles.

cf. déployeurs

4. Lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3 du présent article, ou a formulé une objection au sens de l'article 60, paragraphe 4, point b), la décision ou l'objection est motivée et indique les modalités selon lesquelles le fournisseur ou le fournisseur potentiel peut contester la décision ou l'objection.

5. Le cas échéant, lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3, elle en communique les motifs aux autorités de surveillance du marché des autres États membres dans lesquels le système d'IA a été testé conformément au plan d'essais.

article 77
Pouvoirs des autorités de protection des droits fondamentaux

1. Les autorités ou organismes publics nationaux qui supervisent ou font respecter les obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, y compris le droit à la non-discrimination, en ce qui concerne l'utilisation des systèmes d'IA à haut risque visés à l'annexe III sont habilités à demander toute documentation créée ou conservée en vertu du présent règlement et à y avoir accès dans une langue et un format accessibles lorsque l'accès à cette documentation est nécessaire à l'accomplissement effectif de leur mandat dans les limites de leurs compétences. L'autorité ou l'organisme public concerné informe l'autorité de surveillance du marché de l'État membre concerné de toute demande de ce type.

2. Au plus tard le 2 novembre 2024, chaque État membre identifie les autorités ou organismes publics visés au paragraphe 1 et met la liste de ces autorités ou organismes à la disposition du public. Les États membres notifient la liste à la Commission et aux autres États membres, et tiennent cette liste à jour.

3. Lorsque la documentation visée au paragraphe 1 ne suffit pas pour déterminer s'il y a eu violation des obligations au titre du droit de l'Union protégeant les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 1 peut présenter à l'autorité de surveillance du marché une demande motivée visant à organiser des tests du système d'IA à haut risque par des moyens techniques. L'autorité de surveillance du marché organise les tests avec la participation étroite de l'autorité ou organisme public ayant présenté la demande dans un délai raisonnable après celle-ci.

4. Toute information ou documentation obtenue par les autorités ou organismes publics nationaux visés au paragraphe 1 du présent article en application des dispositions du présent article est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

article 78
Confidentialité

1. La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier:

a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil[57];

b) la mise en œuvre effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits;

c) les intérêts en matière de sécurité nationale et publique;

d) la conduite des procédures pénales ou administratives;

e) les informations classifiées en vertu du droit de l'Union ou du droit national.

2. Les autorités associées à l'application du présent règlement conformément au paragraphe 1 demandent uniquement les données qui sont strictement nécessaires à l'évaluation du risque posé par les systèmes d'IA et à l'exercice de leurs pouvoirs conformément au présent règlement et au règlement (UE) 2019/1020. Elles mettent en place des mesures de cybersécurité adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues, et suppriment les données collectées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues, conformément au droit de l'Union ou au droit national applicable.

3. Sans préjudice des paragraphes 1 et 2, les informations échangées à titre confidentiel entre les autorités nationales compétentes ou entre celles-ci et la Commission ne sont pas divulguées sans consultation préalable de l'«autorité nationale compétente dont elles émanent et du déployeur lorsque les systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, sont utilisés par les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile et lorsque cette divulgation risquerait de porter atteinte aux intérêts en matière de sécurité nationale et publique. Cet échange d'informations ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

cf. déployeurs

Lorsque les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile sont fournisseurs de systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, la documentation technique visée à l'annexe IV reste dans les locaux de ces autorités. Ces autorités veillent à ce que les autorités de surveillance du marché visées à l'article 74, paragraphes 8 et 9, selon le cas, puissent, sur demande, avoir immédiatement accès à la documentation ou en obtenir une copie. Seuls les membres du personnel de l'autorité de surveillance du marché disposant d'une habilitation de sécurité au niveau approprié sont autorisés à avoir accès à cette documentation ou à une copie de celle-ci.

4. Les paragraphes 1, 2 et 3 sont sans effet sur les droits ou obligations de la Commission, des États membres et de leurs autorités compétentes, ainsi que sur les droits ou obligations des organismes notifiés, en matière d'échange d'informations et de diffusion de mises en garde, y compris dans le contexte de la coopération transfrontière, et sur les obligations d'information incombant aux parties concernées en vertu du droit pénal des États membres.

5. La Commission et les États membres peuvent, lorsque cela est nécessaire et conformément aux dispositions pertinentes des accords internationaux et commerciaux, échanger des informations confidentielles avec les autorités de réglementation de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de confidentialité approprié.

article 79
Procédure applicable au niveau national aux systèmes d'IA présentant un risque

1. On entend par systèmes d'IA présentant un risque, un «produit présentant un risque» au sens de l'article 3, point 19), du règlement (UE) 2019/1020, dans la mesure où ils présentent des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes.

2. Lorsque l'autorité de surveillance du marché d'un État membre a des raisons suffisantes de considérer qu'un système d'IA présente un risque au sens du paragraphe 1

57. Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

du présent article, elle procède à une évaluation de la conformité du système d'IA concerné avec l'ensemble des exigences et obligations énoncées dans le présent règlement. Une attention particulière est accordée aux systèmes d'IA présentant un risque pour les groupes vulnérables. Lorsque sont identifiés des risques pour les droits fondamentaux, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux concernés visés à l'article 77, paragraphe 1, et coopère pleinement avec eux. Les opérateurs concernés coopèrent, en tant que de besoin, avec l'autorité de surveillance du marché et avec les autres autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1.

Si, au cours de cette évaluation, l'autorité de surveillance du marché ou, le cas échéant, l'autorité de surveillance du marché en coopération avec l'autorité publique nationale visée à l'article 77, paragraphe 1, constate que le système d'IA ne respecte pas les exigences et obligations énoncées dans le présent règlement, elle invite sans retard injustifié l'opérateur concerné à prendre toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, le retirer du marché ou le rappeler dans un délai qu'elle peut prescrire, et en tout état de cause au plus tard dans les 15 jours ouvrables, ou dans un délai prévu par la législation d'harmonisation de l'Union concernée, le délai le plus court étant retenu.

L'autorité de surveillance du marché informe l'organisme notifié concerné en conséquence. L'article 18 du règlement (UE) 2019/1020 s'applique aux mesures visées au deuxième alinéa du présent paragraphe.

3. Lorsque l'autorité de surveillance du marché considère que la non-conformité n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées de l'opérateur.

4. L'opérateur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.

5. Lorsque l'opérateur d'un système d'IA ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2, l'autorité de surveillance du marché prend toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du système d'IA sur son marché national ou sa mise en service, pour retirer le produit ou le système d'IA autonome de ce marché ou pour le rappeler. L'autorité notifie ces mesures sans retard injustifié à la Commission et aux autres États membres.

6. La notification visée au paragraphe 5 contient toutes les précisions disponibles, notamment les informations nécessaires pour identifier le système d'IA non conforme, son origine et la chaîne d'approvisionnement, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur concerné. En particulier, l'autorité de surveillance du marché indique si la non-conformité découle d'une ou plusieurs des causes suivantes:

a) le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5;

b) le non-respect, par le système d'IA à haut risque, des exigences énoncées au chapitre III, section 2;

c) des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 qui confèrent une présomption de conformité;

d) le non-respect de l'article 50.

7. Les autorités de surveillance du marché autres que l'autorité de surveillance du marché de l'État membre qui a entamé la procédure informent sans retard injustifié la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception de la notification visée au paragraphe 5, aucune objection n'a été émise par une autorité de surveillance du marché d'un État membre ou par la Commission à l'encontre d'une mesure provisoire prise

par une autorité de surveillance du marché d'un autre État membre, cette mesure est réputée justifiée. Cette disposition est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020. Le délai de trois mois visé au présent paragraphe est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 du présent règlement.

9. Les autorités de surveillance du marché veillent à ce que les mesures restrictives appropriées soient prises sans retard injustifié à l'égard du produit ou du système d'IA concerné, par exemple son retrait de leur marché.

article 80
Procédure applicable aux systèmes d'IA classés par le fournisseur comme n'étant pas à haut risque en application de l'annexe III

1. Lorsqu'une autorité de surveillance du marché a des raisons suffisantes de considérer qu'un système d'IA classé par le fournisseur comme n'étant pas à haut risque en application de l'article 6, paragraphe 3, est en réalité à haut risque, elle procède à une évaluation du système d'IA concerné quant à la question de sa classification en tant que système d'IA à haut risque sur la base des conditions énoncées à l'article 6, paragraphe 3, et dans les lignes directrices de la Commission.

2. Lorsque, au cours de cette évaluation, l'autorité de surveillance du marché constate que le système d'IA concerné est à haut risque, elle demande sans retard injustifié au fournisseur concerné de prendre toutes les mesures nécessaires pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement, ainsi que de prendre les mesures correctives appropriées dans un délai que l'autorité de surveillance du marché peut prescrire.

3. Lorsque l'autorité de surveillance du marché considère que l'utilisation du système d'IA concerné n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées du fournisseur.

