

## Vie de l'Association

« Une équipe à votre service » :

N'hésitez pas à les contacter : [Fatima](#), [Sandrine](#), [Thomas](#), [Nathalie](#), [Vanessa](#), [Marina](#) et [Elizabeth](#).

Vous souhaitez adhérer ? Rendez-vous ici : [Adhérer à l'AFCDP](#)

### Université AFCDP des DPD/DPO Nouvelle Édition 2025

[Nous avons le plaisir de vous annoncer le lancement de l'édition 2025 de l'Université AFCDP des DPO](#)

Elle se déroulera les **6 & 7 février 2025** à la Maison de la Chimie à Paris + 5 sessions numériques de mars à novembre

[📄 Les inscriptions sont ouvertes sur le site dédié. 📄](#)

► Si vous souhaitez sponsoriser l'évènement (Nathalie.brunet@afcdp.net)

### Université AFCDP des DPD/DPO Édition 2024

L'édition 2024 était une édition très spéciale,  
à l'occasion des 20 ans de l'AFCDP.

Les 2 journées du 8 et 9 février se sont déroulées  
à la Maison de la Chimie dans une salle comble.

### L'AFCDP prend la parole

Dans le cadre de sa politique de communication, l'AFCDP intervient régulièrement dans les médias pour faire connaître ses activités, partager ses réflexions sur des thèmes de fond, ou réagir aux faits marquants de l'actualité. Vous pouvez retrouver, [dans l'Espace presse du site public](#), les derniers communiqués de presse.

### Assistance aux DPO en difficulté (réservée aux membres)

L'assistance psychologique annoncée lors de l'assemblée générale entre en service. Ce service est strictement réservé aux membres de l'AFCDP.

### Charte de déontologie : nouvelle version

La nouvelle version de la Charte de déontologie du métier de Délégué à la protection des données, approuvée par votre Conseil d'Administration le 19 septembre 2023 est [accessible sur le site public de l'AFCDP](#).

**IMPORTANT** : Si vous avez signé l'ancienne version de la Charte, celle-ci n'est plus valable **depuis le 5 avril 2024**.

## Bienvenue aux nouveaux membres

Nous souhaitons la bienvenue aux nouveaux adhérents de l'AFCDP :  
AGN AVOCATS PARIS - BOUBEKEUR AVOCATS - CENTRE HOSPITALIER DE MARTIGUES - CENTRE HOSPITALIER DU ROUVRAY - CEVA SANTE ANIMALE - CONSTRUCTIONS MECANIKES DE NORMANDIE - CURE51 - DEPARTEMENT DE LA HAUTE-SAVOIE - ECOLE 42 - EON-JAGUIN AVOCAT - FO-CADRES - LYCORIS CONSEIL - PATHE SAS - PH CONSULTING - RGPD SYNERGIE - UNIVERSITE DE LILLE - VIENNE NUMERIQUE

## Ça se passe sur AGORA (réservé aux membres)

### ► Nouveaux groupes

Pour répondre à des sujets d'actualité ou étendre le rayonnement de l'AFCDP, nous créons régulièrement de nouveaux groupes sur AGORA, voici les derniers :

- [Transports](#)
- [Intelligence artificielle](#)
- [Hôtellerie/Restauration](#)
- [Action sociale](#)
- [Formation/Enseignement](#)
- [Vidéoprotection augmentée](#)
- [Retail](#)

### ► Les sanctions de la CNIL et des autorités de contrôle

Nous vous rappelons le groupe AGORA consacré aux sanctions des autorités de contrôle. Nous y publions les informations sur les sanctions majeures prises par les autorités de contrôle européennes. Vous y trouverez également des comptes rendus des auditions devant la Formation restreinte de la CNIL, et si possible, les décisions qui en découlent. (Merci à Bruno Rasle).

Si vous aussi, vous avez connaissance de nouvelles sanctions dont la nature, le montant, ou les attendus méritent d'être connus, n'hésitez pas à le signaler à l'équipe de rédaction.

### ► La discussion du mois

Parmi les dizaines de demandes d'aide que se sont partagées nos Membres le mois dernier, nous en avons sélectionné une, qui a déclenché une riche discussion :

- Unnidata : Avez-vous été contacté ?