4. Le fournisseur veille à ce que toutes les mesures nécessaires soient prises pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement. Lorsque le fournisseur d'un système d'IA concerné ne met pas le système d'IA en conformité avec ces exigences et obligations dans le délai visé au paragraphe 2 du présent article, il fait l'objet d'amendes conformément à l'article 99.

5. Le fournisseur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.

6. Lorsque le fournisseur du système d'IA concerné ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2 du présent article, l'article 79, paragraphe 5 à 9, s'applique.

7. Lorsque, au cours de l'évaluation prévue au paragraphe 1 du présent article, l'autorité de surveillance du marché établit que le système d'IA a été classé à tort par le fournisseur comme n'étant pas à haut risque afin de contourner l'application des exigences figurant au chapitre III, section 2, le fournisseur fait l'objet d'amendes conformément à l'article 99.

8. Dans l'exercice de leur pouvoir de contrôle de l'application du présent article, et conformément à l'article 11 du règlement (UE) 2019/1020, les autorités de surveillance du marché peuvent effectuer des contrôles appropriés, en tenant compte notamment des informations stockées dans la base de données de l'UE visée à l'article 71 du présent règlement.

article 81
Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 79, paragraphe 5, ou dans un délai de 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, l'autorité de surveillance du marché d'un État membre soulève des objections à l'encontre d'une mesure prise par

une autre autorité de surveillance du marché, ou que la Commission estime que cette mesure est contraire au droit de l'Union, la Commission entame sans retard injustifié des consultations avec l'autorité de surveillance du marché de l'État membre concerné et le ou les opérateurs, et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission, dans un délai de six mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, à compter de la notification visée à l'article 79, paragraphe 5, décide si la mesure nationale est justifiée ou non et communique sa décision à l'autorité de surveillance du marché de l'État membre concerné. La Commission informe également toutes les autres autorités de surveillance du marché de sa décision.

2. Lorsque la Commission estime que la mesure prise par l'État membre concerné est justifiée, tous les États membres veillent à prendre des mesures restrictives appropriées à l'égard du système d'IA concerné, par exemple en exigeant le retrait du système d'IA de leur marché sans retard injustifié, et en informent la Commission. Lorsque la Commission estime que la mesure nationale n'est pas justifiée, l'État membre concerné retire la mesure et en informe la Commission.

3. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du système d'IA est attribuée à des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 du présent règlement, la Commission applique la procédure prévue à l'article 11 du règlement (UE) no 1025/2012.

article 82
Systèmes d'IA conformes qui présentent un risque

1. Lorsque, ayant réalisé une évaluation au titre de l'article 79, après avoir consulté l'autorité publique nationale concernée visée à l'article 77, paragraphe 1, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un système d'IA à haut risque soit conforme au présent règlement, il comporte néanmoins un risque pour la santé ou la sécurité des personnes, pour les droits fondamentaux, ou pour d'autres aspects relatifs à la protection de l'intérêt public, elle demande à l'opérateur concerné de prendre toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, une fois mis sur le marché ou mis en service, ne présente plus ce risque, et ce sans retard injustifié, dans un délai qu'elle peut prescrire.

2. Le fournisseur ou autre opérateur concerné s'assure que des mesures correctives sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union dans le délai prescrit par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

3. Les États membres informent immédiatement la Commission et les autres États membres d'une constatation au titre du paragraphe 1. Les informations fournies incluent toutes les précisions disponibles, notamment les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement de ce système d'IA, la nature du risque encouru, ainsi que la nature et la durée des mesures nationales prises.

4. La Commission entame sans retard injustifié des consultations avec les États membres concernés et les opérateurs concernés, et évalue les mesures nationales prises. En fonction des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, si nécessaire, propose d'autres mesures appropriées.

5. La Commission communique immédiatement sa décision aux États membres concernés ainsi qu'aux opérateurs concernés. Elle en informe également les autres États membres.

article 83
Non-conformité formelle

1. Lorsque l'autorité de surveillance du marché d'un État membre fait l'une des constatations ci-après, elle invite le fournisseur concerné à mettre un terme à la non-conformité en question, dans un délai qu'elle peut prescrire:

a) le marquage CE a été apposé en violation de l'article 48;

b) le marquage CE n'a pas été apposé;

c) la déclaration UE de conformité visée à l'article 47 n'a pas été établie;

d) la déclaration UE de conformité visée à l'article 47 n'a pas été établie correctement;

e) l'enregistrement dans la base de données de l'UE visée à l'article 71 n'a pas été effectué;

f) le cas échéant, il n'a pas été désigné de mandataire;

g) la documentation technique n'est pas disponible.

2. Si le cas de non-conformité visé au paragraphe 1 persiste, l'autorité de surveillance du marché de l'État membre concerné prend toutes les mesures appropriées et proportionnées pour restreindre ou interdire la mise à disposition du système d'IA à haut risque sur le marché ou pour assurer son rappel ou son retrait sans tarder du marché.

article 84
Structures de soutien de l'Union pour les essais en matière d'IA

1. La Commission désigne une ou plusieurs structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 21, paragraphe 6, du règlement (UE) 2019/1020 dans le domaine de l'intelligence artificielle.

2. Sans préjudice des tâches visées au paragraphe 1, les structures de soutien de l'Union pour les essais en matière d'IA fournissent également des avis techniques ou scientifiques indépendants à la demande du Comité IA, de la Commission ou des autorités de surveillance du marché.

SECTION 4
Voies de recours

article 85
Droit d'introduire une réclamation auprès d'une autorité de surveillance du marché

Sans préjudice d'autres recours administratifs ou judiciaires, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement peut déposer des réclamations auprès de l'autorité de surveillance du marché concernée.

Conformément au règlement (UE) 2019/1020, ces réclamations sont prises en compte aux fins de l'exercice des activités de surveillance du marché, et sont traitées conformément aux procédures spécifiques établies en conséquence par les autorités de surveillance du marché.

article 86
Droit à l'explication des décisions individuelles

1. Toute personne concernée faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système d'IA à haut risque mentionné à l'annexe III, à l'exception des systèmes énumérés au point 2 de ladite annexe, et qui produit des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux a le droit d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise.

cf. déployeurs

2. Le paragraphe 1 ne s'applique pas à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions à l'obligation prévue audit paragraphe découlent du droit de l'Union ou du droit national dans le respect du droit de l'Union.

3. Le présent article ne s'applique que dans la mesure où le droit visé au paragraphe 1 n'est pas prévu par ailleurs dans le droit de l'Union.

article 87
Signalement de violations et protection des auteurs de signalement

La directive (UE) 2019/1937 s'applique aux signalements de violations du présent règlement et à la protection des personnes signalant ces violations.

SECTION 5
Surveillance, enquêtes, contrôle de l'application et contrôle en ce qui concerne les fournisseurs de modèles d'IA à usage général

article 88
Contrôle de l'exécution des obligations incombant aux fournisseurs de modèles d'IA à usage général

1. La Commission dispose de pouvoirs exclusifs pour surveiller et contrôler le respect du chapitre V, en tenant compte des garanties procédurales prévues à l'article 94. La Commission confie l'exécution de ces tâches au Bureau de l'IA, sans préjudice des pouvoirs d'organisation dont elle dispose ainsi que de la répartition des compétences entre les États membres et l'Union fondée sur les traités.

2. Sans préjudice de l'article 75, paragraphe 3, les autorités de surveillance du marché peuvent demander à la Commission d'exercer les pouvoirs prévus dans la présente section, lorsque cela est nécessaire et proportionné pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

article 89
Mesures de contrôle

1. Aux fins de l'exécution des tâches qui lui sont conférées dans le cadre de la présente section, le Bureau de l'IA peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs de modèles d'IA à usage général, y compris leur adhésion à des codes de bonne pratique approuvés.

2. Les fournisseurs en aval ont le droit d'introduire une réclamation pour violation du présent règlement. La réclamation est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné;

b) une description des faits pertinents, les dispositions concernées du présent règlement et la raison pour laquelle le fournisseur en aval considère que le fournisseur du modèle d'IA à usage général concerné a enfreint le présent règlement;

c) toute autre information que le fournisseur en aval qui a envoyé la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

article 90
Alertes de risques systémiques données par le groupe scientifique

1. Le groupe scientifique peut adresser une alerte qualifiée au Bureau de l'IA lorsqu'il a des raisons de soupçonner:

a) qu'un modèle d'IA à usage général présente un risque concret identifiable au niveau de l'Union; ou

b) qu'un modèle d'IA à usage général satisfait aux conditions visées à l'article 51.

2. À la suite d'une telle alerte qualifiée, la Commission, par l'intermédiaire du Bureau de l'IA et après en avoir informé le Comité IA, peut exercer les pouvoirs prévus à la présente section aux fins de l'évaluation de la question. Le Bureau de l'IA informe le Comité IA de toute mesure prise conformément aux articles 91 à 94.

3. L'alerte qualifiée est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné présentant un risque systémique;

b) une description des faits pertinents et les motifs de l'alerte donnée par le groupe scientifique;

c) toute autre information que le groupe scientifique juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

article 91
Pouvoir de demander de la documentation et des informations

1. La Commission peut demander au fournisseur du modèle d'IA à usage général concerné de fournir la documentation établie par le fournisseur conformément aux articles 53 et 55, ou toute information supplémentaire nécessaire pour évaluer la conformité du fournisseur avec le présent règlement.

2. Avant d'envoyer la demande d'informations, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Sur demande dûment motivée du groupe scientifique, la Commission peut adresser une demande d'informations au fournisseur d'un modèle d'IA à usage général, lorsque l'accès à ces informations est nécessaire et proportionné pour l'accomplissement des tâches du groupe scientifique au titre de l'article 68, paragraphe 2.

4. La demande d'informations mentionne la base juridique et l'objet de la demande, précise quelles informations sont requises, fixe un délai dans lequel les informations doivent être fournies, et indique les amendes prévues à l'article 101 en cas de fourniture d'informations inexactes, incomplètes ou trompeuses.

5. Le fournisseur du modèle d'IA à usage général concerné, ou son représentant, fournit les informations demandées. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas de personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts fournissent les informations demandées pour le compte du fournisseur du modèle d'IA à usage général concerné. Les avocats dûment habilités à agir peuvent fournir des informations pour le compte de leurs clients. Les clients demeurent néanmoins pleinement responsables si les informations fournies sont incomplètes, inexactes ou trompeuses.

article 92
Pouvoir de procéder à des évaluations

1. Le Bureau de l'IA, après consultation du Comité IA, peut procéder à des évaluations du modèle d'IA à usage général concerné:

a) pour évaluer le respect, par le fournisseur, des obligations prévues par le présent règlement, lorsque les informations recueillies en vertu de l'article 91 sont insuffisantes; ou

b) pour enquêter sur les risques systémiques, au niveau de l'Union, des modèles d'IA à usage général présentant un risque systémique, en particulier à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a).

2. La Commission peut décider de désigner des experts indépendants chargés de procéder à des évaluations pour son compte, y compris des experts du groupe scientifique établi en vertu de l'article 68. Les experts indépendants désignés pour cette tâche satisfont aux critères énoncés à l'article 68, paragraphe 2.

3. Aux fins du paragraphe 1, la Commission peut demander l'accès au modèle d'IA à usage général concerné par l'intermédiaire d'API ou d'autres moyens et outils techniques appropriés, y compris le code source.

4. La demande d'accès indique la base juridique, l'objet et les motifs de la demande et fixe le délai dans lequel l'accès doit être accordé, ainsi que les amendes prévues à l'article 101 en cas de non-fourniture de l'accès.

5. Les fournisseurs du modèle d'IA à usage général concerné ou son représentant fournissent les informations requises. Dans le cas de personnes morales, d'entreprises

ou de sociétés, ou lorsque le fournisseur n'a pas la personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts, accordent l'accès demandé pour le compte du fournisseur du modèle d'IA à usage général concerné.

6. La Commission adopte des actes d'exécution établissant les modalités détaillées et les conditions des évaluations, y compris les modalités détaillées d'intervention d'experts indépendants, et la procédure relative à leur sélection. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Avant de demander l'accès au modèle d'IA à usage général concerné, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général afin de recueillir davantage d'informations sur les essais internes du modèle, les garanties internes visant à prévenir les risques systémiques, ainsi que d'autres procédures internes et les mesures que le fournisseur a prises pour atténuer ces risques.

article 93
Pouvoir de demander des mesures

1. Lorsque cela est nécessaire et approprié, la Commission peut demander aux fournisseurs:

a) de prendre les mesures appropriées pour se conformer aux obligations énoncées à aux articles 53 et 54;

b) de mettre en œuvre des mesures d'atténuation, lorsque l'évaluation effectuée conformément à l'article 92 a suscité des préoccupations sérieuses et fondées quant à un risque systémique au niveau de l'Union;

c) de restreindre la mise à disposition du modèle sur le marché, de le retirer ou de le rappeler.

2. Avant qu'une mesure ne soit demandée, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Si, au cours du dialogue structuré visé au paragraphe 2, le fournisseur du modèle d'IA à usage général présentant un risque systémique s'engage à mettre en œuvre des mesures d'atténuation pour faire face à un risque systémique au niveau de l'Union, la Commission peut, par une décision, rendre ces engagements contraignants et déclarer qu'il n'y a plus lieu d'agir.

article 94
Droits procéduraux des opérateurs économiques du modèle d'IA à usage général

L'article 18 du règlement (UE) 2019/1020 s'applique mutatis mutandis aux fournisseurs du modèle d'IA à usage général, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

CHAPITRE X
CODES DE CONDUITE ET LIGNES DIRECTRICES

Codes de conduites et lignes directrices

article 95
Codes de conduite pour l'application volontaire de certaines exigences

1. Le Bureau de l'IA et les États membres encouragent et facilitent l'élaboration de codes de conduite, comportant des mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire, aux systèmes d'IA autres que les systèmes d'IA à haut risque, de tout ou partie des exigences énoncées au chapitre III, section 2, en tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur permettant l'application de ces exigences.

2. Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les systèmes d'IA, sur la base d'objectifs clairs et d'indica-

cf. déployeurs

teurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres:

a) les éléments applicables prévus dans les lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance;

b) l'évaluation et la réduction au minimum de l'incidence des systèmes d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA;

c) la promotion de la maîtrise de l'IA, en particulier chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA;

d) la facilitation d'une conception inclusive et diversifiée des systèmes d'IA, notamment par la mise en place d'équipes de développement inclusives et diversifiées et la promotion de la participation des parties prenantes à ce processus;

e) l'évaluation et la prévention de l'impact négatif des systèmes d'IA sur les personnes ou groupes de personnes vulnérables, y compris en ce qui concerne l'accessibilité pour les personnes handicapées, ainsi que sur l'égalité de genre.

3. Les codes de conduite peuvent être élaborés par des fournisseurs ou déployeurs individuels de systèmes d'IA ou par des organisations les représentant ou par les deux, y compris avec la participation de toute partie intéressée et de leurs organisations représentatives, y compris des organisations de la société civile et le monde universitaire. Les codes de conduite peuvent porter sur un ou plusieurs systèmes d'IA, compte tenu de la similarité de la destination des systèmes concernés.

cf. déployeurs

4. Le Bureau de l'IA et les États membres prennent en considération les intérêts et les besoins spécifiques des PME, y compris les jeunes pousses, lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

article 96
Lignes directrices de la Commission sur la mise en œuvre du présent règlement

1. La Commission élabore des lignes directrices sur la mise en œuvre pratique du présent règlement, et en particulier sur:

a) l'application des exigences et obligations visées aux articles 8 à 15 et à l'article 25;

b) les pratiques interdites visées à l'article 5;

c) la mise en œuvre pratique des dispositions relatives aux modifications substantielles;

d) la mise en œuvre pratique des obligations de transparence prévues à l'article 50;

e) des informations détaillées sur la relation entre le présent règlement et la législation d'harmonisation de l'Union dont la liste figure à l'annexe I ainsi que d'autres actes législatifs pertinents de l'Union, y compris en ce qui concerne la cohérence de leur application;

f) l'application de la définition d'un système d'IA telle qu'elle figure à l'article 3, point 1).

Lorsqu'elle publie ces lignes directrices, la Commission accorde une attention particulière aux besoins des PME, y compris les jeunes pousses, des pouvoirs publics locaux et des secteurs les plus susceptibles d'être affectés par le présent règlement.

Les lignes directrices visées au premier alinéa du présent paragraphe tiennent dûment compte de l'état de la technique généralement reconnu en matière d'IA, ainsi que des normes harmonisées et spécifications communes pertinentes visées aux articles 40 et 41, ou des normes harmonisées ou spécifications techniques qui sont énoncées en vertu de la législation d'harmonisation de l'Union.

2. À la demande des États membres ou du Bureau de l'IA, ou de sa propre initiative, la Commission met à jour les lignes directrices précédemment adoptées lorsque cela est jugé nécessaire.

CHAPITRE XI
DÉLÉGATION DE POUVOIR ET PROCÉDURE DE COMITÉ

Délégation de pouvoir - Comité

article 97
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, est conféré à la Commission pour une durée de cinq ans à partir du 1er août 2024. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 6, paragraphe 6 ou 7, de l'article 7, paragraphe 1 ou 3, de l'article 11, paragraphe 3, de l'article 43, paragraphe 5 ou 6, de l'article 47, paragraphe 5, de l'article 51, paragraphe 3, de l'article 52, paragraphe 4, ou de l'article 53, paragraphe 5 ou 6, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

article 98
Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

CHAPITRE XII
SANCTIONS

sanctions

article 99
Sanctions

1. Conformément aux conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions et autres mesures d'exécution, qui

peuvent également comprendre des avertissements et des mesures non monétaires, applicables aux violations du présent règlement commises par des opérateurs, et prennent toute mesure nécessaire pour veiller à la mise en œuvre correcte et effective de ces sanctions, tenant ainsi compte des lignes directrices publiées par la Commission en vertu de l'article 96. Ces sanctions doivent être effectives, proportionnées et dissuasives. Elles tiennent compte des intérêts des PME, y compris les jeunes pousses, et de leur viabilité économique.