### ► Des offres d'emploi

L'espace emplois de l'AFCDP - le seul dédié au métier de DPO - [comporte diverses opportunités de poste](#). Si vous recrutez, n'hésitez pas à inciter votre service Ressources Humaines à y publier également l'offre de poste.

Vous souhaitez déposer votre CV ? Utilisez l'[espace emplois sur le site AFCDP](#)

### Et toujours...

- ◆ [Le job board dédié au DPO](#)
- ◆ [La place de marché RGPD \(modalités d'utilisation\)](#)

### ► Les fiches pratiques à votre disposition

- ◆ Le GT « DPO Groupe » a dévoilé ses différents travaux !
- => Un guide pratique pour organiser et animer son réseau
- => Une trame d'accord entre RTC, en anglais, et en français.

### ► « Serious game » - RGPD Challenge

[Le jeu inventé par l'AFCDP](#) a été présenté lors de l'Assemblée générale du 13 juin 2023. Si vous souhaitez l'utiliser au sein de votre entité, veuillez retourner le bon de commande sur demande par email ([back-office@afcdp.net](mailto:back-office@afcdp.net)).

Son prix unitaire (une boîte contenant 2 jeux de cartes) est de **30 €**.

Le règlement doit être effectué par virement bancaire et l'envoi sera effectué à réception du règlement.

### ► Les illustrations BD (réservées aux membres)

Plusieurs lots d'illustrations réalisés par le dessinateur Luc Tesson sont à la disposition des membres pour leurs campagnes de sensibilisation...

**Et les nouvelles illustrations 2024 ont été dévoilées à l'Assemblée générale du 26 juin 2024 !**

### ► La Web Télé de l'AFCDP

La Web Télé est le catalogue des vidéos mises à disposition des membres de l'AFCDP sur Agora. Certains webinaires de l'AFCDP sont enregistrés. Vous pouvez les retrouver sur la page de la Web Télé. Ont été ajoutés récemment :

- Webinaire du groupe de travail Marketing digital sur l'Intelligence artificielle (IA)
- Colloque Opportunités et défis de l'utilisation secondaire des données de santé
- Webinaire CEDPO - One Technology, Many Perspectives - Global - Approaches to AI Regulation
- Webinaire démo outil WebSiteAudit du CEPD-EDPB

Vous pouvez aussi retrouver :

- l'Assemblée générale du 13 juin 2023
- les premières vidéos de l'Université 2024 (réservé aux inscrits)
- les vidéos de l'Université 2023, accessibles progressivement même aux non-inscrits (après un délai d'un an)

## La parole est aux membres

**Découvrez régulièrement le témoignage d'un(e) membre de l'AFCDP. Après tout, ce sont les membres qui en parlent le mieux ! Vous aussi vous souhaitez témoigner ? Écrivez-nous : [marina.casas@afcdp.net](mailto:marina.casas@afcdp.net)**

*« Lorsque l'AFCDP m'a proposé d'animer l'un des sous-groupes de travail "DPO Groupe", j'ai vraiment hésité... Les travaux collectifs, c'est tout ou rien. Lorsqu'il a été ajouté que je pouvais convier un co-animateur, c'est tout naturellement que je me suis tournée vers Hervé Fortin qui m'a fait l'honneur d'accepter. Les objectifs étaient alors clairs : ne pas laisser l'occasion aux travaux de s'enliser et aux bonnes volontés de s'essouffler en (1) consultant tout au long du processus les membres concernés, (2) se donnant un rythme sur une période fixe de 6 mois et (3) ayant en tête une ligne d'arrivée ambitieuse mais atteignable avec un premier livrable opérationnel à la clé. C'était une première pour moi, et quel bonheur de découvrir à cette occasion des membres impliqués, dynamiques et désireux de partager ! Un immense merci à eux et, en particulier, à nos 4 coordinateurs thématiques ainsi qu'à nos contacts dédiés de l'AFCDP pour ce beau travail collectif qui était on ne peut plus d'actualité en cette période des Jeux. »*

Ceci est le témoignage de [Lucy Savary](#), DPO groupe AEF - ALIXIO - ARFILIA.

## Actualité des Groupes de Travail de l'AFCDP

♦ Dans le cadre du **Cybermois**, l'AFCDP organisait le 7 octobre 2024 à Lille, dans les locaux de la **Région Hauts-de-France**, un colloque intitulé « **Cybersécurité : les DPO et RSSI en première ligne** », sous l'animation de Nicolas Samarcq, Administrateur AFCDP.