2. Les États membres informent la Commission, sans retard et au plus tard à la date d'entrée en application, du régime des sanctions et des autres mesures d'exécution visées au paragraphe 1, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'amendes administratives pouvant aller jusqu'à 35 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

4. La non-conformité avec l'une quelconque des dispositions suivantes relatives aux opérateurs ou aux organismes notifiés, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu:

a) les obligations incombant aux fournisseurs en vertu de l'article 16;

b) les obligations incombant aux mandataires en vertu de l'article 22;

c) les obligations incombant aux importateurs en vertu de l'article 23;

d) les obligations incombant aux distributeurs en vertu de l'article 24;

e) les obligations incombant aux déployeurs en vertu de l'article 26;

cf. déployeurs

f) les exigences et obligations applicables aux organismes notifiés en application de l'article 31, de l'article 33, paragraphes 1, 3 et 4, ou de l'article 34;

g) les obligations de transparence pour les fournisseurs et les déployeurs conformément à l'article 50.

cf. déployeurs

5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 7 500 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

6. Dans le cas des PME, y compris les jeunes pousses, chaque amende visée au présent article s'élève au maximum aux pourcentages ou montants visés aux paragraphes 3, 4 et 5, le chiffre le plus faible étant retenu.

7. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et, le cas échéant, il est tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné, ainsi que, le cas échéant, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour la même violation;

c) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités au même opérateur pour des violations d'autres dispositions du droit de l'Union ou du droit national, lorsque ces violations résultent de la même activité ou omission constituant une violation pertinente au sens du présent règlement;

d) la taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet la violation;

e) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation;

f) le degré de coopération établi avec les autorités nationales compétentes en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

g) le degré de responsabilité de l'opérateur, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

h) la manière dont les autorités nationales compétentes ont eu connaissance de la violation, notamment si, et dans quelle mesure, l'opérateur a notifié la violation;

i) le fait que la violation a été commise délibérément ou par négligence;

j) toute mesure prise par l'opérateur pour atténuer le préjudice subi par les personnes concernées.

8. Chaque État membre établit les règles déterminant dans quelle mesure des amendes administratives peuvent être imposées à des autorités et organismes publics établis sur son territoire.

9. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes sont imposées par les juridictions nationales compétentes ou par d'autres organismes, selon le cas prévu dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

10. L'exercice des pouvoirs conférés par le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit national, y compris des recours juridictionnels effectifs et une procédure régulière.

11. Les États membres font rapport chaque année à la Commission sur les amendes administratives qu'ils ont infligées au cours de l'année concernée, conformément au présent article, ainsi que sur toute action en justice ou procédure judiciaire connexe.

article 100
Amendes administratives imposées aux institutions, organes et organismes de l'Union

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions, organes et organismes de l'Union relevant du champ d'application du présent règlement. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et il est dûment tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné ainsi que, s'il y a lieu, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) le degré de responsabilité de l'institution, organe ou organisme de l'Union, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

c) toute mesure prise par l'institution, organe ou organisme de l'Union pour atténuer les dommages subis par les personnes touchées;

d) le niveau de coopération établi avec le Contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, y compris le respect de toute mesure précédemment ordonnée par le Contrôleur européen de la protection des données à l'encontre de l'institution, organe ou organisme de l'Union concerné pour le même objet;

e) toute violation similaire commise précédemment par l'institution, organe ou organisme de l'Union;

f) la manière dont le Contrôleur européen de la protection des données a eu connaissance de la violation, notamment si, et le cas échéant dans quelle mesure, l'institution, organe ou organisme de l'Union a notifié la violation;

g) le budget annuel de l'institution, organe ou organisme de l'Union.

2. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'une amende administrative pouvant aller jusqu'à 1 500 000 EUR.

3. La non-conformité du système d'IA avec les exigences ou obligations au titre du présent règlement, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 750 000 EUR.

4. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, organe ou organisme de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue sur l'éventuelle infraction. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les éléments et les circonstances au sujet desquels les parties concernées ont pu formuler des observations. Les éventuels plaignants sont étroitement associés à la procédure.

5. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.

6. Les fonds collectés en imposant des amendes en vertu du présent article contribuent au budget général de l'Union. Les amendes ne compromettent pas le bon fonctionnement de l'institution, organe ou organisme de l'Union faisant l'objet d'une amende.

7. Le Contrôleur européen de la protection des données informe chaque année la Commission des amendes administratives qu'il a infligées en vertu du présent article ainsi que de toute action en justice ou procédure judiciaire qu'il a engagée.

article 101
Amendes applicables aux fournisseurs de modèles d'IA à usage général

1. La Commission peut infliger aux fournisseurs de modèles d'IA à usage général des amendes n'excédant pas 3 % de leur chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, ou 15 000 000 EUR, le montant le plus élevé étant retenu, lorsque la Commission constate que le fournisseur, de manière délibérée ou par négligence:

a) a enfreint les dispositions pertinentes du présent règlement;

b) n'a pas donné suite à une demande de document ou d'informations au titre de l'article 91, ou a fourni des informations inexactes, incomplètes ou trompeuses;

c) ne s'est pas conformé à une mesure demandée au titre de l'article 93;

d) n'a pas donné à la Commission accès au modèle d'IA à usage général ou au modèle d'IA à usage général présentant un risque systémique en vue de procéder à une évaluation conformément à l'article 92.

Pour fixer le montant de l'amende ou de l'astreinte, il y a lieu de prendre en considération la nature, la gravité et la durée de la violation, tout en tenant dûment compte des principes de proportionnalité et d'adéquation. La Commission tient également compte des engagements pris conformément à l'article 93, paragraphe 3, ou pris dans les codes de bonne pratique pertinents conformément à l'article 56.

2. Avant d'adopter la décision en vertu du paragraphe 1, la Commission communique ses constatations préliminaires au fournisseur du modèle d'IA à usage général, et lui donne la possibilité d'être entendu.

3. Les amendes infligées conformément au présent article sont effectives, proportionnées et dissuasives.

4. Les informations relatives aux amendes infligées en vertu du présent article sont en outre communiquées au Comité IA, le cas échéant.

5. La Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission a fixé une amende au titre du présent article. Elle peut supprimer, réduire ou majorer l'amende infligée.

6. La Commission adopte des actes d'exécution contenant les modalités détaillées des procédures et des garanties procédurales en vue de l'adoption éventuelle de décisions en vertu du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

CHAPITRE XIII
DISPOSITIONS FINALES

Dispositions finales

article 102
Modification du règlement (CE) no 300/2008

À l'article 4, paragraphe 3, du règlement (CE) no 300/2008, l'alinéa suivant est ajouté:

«Lors de l'adoption de mesures détaillées relatives aux spécifications techniques et aux procédures d'approbation et d'utilisation des équipements de sûreté en ce qui concerne les systèmes d'intelligence artificielle au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*1), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 103
Modification du règlement (UE) no 167/2013

À l'article 17, paragraphe 5, du règlement (UE) no 167/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*2), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 104
Modification du règlement (UE) no 168/2013

À l'article 22, paragraphe 5, du règlement (UE) no 168/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*3), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 105
Modification de la directive 2014/90/UE

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté:

«5. Pour les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*4), lorsqu'elle exerce ses activités conformément au paragraphe 1 et qu'elle adopte des spécifications techniques et des normes d'essai conformément aux paragraphes 2 et 3, la Commission tient compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 106
Modification de la directive (UE) 2016/797

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté:

«12. Lors de l'adoption d'actes délégués conformément au paragraphe 1 et d'actes d'exécution conformément au paragraphe 11 en ce qui concerne les systèmes d'intelli-

gence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*5), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 107
Modification du règlement (UE) 2018/858

À l'article 5 du règlement (UE) 2018/858, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes délégués conformément au paragraphe 3 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*6), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 108
Modifications du règlement (UE) 2018/1139

Le règlement (UE) 2018/1139 est modifié comme suit:

1) À l'article 17, le paragraphe suivant est ajouté:

«3. Sans préjudice du paragraphe 2, lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*7), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*7) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).»."

2) À l'article 19, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

3) À l'article 43, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

4) À l'article 47, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

5) À l'article 57, le paragraphe suivant est ajouté:

«Lors de l'adoption de ces actes d'exécution en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

6) À l'article 58, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécu-

rité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

article 109
Modification du règlement (UE) 2019/2144

À l'article 11 du règlement (UE) 2019/2144, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes d'exécution conformément au paragraphe 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*8), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

article 110
Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828 du Parlement européen et du Conseil[58], le point suivant est ajouté:

«68)Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

article 111
Systèmes d'IA déjà mis sur le marché ou mis en service et modèles d'IA à usage général déjà mis sur le marché

1. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), les systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe X et mis sur le marché ou mis en service avant le 2 août 2027 sont mis en conformité avec le présent règlement au plus tard le 31 décembre 2030.