♦ **En novembre, trois nouveaux groupes de travail AFCDP ont été lancés :**

- **Groupe « [Formation et Enseignement](#) »** : la réunion de lancement s'est tenue le 6 novembre 2024.
- **Intergroupe « [Vidéoprotection augmentée](#) »**. Le GT vidéoprotection augmentée a pour ambition, si ce n'est de faire évoluer la doctrine actuelle, à tout le moins de la préciser. L'objectif sera de réétudier la position de la CNIL de 2022, et de recenser un certain nombre de vos questionnements, afin de les lui soumettre. Une réunion de lancement a eu lieu le 25 novembre 2024. Les membres vont désormais travailler sur un questionnaire en vue de consolider leurs problématiques.
- **Lancement du groupe sectoriel « [Retail](#) »**. Face au nombre croissant de cyberattaque que connaît ce secteur, il a paru indispensable de créer un groupe de travail sectoriel au sein de l'AFCDP, afin de pouvoir concilier sécurité des données, mais aussi et avant tout, la protection des données des personnes concernées/consommateurs. La réunion de lancement s'est tenue le 28 novembre 2024.

♦ **Et pour les réunions en présentiel... :**

 **Favoriser les rencontres entre pairs : devenez l'hôte de la prochaine réunion de votre groupe préféré ! **

Devenez l'hôte de la prochaine réunion de votre groupe préféré ! Prenez l'initiative, aidez les animateurs, et participez au rayonnement de la protection des données. Voici cinq bonnes raisons de recevoir les membres :

- Faire connaître son entité (sans forme de publicité) à un ensemble de confrères ; l'occasion de faire une présentation ;
- Faire participer sa Direction à ce genre de rencontres ;
- Débloquer, parmi des moments « off » comme la pause café, des problématiques internes complexes ;
- Participer au rayonnement de l'association ;
- Rencontrer les DPO d'une même région.

## Manifestations

### Agenda des prochaines réunions de l'AFCDP

Nous vous rappelons que les réunions sont ouvertes à tous les membres, même les réunions des groupes régionaux. Profitez de la visioconférence pour découvrir les travaux des autres groupes. Inscrivez-vous !

- ♦ 2 décembre - Bègles - « [Sud Ouest](#) »
- ♦ 4 décembre - Visio - « [Formation/Enseignement](#) »
- ♦ 9 décembre - Visio - « [Hôtellerie/Restauration](#) »

- ◆ 12 décembre - Kremlin-Bicêtre - « [Données de santé](#) »
- ◆ 13 décembre - Hyères - « [Méditerranée Ouest](#) »
- ◆ 31 janvier - Visio - « [Transports](#) »

Sous-groupes :

- ◆ 12 décembre - Visio - Sous-groupe « NIS 2 & RGPD » (Données de santé)

**Et ne ratez pas non plus les rencontres suivantes (en cours d'organisation) :**

- ◆ 16 décembre - Visio - « [Vidéoprotection augmentée](#) »
- ◆ 3 février - Visio - « [Médico-social](#) »
- ◆ 21 janvier - MEL - « [Nord](#) »

## Partenariats

### La MalletteCyber de [Cybermalveillance.gouv.fr](#)

Suite à l'appel lancé sur Agora, trois membres de l'AFCDP ont participé le 25 novembre 2024 à un atelier organisé par le GIP Acyma, pour adapter la MalletteCyber de [Cybermalveillance.gouv.fr](#) au monde des TPE/PME. Merci à eux pour leur contribution.

### ANSSI – MonAideCyber

Rejoignez la communauté des Aidants dans le cadre du dispositif MonAideCyber ! [MonAideCyber](#) est un projet du Laboratoire d'innovation de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'objectif de ce dispositif est d'accompagner les entités publiques, les associations et les entreprises souhaitant mener une première démarche de sécurisation informatique.

### Salon CBC

L'AFCDP était présente au [salon le 28 novembre à Toulouse](#). C'était aussi l'occasion pour le groupe régional de se réunir et de se faire connaître.

### L'AFCDP a rejoint le dispositif « France Num »

L'AFCDP est partenaire de [France Num](#), « l'initiative gouvernementale pour la transformation numérique des très petites entreprises (TPE) et petites et moyennes entreprises (PME) ».

### Journée CNIL/RGPD à Montpellier

Une nouvelle **journée CNIL/RGPD** a lieu le **4 décembre 2024** par la CNIL, en partenariat avec l'AFCDP, la Région Occitanie, La Métropole et l'Université de Montpellier à l'Institut de Botanique de Montpellier. Au programme : Actualités RGPD, le DPO au quotidien, la gestion des plaintes, la gestion des risques cyber....

### « La cohérence du droit des données » : un colloque de l'Université Lyon III

L'Université Lyon III-Jean Moulin tiendra le 13 février 2025 un colloque consacré à « LA cohérence du droit des données », sous la direction scientifique de Ludovic Pailler, professeur de droit privé et sciences criminelles, et de Claire Brunerie doctorante. Au programme, la cohérence formelle (cohérence des sources écrites et des sources non écrites) et la cohérence substantielle (cohérence des notions et cohérence des méthodes). [L'inscription est gratuite, mais sera obligatoire sur le site dédié.](#)

## CEDPO

► **CEDPO organise un webinaire sur le « data scraping » le 3 décembre 2024 à 15 h CET**

Ce webinaire sera consacré au data scraping, une pratique largement utilisée pour l'entraînement des modèles d'intelligence artificielle, mais qui soulève des questions importantes sur sa légalité, son équité et sa conformité avec les réglementations en matière de protection des données et d'IA.

Les discussions porteront sur les cadres légaux actuels et les perspectives pour assurer une utilisation responsable du data scraping.

Les intervenants seront :

- Paul Jordan : Senior Policy Advisor, CEDPO
- Daniel Solove : Professeur de droit de la propriété intellectuelle et de la technologie à la George Washington University Law School
- Woodrow Hartzog : Professeur de droit à la Boston University School of Law
- David Patariu : Avocat et spécialiste du droit à la vie privée
- Jared Browne : Président du groupe de travail IA & Données de CEDPO, Responsable de la protection des données et de la gouvernance de l'IA chez Fexco Group

► **CEDPO publie un communiqué sur la Conférence des DPO 2024 à Bruxelles**

CEDPO a publié un communiqué suite à sa première conférence, la CEDPO DPO Conference, qui s'est tenue à Bruxelles le 14 octobre 2024 sur le thème : « Le DPO à l'ère numérique ». Cet événement a rassemblé des experts et décideurs européens pour discuter du rôle essentiel du DPO face aux évolutions technologiques et réglementaires, notamment dans les domaines de l'intelligence artificielle et de la cybersécurité.

Le communiqué met en avant l'importance du RGPD comme catalyseur d'un changement culturel au sein des organisations. Il souligne également les défis et opportunités auxquels les DPO sont confrontés, dans un contexte marqué par l'émergence de nouvelles réglementations européennes telles que le **Digital Services Act**, le **Digital Markets Act**, le **Data Governance Act**, le **Data Act**, **NIS2** et l'**AI Act**.

Parmi les principaux enseignements de la conférence :

- **Le DPO à un carrefour** : Les DPO doivent s'adapter à un paysage réglementaire en constante évolution, tout en surmontant les défis liés à la disponibilité des ressources nécessaires à l'accomplissement de leurs missions.
- **Sensibilisation et leadership** : Les DPO sont appelés à jouer un rôle clé dans la sensibilisation des employés et des dirigeants aux implications de l'IA sur le traitement des données personnelles.
- **Développement continu** : La montée en compétences et la capacité à diriger des équipes multidisciplinaires deviennent indispensables pour répondre aux exigences des nouvelles réglementations.

Le communiqué complet (en anglais) est disponible sur le site de CEDPO. Vous pouvez le consulter en cliquant sur ce lien : [Communiqué de la Conférence DPO 2024](#).

► **CEDPO a participé à l'évènement du CEPD sur les modèles « Consent or Pay » le 18 novembre 2024**

Le 18 novembre 2024, CEDPO a participé à l'évènement organisé par le Comité européen de la protection des données (CEPD) consacré aux futures lignes directrices sur les modèles « Consentir ou Payer ». Cet événement en ligne a réuni environ 200 participants

issus d'associations sectorielles, d'entreprises, d'ONG et du milieu académique pour discuter de ces modèles où les utilisateurs doivent choisir entre consentir au traitement de leurs données personnelles ou payer une redevance pour accéder à un service.