Il est tenu compte des exigences énoncées dans le présent règlement lors de l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe X devant être effectuée conformément à ces actes juridiques et lorsque ces actes juridiques sont remplacés ou modifiés.

2. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), le présent règlement s'applique aux opérateurs de systèmes d'IA à haut risque, autres que les systèmes visés au paragraphe 1 du présent article, qui ont été mis sur le marché ou mis en service avant le 2 août 2026, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leurs conceptions. En tout état de cause, les fournisseurs et les déployeurs de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques prennent les mesures nécessaires pour se conformer aux exigences et obligations du présent règlement au plus tard le 2 août 2030.

cf. déployeurs

3. Les fournisseurs de modèles d'IA à usage général qui ont été mis sur le marché avant le 2 août 2025 prennent les mesures nécessaires pour se conformer aux obligations prévues par le présent règlement au plus tard le 2 août 2027.

article 112
Évaluation et réexamen

1. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III et la liste des pratiques d'IA interdites figurant à l'article 5, une fois par an après l'entrée en vigueur du présent règlement et jusqu'à la fin de la période de délégation de pouvoir

58. Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

énoncée à l'article 97. La Commission transmet les conclusions de cette évaluation au Parlement européen et au Conseil.

2. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen et au Conseil sur les éléments suivants:

a) la nécessité de modifications pour étendre des rubriques de domaine existantes ou ajouter de nouvelles rubriques de domaine dans l'annexe III;

b) les modifications de la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires au titre de l'article 50;

c) les modifications visant à renforcer l'efficacité du système de surveillance et de gouvernance.

3. Au plus tard le 2 août 2029 et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Le rapport comprend une évaluation en ce qui concerne la structure de contrôle de l'application ainsi que l'éventuelle nécessité d'une agence de l'Union pour remédier aux lacunes identifiées. Sur la base des constatations, ce rapport est, le cas échéant, accompagné d'une proposition de modification du présent règlement. Les rapports sont publiés.

4. Les rapports visés au paragraphe 2 prêtent une attention particulière aux éléments suivants:

a) l'état des ressources financières, techniques et humaines dont les autorités nationales compétentes ont besoin pour mener efficacement à bien les missions qui leur sont dévolues par le présent règlement;

b) l'état des sanctions, notamment les amendes administratives visées à l'article 99, paragraphe 1, appliquées par les États membres en cas de violation du présent règlement;

c) les normes harmonisées adoptées et les spécifications communes élaborées à l'appui du présent règlement;

d) le nombre d'entreprises qui arrivent sur le marché après l'entrée en application du présent règlement, et combien d'entre elles sont des PME.

5. Au plus tard le 2 août 2028, la Commission évalue le fonctionnement du Bureau de l'IA, afin de déterminer si des pouvoirs et compétences suffisants lui ont été conférés pour s'acquitter de ses tâches, et s'il serait pertinent et nécessaire pour la bonne mise en œuvre et l'application correcte du présent règlement de renforcer le Bureau de l'IA et ses compétences d'exécution et d'accroître ses ressources. La Commission présente un rapport sur son évaluation au Parlement européen et au Conseil.

6. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission présente un rapport sur l'examen de l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, et évalue la nécessité de mesures ou d'actions supplémentaires, y compris de mesures ou d'actions contraignantes. Ce rapport est présenté au Parlement européen et au Conseil et il est rendu public.

7. Au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au chapitre III, section 2, pour les systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque, y compris en ce qui concerne la durabilité environnementale.

8. Aux fins des paragraphes 1 à 7, le Comité IA, les États membres et les autorités nationales compétentes fournissent des informations à la Commission à la demande de cette dernière et sans retard injustifié.

9. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 à 7, la Commission tient compte des positions et des conclusions du Comité IA, du Parlement européen, du Conseil et d'autres organismes ou sources pertinents.

10. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies, de l'effet des systèmes d'IA sur la santé et la sécurité, ainsi que sur les droits fondamentaux, et à la lumière de l'état d'avancement de la société de l'information.

11. Pour orienter les évaluations et les réexamens visés aux paragraphes 1 à 7 du présent article, le Bureau de l'IA entreprend de mettre au point une méthode objective et participative pour l'évaluation des niveaux de risque fondée sur les critères décrits dans les articles pertinents et l'inclusion de nouveaux systèmes dans:

a) la liste figurant à l'annexe III, y compris l'extension des rubriques de domaine existantes ou l'ajout de nouvelles rubriques de domaine dans ladite annexe;

b) la liste des pratiques interdites figurant à l'article 5; et

c) la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires en application de l'article 50.

12. Toute modification du présent règlement en vertu du paragraphe 10, ou tout acte délégué ou acte d'exécution pertinent, qui concerne la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, tient compte des spécificités réglementaires de chaque secteur, ainsi et des mécanismes de gouvernance, d'évaluation de la conformité et d'applications existants et des autorités qui y sont établies.

13. Au plus tard le 2 août 2031, la Commission procède à une évaluation de sa mise en application dont elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du présent règlement. Sur la base des conclusions, ce rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure de contrôle de l'application ainsi que la nécessité d'une agence de l'Union pour remédier aux lacunes identifiées.

article 113
Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Il est applicable à partir du 2 août 2026.

Toutefois:

a) les chapitres I et II sont applicables à partir du 2 février 2025;

b) le chapitre III, section 4, le chapitre V, le chapitre VII, le chapitre XII et l'article 78 s'appliquent à partir du 2 août 2025, à l'exception de l'article 101;

c) l'article 6, paragraphe 1, et les obligations correspondantes du présent règlement s'appliquent à partir du 2 août 2027.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 13 juin 2024.

Par le Parlement européen
La présidente
R. METSOLA

Par le Conseil
Le président
M. MICHEL

Annexes

ANNEXE I
Liste de la législation d'harmonisation de l'Union

Section A.
Liste de la législation d'harmonisation de l'Union fondée sur le nouveau cadre législatif

1. Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24);
2. Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1);
3. Directive 2013/53/UE du Parlement européen et du Conseil du 20 novembre 2013 relative aux bateaux de plaisance et aux véhicules nautiques à moteur et abrogeant la directive 94/25/CE (JO L 354 du 28.12.2013, p. 90);
4. Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs (JO L 96 du 29.3.2014, p. 251);
5. Directive 2014/34/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles (JO L 96 du 29.3.2014, p. 309);
6. Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62);
7. Directive 2014/68/UE du Parlement européen et du Conseil du 15 mai 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des équipements sous pression (JO L 189 du 27.6.2014, p. 164);
8. Règlement (UE) 2016/424 du Parlement européen et du Conseil du 9 mars 2016 relatif aux installations à câbles et abrogeant la directive 2000/9/CE (JO L 81 du 31.3.2016, p. 1);
9. Règlement (UE) 2016/425 du Parlement européen et du Conseil du 9 mars 2016 relatif aux équipements de protection individuelle et abrogeant la directive 89/686/CEE du Conseil (JO L 81 du 31.3.2016, p. 51);
10. Règlement (UE) 2016/426 du Parlement européen et du Conseil du 9 mars 2016 concernant les appareils brûlant des combustibles gazeux et abrogeant la directive 2009/142/CE (JO L 81 du 31.3.2016, p. 99);
11. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) no 178/2002 et le règlement (CE) no 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1);
12. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

Section B.
Liste des autres législations d'harmonisation de l'Union

13. Règlement (CE) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) no 2320/2002 (JO L 97 du 9.4.2008, p. 72);

14. Règlement (UE) no 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52);
15. Règlement (UE) no 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1);
16. Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146);
17. Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44);
18. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) no 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1);
19. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) no 78/2009, (CE) no 79/2009 et (CE) no 661/2009 du Parlement européen et du Conseil et les règlements (CE) no 631/2009, (UE) no 406/2010, (UE) no 672/2010, (UE) no 1003/2010, (UE) no 1005/2010, (UE) no 1008/2010, (UE) no 1009/2010, (UE) no 19/2011, (UE) no 109/2011, (UE) no 458/2011, (UE) no 65/2012, (UE) no 130/2012, (UE) no 347/2012, (UE) no 351/2012, (UE) no 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1);
20. Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) no 2111/2005, (CE) no 1008/2008, (UE) no 996/2010, (UE) no 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) no 552/2004 et (CE) no 216/2008 du Parlement européen et du Conseil et le règlement (CEE) no 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1), dans la mesure où il concerne la conception, la production et la mise sur le marché des aéronefs visés à son article 2, paragraphe 1, points a) et b), lorsque cela concerne des aéronefs sans équipage à bord et leurs moteurs, hélices, pièces et équipements de contrôle à distance.

ANNEXE II
Liste des infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii)

Infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii):

— terrorisme,

— traite des êtres humains,

— exploitation sexuelle des enfants et pédopornographie,

— trafic de stupéfiants ou de substances psychotropes,

— trafic d'armes, de munitions ou d'explosifs,

— homicide volontaire, coups et blessures graves,

— trafic d'organes ou de tissus humains,

— trafic de matières nucléaires ou radioactives,

— enlèvement, séquestration ou prise d'otage,

— crimes relevant de la compétence de la Cour pénale internationale,

— détournement d'avion ou de navire,

— viol,

— criminalité environnementale,

— vol organisé ou à main armée,

— sabotage,

— participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus.