Les discussions ont porté sur plusieurs thèmes :

- **Consentement librement donné : éléments clés à évaluer**  
Analyse des critères essentiels pour garantir que le consentement des utilisateurs est réellement libre, sans pression ni déséquilibre de pouvoir.
- **Alternatives gratuites sans publicité comportementale**  
Exploration de la possibilité d'offrir une alternative gratuite avec des formes de publicité moins intrusives, comme la publicité contextuelle.
- **Définition d'une alternative équivalente**  
Discussion sur ce qui constitue une « alternative équivalente » permettant aux utilisateurs de refuser le traitement de leurs données personnelles tout en accédant à un service similaire en termes de qualité et de fonctionnalités.
- **Tarifification appropriée pour une alternative**  
Évaluation des critères pour déterminer si un tarif pour une alternative équivalente est justifié et proportionné, en tenant compte des droits fondamentaux et de l'autonomie des utilisateurs.

Cet échange a permis de recueillir des perspectives variées pour éclairer la rédaction des futures lignes directrices du CEPD sur ce sujet complexe. Aucun calendrier n'a été communiqué concernant la publication de ces lignes directrices. CEDPO continuera de suivre attentivement les développements et informera ses membres des avancées. Un grand merci aux membres de l'AFCDP pour leurs précieuses contributions.

► **CEDPO rejoint le groupe de travail du Bureau européen de l'IA pour l'élaboration du premier Code de bonne pratique sur les modèles d'IA à usage général**

CEDPO a été sélectionné par le Bureau Européen de l'IA pour rejoindre le groupe de travail chargé d'élaborer le premier Code de bonne pratique sur les modèles d'IA à usage général.

Parmi près de 1 000 organisations et individus du monde entier ayant soumis leur candidature, CEDPO a été choisi pour contribuer à cette initiative majeure. Ce Code de bonne pratique aura pour objectif de détailler les dispositions du règlement sur l'IA pour les fournisseurs de modèles d'IA à usage général et pour ceux présentant des risques systémiques. Nous sommes impatients de commencer ce travail essentiel et de contribuer ainsi à la bonne application du règlement sur l'IA au niveau de l'Union européenne.

► **CEDPO a participé à l'évènement du CEPD sur les modèles d'IA**

Les représentants du groupe de travail sur l'intelligence artificielle de CEDPO ont participé à l'évènement organisé par le Comité européen de la protection des données (CEPD) le 5 novembre. Cet évènement avait pour objectif de recueillir les contributions des parties prenantes dans le cadre de la demande d'avis de l'autorité irlandaise de protection des données (DPC) en vertu de l'article 64(2) du RGPD. Les discussions ont porté sur le traitement des données personnelles aux différentes étapes d'entraînement et d'utilisation des modèles d'IA, ainsi que sur les bases juridiques permettant ce traitement.

► Le groupe de travail sur **l'Intelligence artificielle** a dévoilé le deuxième numéro de la série « Micro-Insights », intitulé « Le DPO est-il la bonne personne pour devenir le responsable de l'intelligence artificielle ? ». Cet article explore l'évolution du rôle du DPO face au développement et à la démocratisation des systèmes d'intelligence artificielle, ainsi qu'à l'entrée en vigueur du règlement IA. Il examine également la pertinence de

confier au DPO le rôle de responsable de l'intelligence artificielle (AI Officer). Vous pouvez télécharger cet article (en anglais) [sur le site de CEDPO en cliquant ici](#). Retrouvez le premier numéro, sur la réglementation des modèles d'IA à usage général, en cliquant [ici](#).

### ► Newsletter

Vous pouvez désormais vous abonner à la newsletter de CEDPO directement [sur LinkedIn](#).