ANNEXE III
Systèmes d'IA à haut risque visés à l'article 6, paragraphe 2

Les systèmes d'IA à haut risque au sens de l'article 6, paragraphe 2, sont les systèmes d'IA répertoriés dans l'un des domaines suivants:

1. Biométrie, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

   a) systèmes d'identification biométrique à distance.
   Cela n'inclut pas les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique dont la seule finalité est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être;

   b) systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques;

   c) systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.

2. Infrastructures critiques: systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.

3. Éducation et formation professionnelle:

   a) systèmes d'IA destinés à être utilisés pour déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle, à tous les niveaux;

   b) systèmes d'IA destinés à être utilisés pour évaluer les acquis d'apprentissage, y compris lorsque ceux-ci sont utilisés pour orienter le processus d'apprentissage de personnes physiques dans les établissements d'enseignement et de formation professionnelle, à tous les niveaux;

   c) systèmes d'IA destinés à être utilisés pour évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre, dans le contexte ou au sein d'établissements d'enseignement et de formation professionnelle à tous les niveaux;

   d) systèmes d'IA destinés à être utilisés pour surveiller et détecter des comportements interdits chez les étudiants lors d'examens dans le contexte d'établissements d'enseignement et de formation ou en leur sein à tous les niveaux;

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant:

   a) systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats;

b) systèmes d'IA destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

5. Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels:

a) systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services;

b) systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières;

c) systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie;

d) systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence.

6. Répression, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales;

b) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives, en tant que polygraphes ou outils similaires;

c) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales;

d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer le risque qu'une personne physique commette une infraction ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes;

e) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière ou de l'exécution de sanctions pénales.

7. Migration, asile et gestion des contrôles aux frontières, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, en tant que polygraphes et outils similaires;

b) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour évaluer un risque, y compris un risque pour la sécurité, un risque de migration irrégulière ou un risque pour la santé, posé par une personne

physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre;

c) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour aider les autorités publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, y compris les évaluations connexes de la fiabilité des éléments de preuve;

d) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques, à l'exception de la vérification des documents de voyage.

8. Administration de la justice et processus démocratiques:

a) systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom, pour les aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige;

b) systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums. Sont exclus les systèmes d'IA aux sorties desquels les personnes physiques ne sont pas directement exposées, tels que les outils utilisés pour organiser, optimiser ou structurer les campagnes politiques sous l'angle administratif ou logistique.

ANNEXE IV
Documentation technique visée à l'article 11, paragraphe 1

La documentation technique visée à l'article 11, paragraphe 1, contient au moins les informations ci-après, selon le système d'IA concerné:

1. une description générale du système d'IA, y compris:

a) la destination, le nom du fournisseur et la version du système, faisant apparaître sa relation aux versions précédentes;

b) la manière dont le système d'IA interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels, y compris avec d'autres systèmes d'IA, qui ne font pas partie du système d'IA lui-même, le cas échéant;

c) les versions des logiciels ou des micrologiciels pertinents et toute exigence relative aux mises à jour de la version;

d) la description de toutes les formes sous lesquelles le système d'IA est mis sur le marché ou mis en service, telles que les packs logiciels intégrés dans du matériel informatique, les téléchargements ou les API;

e) la description du matériel informatique sur lequel le système d'IA est destiné à être exécuté;

f) lorsque le système d'IA est un composant de produits, des photographies ou des illustrations montrant les caractéristiques externes, le marquage et la disposition interne de ces produits;

g) une description de base de l'interface utilisateur fournie au déployeur;

cf. déployeurs

h) une notice d'utilisation à l'intention du déployeur et une description de base de l'interface utilisateur fournie au déployeur, le cas échéant;

2. une description détaillée des éléments du système d'IA et de son processus de développement, y compris:

a) les méthodes et étapes suivies pour le développement du système d'IA, y compris, le cas échéant, le recours à des systèmes ou outils pré-entraînés fournis par des tiers et la manière dont ceux-ci ont été utilisés, intégrés ou modifiés par le fournisseur;

b) les spécifications de conception du système, à savoir la logique générale du système d'IA et des algorithmes; les principaux choix de conception, y compris le raisonnement et les hypothèses retenues, y compris en ce qui concerne les personnes ou les groupes de personnes à l'égard desquels le système est destiné à être utilisé; les principaux choix de classification; ce que le système est conçu pour optimiser, ainsi que la pertinence des différents paramètres; la description des sorties attendues du système et de leur qualité; les décisions relatives aux compromis éventuels en ce qui concerne les solutions techniques adoptées pour se conformer aux exigences énoncées au chapitre III, section 2;

c) la description de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global; les ressources informatiques utilisées pour développer, entraîner, mettre à l'essai et valider le système d'IA;

d) le cas échéant, les exigences relatives aux données en ce qui concerne les fiches décrivant les méthodes et techniques d'entraînement et les jeux de données d'entraînement utilisés, y compris une description générale de ces jeux de données et des informations sur leur provenance, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées; les procédures d'étiquetage (par exemple pour l'apprentissage supervisé), les méthodes de nettoyage des données (par exemple la détection des valeurs aberrantes);

e) l'évaluation des mesures de contrôle humain nécessaires conformément à l'article 14, y compris une évaluation des mesures techniques nécessaires pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA, conformément à l'article 13, paragraphe 3, point d);

cf. déployeurs

f) le cas échéant, une description détaillée des modifications prédéterminées du système d'IA et de ses performances, ainsi que toutes les informations pertinentes relatives aux solutions techniques adoptées pour garantir que continue d'être assurée la conformité du système d'IA aux les exigences pertinentes énoncées au chapitre III, section 2;

g) les procédures de validation et d'essai utilisées, y compris les informations sur les données de validation et d'essai utilisées et leurs principales caractéristiques; les indicateurs utilisés pour mesurer l'exactitude, la robustesse et le respect des autres exigences pertinentes énoncées au chapitre III, section 2, ainsi que les éventuelles incidences discriminatoires; les journaux de test et tous les rapports de test datés et signés par les personnes responsables, y compris en ce qui concerne les modifications prédéterminées visées au point f);

h) les mesures de cybersécurité qui ont été prises;

3. des informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, en particulier en ce qui concerne: les capacités et les limites du système sur le plan de sa performance, y compris le degré d'exactitude pour des personnes ou des groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé et le niveau global d'exactitude prévu par rapport à sa destination; les résultats non intentionnels et sources de risques prévisibles pour la santé et la sécurité, les droits fondamentaux et en termes de discrimination compte tenu de la destination du système d'IA; les mesures de contrôle humain nécessaires conformément à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA; les spécifications concernant les données d'entrée, le cas échéant;

4. une description de l'adéquation des indicateurs de performance à ce système d'IA spécifique;

5. une description détaillée du système de gestion des risques conformément à l'article 9;

6. une description des modifications pertinentes apportées par le fournisseur au système tout au long de son cycle de vie;

7. une liste des normes harmonisées appliquées, en totalité ou en partie, dont les références ont été publiées au Journal officiel de l'Union européenne; lorsqu'aucune norme harmonisée de ce type n'a été appliquée, une description détaillée des solutions adoptées pour satisfaire aux exigences énoncées au cha-

pitre III, section 2, y compris une liste des autres normes pertinentes et spécifications techniques appliquées;

8. une copie de la déclaration UE de conformité visée à l'article 47;
9. une description détaillée du système en place pour évaluer les performances du système d'IA après la commercialisation conformément à l'article 72, y compris le plan de surveillance après commercialisation visé à l'article 72, paragraphe 3.

ANNEXE V
Déclaration UE de conformité

La déclaration UE de conformité visée à l'article 47 contient l'ensemble des informations suivantes:

1. le nom et le type du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
2. le nom et l'adresse du fournisseur ou, le cas échéant, de son mandataire;
3. une attestation certifiant que la déclaration UE de conformité visée à l'article 47 est établie sous la seule responsabilité du fournisseur;
4. une déclaration attestant que le système d'IA respecte le présent règlement et, le cas échéant, toute autre législation de l'Union applicable prévoyant l'établissement de la déclaration UE de conformité visée à l'article 47;
5. lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680;

cf. RGPD

6. des références aux éventuelles normes harmonisées pertinentes utilisées ou aux éventuelles autres spécifications communes par rapport auxquelles la conformité est déclarée;
7. le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;
8. le lieu et la date de délivrance de la déclaration, le nom et la fonction du signataire ainsi que la mention de la personne pour le compte de laquelle ce dernier a signé, et une signature.

ANNEXE VI
Procédure d'évaluation de la conformité fondée sur le contrôle interne

1. La procédure d'évaluation de la conformité fondée sur le contrôle interne est la procédure d'évaluation de la conformité décrite aux points 2, 3 et 4.
2. Le fournisseur vérifie que le système de gestion de la qualité établi est conforme aux exigences de l'article 17.
3. Le fournisseur examine les informations contenues dans la documentation technique afin d'évaluer la conformité du système d'IA aux exigences essentielles pertinentes énoncées au chapitre III, section 2.
4. Le fournisseur vérifie également que le processus de conception et de développement du système d'IA et son système de surveillance après commercialisation prévu à l'article 72 sont cohérents avec la documentation technique.

ANNEXE VII
Conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique

1 Introduction

La conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique est la procédure d'évaluation de la conformité décrite aux points 2 à 5.

2. Vue d'ensemble

Le système de gestion de la qualité approuvé pour la conception, le développement et les essais des systèmes d'IA conformément à l'article 17 est examiné conformément au point 3 et soumis à la surveillance spécifiée au point 5. La documentation technique du système d'IA est examinée conformément au point 4.

3. Système de gestion de la qualité

3.1. La demande du fournisseur comprend:

a) le nom et l'adresse du fournisseur, ainsi que le nom et l'adresse d'un mandataire si la demande est introduite par celui-ci;

b) la liste des systèmes d'IA couverts par le même système de gestion de la qualité;

c) la documentation technique de chaque système d'IA couvert par le même système de gestion de la qualité;

d) la documentation relative au système de gestion de la qualité qui couvre tous les aspects énumérés à l'article 17;

e) une description des procédures en place pour garantir que le système de gestion de la qualité reste adéquat et efficace;

f) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de gestion de la qualité est évalué par l'organisme notifié, qui détermine s'il satisfait aux exigences visées à l'article 17.

La décision est notifiée au fournisseur ou à son mandataire.

La notification contient les conclusions de l'évaluation du système de gestion de la qualité et la décision d'évaluation motivée.

3.3. Le système de gestion de la qualité tel qu'approuvé continue d'être mis en œuvre et adapté par le fournisseur afin de rester adéquat et efficace.

3.4. Toute modification envisagée du système de gestion de la qualité approuvé ou de la liste des systèmes d'IA couverts par ce dernier est portée à l'attention de l'organisme notifié par le fournisseur.

Les modifications proposées sont examinées par l'organisme notifié, qui décide si le système de gestion de la qualité modifié continue de satisfaire aux exigences visées au point 3.2, ou si une réévaluation est nécessaire.

L'organisme notifié notifie sa décision au fournisseur. La notification contient les conclusions de l'examen des modifications et la décision d'évaluation motivée.

4. Contrôle de la documentation technique

4.1. Outre la demande visée au point 3, une demande est déposée par le fournisseur auprès d'un organisme notifié de son choix pour l'évaluation de la documentation technique relative au système d'IA que le fournisseur prévoit de mettre sur le marché ou de mettre en service et qui est couvert par le système de gestion de la qualité visé au point 3.

4.2. La demande comprend:

a) le nom et l'adresse du fournisseur;

b) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié;

c) la documentation technique visée à l'annexe IV.

4.3. La documentation technique est examinée par l'organisme notifié. Lorsque cela est pertinent et dans les limites de ce qui est nécessaire à l'accomplissement de ses tâches, l'organisme notifié se voit accorder un accès complet aux jeux de données d'entraînement, de validation et d'essai utilisés, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'API ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

4.4. Lors de l'examen de la documentation technique, l'organisme notifié peut exiger que le fournisseur apporte des preuves supplémentaires ou effectue des essais

supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA avec les exigences énoncées au chapitre III, section 2. Lorsque l'organisme notifié n'est pas satisfait des essais effectués par le fournisseur, l'organisme notifié effectue directement des essais adéquats, le cas échéant.

4.5. Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, l'accès aux modèles d'entraînement et aux modèles entraînés du système d'IA, y compris à ses paramètres pertinents, est aussi accordé à l'organisme notifié. Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.

4.6. La décision de l'organisme notifié est notifiée au fournisseur ou à son mandataire. La notification contient les conclusions de l'évaluation de la documentation technique et la décision d'évaluation motivée.

Lorsque le système d'IA est conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié délivre un certificat d'évaluation UE de la documentation technique. Le certificat indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du système d'IA.

Le certificat et ses annexes contiennent toutes les informations pertinentes pour permettre l'évaluation de la conformité du système d'IA et le contrôle du système d'IA pendant son utilisation, le cas échéant.

Lorsque le système d'IA n'est pas conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié refuse de délivrer un certificat d'évaluation UE de la documentation technique et en informe le demandeur, en lui précisant les raisons de son refus.

Lorsque le système d'IA ne satisfait pas à l'exigence relative aux données utilisées pour l'entraîner, il devra être entraîné à nouveau avant l'introduction d'une nouvelle demande d'évaluation de la conformité. Dans ce cas, la décision d'évaluation motivée de l'organisme notifié refusant de délivrer le certificat d'évaluation UE de la documentation technique contient des considérations spécifiques sur la qualité des données utilisées pour entraîner le système d'IA, en particulier sur les raisons de la non-conformité.

4.7. Les éventuelles modifications du système d'IA susceptibles d'avoir une incidence sur la conformité du système d'IA avec les exigences ou sur sa destination sont évaluées par l'organisme notifié qui a délivré le certificat d'évaluation UE de la documentation technique. Le fournisseur informe cet organisme notifié de son intention d'introduire une telle modification ou s'il prend autrement connaissance de l'existence de telles modifications. Les modifications envisagées sont évaluées par l'organisme notifié, qui décide si elles nécessitent une nouvelle évaluation de la conformité conformément à l'article 43, paragraphe 4, ou si elles peuvent faire l'objet d'un document complémentaire au certificat d'évaluation UE de la documentation technique. Dans ce dernier cas, l'organisme notifié évalue les modifications, informe le fournisseur de sa décision et, lorsque les modifications sont approuvées, lui fournit un document complémentaire au certificat d'évaluation UE de la documentation technique.

5. Surveillance du système de gestion de la qualité approuvé

5.1. Le but de la surveillance effectuée par l'organisme notifié visé au point 3 est de s'assurer que le fournisseur se conforme dûment aux conditions du système de gestion de la qualité approuvé.

5.2. À des fins d'évaluation, le fournisseur autorise l'organisme notifié à accéder aux locaux où les systèmes d'IA sont conçus, développés ou mis à l'essai. Le fournisseur partage en outre avec l'organisme notifié toutes les informations nécessaires.

5.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fournisseur maintient et applique le système de gestion de la qualité; il transmet un rapport d'audit au fournisseur. Dans le cadre de ces audits, l'organisme notifié peut effectuer des essais supplémentaires des systèmes d'IA pour lesquels un certificat d'évaluation UE de la documentation technique a été délivré.

ANNEXE VIII
Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque conformément à l'article 49

Section A - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 1

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 1:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA ainsi que des composants et fonctions gérées au moyen de ce système d'IA;
6. une description de base et concise des informations utilisées par le système (données, entrées) et de sa logique de fonctionnement;
7. le statut du système d'IA (sur le marché ou en service; plus mis sur le marché/en service, rappelé);
8. le type, le numéro et la date d'expiration du certificat délivré par l'organisme notifié et le nom ou le numéro d'identification de cet organisme notifié, le cas échéant;
9. une copie numérisée du certificat visé au point 8, le cas échéant;
10. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union;
11. une copie de la déclaration UE de conformité visée à l'article 47;
12. une notice d'utilisation en format électronique; ces informations ne sont pas à fournir pour les systèmes d'IA à haut risque dans les domaines des activités répressives ou de la migration, de l'asile et de la gestion des contrôles aux frontières visés à l'annexe III, points 1, 6 et 7;
13. une adresse URL vers des informations supplémentaires (facultatif).

Section B - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 2

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à enregistrer conformément à l'article 49, paragraphe 2:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA;
6. la ou les conditions visées à l'article 6, paragraphe 3, sur la base desquelles le système d'IA est considéré comme n'étant pas à haut risque;
7. un résumé succinct des motifs pour lesquels le système d'IA est considéré comme n'étant pas à haut risque en application de la procédure prévue à l'article 6, paragraphe 3;
8. le statut du système d'IA (sur le marché ou en service; plus sur le marché/en service, rappelé);

9. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union.

Section C - Informations à fournir par les déployeurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 3

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 3:

1. le nom, l'adresse et les coordonnées du déployeur;
2. le nom, l'adresse et les coordonnées de toute personne qui soumet des informations au nom du déployeur;
3. l'adresse URL de l'entrée du système d'IA dans la base de données de l'UE par son fournisseur;
4. une synthèse des conclusions de l'analyse d'impact sur les droits fondamentaux réalisée conformément à l'article 27;
5. un résumé de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, comme précisé à l'article 26, paragraphe 8, du présent règlement, le cas échéant.

cf. déployeurs

cf. RGPD art. 35

ANNEXE IX
Informations à fournir lors de l'enregistrement de systèmes d'IA à haut risque énumérés à l'annexe III en ce qui concerne les essais en conditions réelles conformément à l'article 60

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les essais en conditions réelles à enregistrer conformément à l'article 60:

1. un numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles;
2. le nom et les coordonnées du fournisseur ou du fournisseur potentiel et des déployeurs participant aux essais en conditions réelles;
3. une brève description du système d'IA et de sa destination, ainsi que d'autres informations nécessaires à l'identification du système;
4. une synthèse des caractéristiques principales du plan d'essais en conditions réelles;
5. des informations sur la suspension ou la cessation des essais en conditions réelles.

cf. déployeurs

ANNEXE X
Actes législatifs de l'Union relatifs aux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

1. Système d'information Schengen
   a) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).
   b) Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) no 1987/2006 (JO L 312 du 7.12.2018, p. 14).
   c) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du

système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) no 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

2. Système d'information sur les visas

   a) Règlement (UE) 2021/1133 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) no 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système d'information sur les visas (JO L 248 du 13.7.2021, p. 1).

   b) Règlement (UE) 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) no 767/2008, (CE) no 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 et (UE) 2019/1896 du Parlement européen et du Conseil et abrogeant les décisions 2004/512/CE et 2008/633/JAI du Conseil, aux fins de réformer le système d'information sur les visas (JO L 248 du 13.7.2021, p. 11).

3. Eurodac

   Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'«Eurodac» pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1315, (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) no 603/2013 du Parlement européen et du Conseil (JO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Système d'entrée/de sortie

   Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) no 767/2008 et (UE) no 1077/2011 (JO L 327 du 9.12.2017, p. 20).

5. Système européen d'information et d'autorisation concernant les voyages

   a) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) no 1077/2011, (UE) no 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).

   b) Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (JO L 236 du 19.9.2018, p. 72).

6. Système européen d'information sur les casiers judiciaires concernant des ressortissants de pays tiers et des apatrides

   Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

7. Interopérabilité

   a) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modi-

fiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI (JO L 135 du 22.5.2019, p. 27).

b) Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).

ANNEXE XI
Documentation technique visée à l'article 53, paragraphe 1, point a) – documentation technique pour les fournisseurs de modèles d'IA à usage général

Section 1
Informations devant être fournies par tous les fournisseurs de modèles d'IA à usage général

La documentation technique visée à l'article 53, paragraphe 1, point a), contient au moins les informations ci-après, en fonction de la taille et du profil de risque du modèle:

1. Une description générale du modèle d'IA à usage général, y compris:
   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
   b) les politiques applicables en matière d'utilisation acceptable;
   c) la date de publication et les méthodes de distribution;
   d) l'architecture et le nombre de paramètres;
   e) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
   f) la licence.
2. Une description détaillée des éléments du modèle visés au point 1, et des informations pertinentes sur le processus de développement, y compris les éléments suivants:
   a) les moyens techniques (p. ex.: notice d'utilisation, infrastructure, outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;
   b) les spécifications de conception du modèle et du processus d'entraînement, y compris les méthodes et techniques d'entraînement, les principaux choix de conception, y compris le raisonnement et les hypothèses retenues; ce que le modèle est conçu pour optimiser, ainsi que la pertinence des différents paramètres, le cas échéant;
   c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation (p. ex.: nettoyage, filtrage, etc.), le nombre de points de données, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées, ainsi que toutes les autres mesures visant à détecter l'inadéquation des sources de données et les méthodes permettant de détecter les biais identifiables, le cas échéant;
   d) les ressources informatiques utilisées pour entraîner le modèle (p. ex.: nombre d'opérations en virgule flottante), le temps d'entraînement et d'autres détails pertinents liés à l'entraînement;
   e) la consommation d'énergie connue ou estimée du modèle.

   En ce qui concerne le point e), lorsque la consommation d'énergie du modèle est inconnue, la consommation d'énergie peut être estimée en s'appuyant sur des informations concernant les ressources informatiques utilisées.

Section 2
Informations devant être fournies par les fournisseurs de modèles d'IA à usage général présentant un risque systémique

1. Une description détaillée des stratégies d'évaluation, y compris les résultats de l'évaluation, sur la base des protocoles et outils d'évaluation publics disponibles ou d'autres méthodes d'évaluation. Les stratégies d'évaluation comprennent des critères, des indicateurs et les méthodes d'évaluation pour l'identification des limites.
2. Le cas échéant, une description détaillée des mesures mises en place pour effectuer des essais contradictoires internes et/ou externes (p. ex.: méthode de l'équipe rouge), des adaptations de modèles, y compris l'alignement et le réglage fin.
3. Le cas échéant, une description détaillée de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global.

ANNEXE XII
Informations relatives à la transparence visées à l'article 53, paragraphe 1, point b) – documentation technique pour les fournisseurs de modèles d'IA à usage général aux fournisseurs en aval qui intègrent le modèle dans leur système d'IA

Les informations visées à l'article 53, paragraphe 1, point b) comprennent au moins:

1. Une description générale du modèle d'IA à usage général, y compris:
   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
   b) les politiques applicables en matière d'utilisation acceptable;
   c) la date de publication et les méthodes de distribution;
   d) la manière dont le modèle interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels qui ne font pas partie du modèle lui-même, le cas échéant;
   e) les versions des logiciels pertinents liés à l'utilisation du modèle d'IA à usage général, le cas échéant;
   f) l'architecture et le nombre de paramètres;
   g) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
   h) la licence pour le modèle.
2. Une description des éléments du modèle et de son processus de développement, notamment:
   a) les moyens techniques (p. ex.: la notice d'utilisation, l'infrastructure, les outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;
   b) les modalités (p. ex.: texte, image, etc.) et le format des entrées et des sorties, ainsi que leur taille maximale (p. ex.: taille de la fenêtre de contexte, etc.);
   c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation.

ANNEXE XIII
Critères de désignation des modèles d'IA à usage général présentant un risque systémique visés à l'article 51

Aux fins de déterminer si un modèle d'IA à usage général a des capacités ou un impact équivalents à ceux énoncés à l'article 51, paragraphe 1, point a), la Commission tient compte des critères suivants:

a) le nombre de paramètres du modèle;

b) la qualité ou la taille du jeu de données, par exemple mesurée en tokens;

c) la quantité de calcul utilisée pour l'entraînement du modèle, mesurée en nombre d'opérations en virgule flottante ou indiquée par une combinaison d'autres variables telles que le coût estimé de l'entraînement, le temps estimé nécessaire à l'entraînement ou la consommation d'énergie estimée pour l'entraînement;

d) les modalités d'entrée et de sortie du modèle, telles que la conversion de texte en texte (grands modèles de langage), la conversion de texte en image, la multimodalité et les seuils de l'état de l'art pour déterminer les capacités à fort impact pour chaque modalité, ainsi que le type spécifique d'entrées et de sorties (p. ex.: séquences biologiques);

e) les critères de référence et les évaluations des capacités du modèle, y compris en tenant compte du nombre de tâches ne nécessitant pas d'entraînement supplémentaire, sa capacité d'adaptation à apprendre de nouvelles tâches distinctes, son niveau d'autonomie et d'extensibilité, ainsi que les outils auxquels il a accès;

f) si le modèle a un impact important sur le marché intérieur en raison de sa portée, qui est présumée lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union;

g) le nombre d'utilisateurs finaux inscrits.

INDEX

(les numéros renvoient aux pages de ce document)

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

A propos de l’AFCDP

www.afcdp.net

L’AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé un nouveau métier, celui de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés), préfigurateur du Délégué à la protection des données créé par le RGPD.

L'AFCDP est l'association représentative des Délégués à la protection des données (DPD ou DPO pour Data Privacy Officer), mais elle rassemble largement. Au-delà des professionnels de la protection des données et des Délégués désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Quelques membres de l'AFCDP : 3 Suisses, Accor, Action contre la faim, Adecco, Aéroports de Paris, AG2R La Mondiale, American Hospital of Paris, Assemblée nationale, Association des paralysés de France, Autorité des marchés financiers, AXA, Banque de France, BP France, Carrefour, Caisse nationale des allocations familiales, CHU de Bordeaux, Clermont-Ferrand, Nice, Poitiers et Toulouse, CNES, Communauté Urbaine de Marseille Provence, Conseil Général de Seine-Maritime, CPAM des Bouches du Rhône, Crédit Immobilier de France, Départements de Charente-Maritime, de Corrèze, de Gironde, de la Manche, Ecole Polytechnique, Fédération Nationale des Tiers de Confiance, La Française des Jeux, Gendarmerie Nationale, Orange, IBM France, INRA, Institut Curie, Groupe Casino, Laboratoire Yves Rocher, Legrand, Malakoff Mederic, Michelin, La Poste, Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche, Monnaie de Paris, Olympique de Marseille, Port autonome de Dunkerque, Randstad, RATP, Région Haute Normandie, Région Lorraine, Sénat, SNCF, Total, Ville de Metz, de Lyon, de Paris, de Saint-Etienne, Venteprivée.com, Vinci Energies, VVF Villages.

Ce document est un guide pratique destiné aux adhérents de l'AFCDP.
Il ne constitue pas une référence légale.

www.afcdp.net

Version 1.3
15 juillet 2024