## Sujets récemment abordés dans AGORA AFCDP (réservé aux membres)

- Unnidata : Avez-vous été contacté ?
- Fuite de données massive chez l'opérateur Free
- Information réutilisation des données à des fins de recherche majeurs protégés (MR 004)
- Avez-vous des informations sur le consentement au traitement de données sensibles en milieu carcéral ?
- Quelles mesures RGPD pour les dispositifs ROC et FIDES visant les Établissements de santé ?
- Dans quel délai dois-je communiquer sur une violation de données ?
- Traitement sans fondement licite : Que doit faire le DPO : Alerter le RT ? Signalement auprès de la CNIL ?
- Comment gérez-vous le droit à l'image des agents dans le cadre de photos prises pour un évènement ?
- Notaire : quel fondement juridique ?
- Vidéoprotection augmentée/dépôts sauvages espace public ?
- Journée CNIL/RGPD le 4 décembre 2024 à Montpellier
- Quelle information aux personnes concernées lors de l'intégration d'un QR code dans un wallet mobile : jusqu'où aller dans le détail des flux de données ?
- Lettre AFCDP n° 209 - L'actualité des données personnelles - novembre 2024
- Vidéosurveillance sans enregistrement - formalités ?
- Faut-il transmettre son numéro fiscal à Vinted dans le cadre de la directive DAC7 ?
- L'autorisation du droit à l'image et l'engagement de confidentialité concernant le traitement des données à caractère personnel par les salariés ont-ils une valeur juridique s'ils sont « signés » par
- Grille de salaire DPO
- France : La CNIL propose de nouveaux webinaires pour les professionnels
- Est-il nécessaire de faire une AIDP pour l'installation de caméras de vidéosurveillance avec lecture de plaques d'immatriculation ?
- Caméra piéton et AIPD ?
- Que pensez-vous de cette suggestion d'une collaboration CLUSIF/AFCDP pour un GT commun sur l'IA ?
- Durées de conservation en matière RH et code du travail : Comment arbitrer des intérêts opposés ?
- Prise de note basé sur l'IA : Avez-vous déjà évalué des traitements associés à cette pratique et/ou pris des mesures techniques et organisationnelles complémentaires ?
- France Travail/Inscription automatique : Faut-il recueillir le consentement et sous quelle forme ?
- Si votre réseau num, ordi, tel, impr sont HS suite à ransomware : avez-vous prévu un mode dégradé comme pour les autres services de votre collectivité ?



- Les données collectées en ACM sont-elles considérées comme des données de santé au sens du RGPD et nécessitent-elles un hébergement certifié HDS en cas d'externalisation ?
- Préparation d'un questionnaire cyber sécurité pour les entités soumises à NIS2 (Données de santé)
- Quelle mention légale doit apparaître sur les chèques déjeuner ?
- Abus envers un DPO : avez-vous des suggestion de réaction ?
- Est-ce que vous avez un kit de conformité RGPD pour les applications mobiles/app mobile, à destination des éditeurs ou développeurs d'app ?
- Y a-t-il un délai de prescription applicable à un contrôle CNIL ?
- Nouveau guide de la CNIL
- Analyse d'impact pour Office 365 ?
- Comment rédiger une politique de confidentialité pour les collaborateurs clairs ?
- Google Tag Manager : Quelle base légale ?
- Lancement de l'intergroupe vidéoprotection augmentée - 25 novembre de 14 h à 16 h (visio)
- Absence de DPO : Kourou devra payer 6900 euros... et peut-être plus
- Agence d'intérim (ETT) et entreprise utilisatrice (EU) : quels transferts de données autorisés dans le cadre des accidents du travail ?
- Demande DCP pour Lutte anti-fraude : peut-on transmettre des données personnelles ?
- Quel lien entre les collectivités et les directeurs d'école ?

## Délibérations de la CNIL

### Les délibérations de la CNIL publiées au Journal officiel ce mois-ci

20/11/2024 - [Décision du 7 novembre 2024 relative à l'organisation des services de la Commission nationale de l'informatique et des libertés](#)

## L'actualité des données personnelles (France)

### **Procès du pirate qui s'était attaqué au Pass Navigo**

Un jeune homme de vingt ans de l'Est parisien a raconté le 7 novembre ses errances informatiques aux juges de la 13e chambre correctionnelle du tribunal judiciaire de Paris. Après avoir lancé des attaques par bourrage d'identifiants contre Île-de-France Mobilités, ses huit millions de requêtes envoyées lui avaient permis l'accès à 4 230 comptes d'utilisateurs. « [Un enfant de douze ans peut faire la même chose, j'ai appris en regardant une vidéo sur YouTube](#) », s'est maladroitement défendu le jeune homme. Son avocat ajoute que « n'importe qui aurait pu accéder aux données d'Île-de-France Mobilités à cause de l'absence d'authentification forte ». Le délibéré sera rendu le 10 décembre. (Merci à Bruno Rasle)

### **Surveillance disproportionnée des salariés : 75 000 € d'amende proposés**

La Formation restreinte de la CNIL s'est réunie le 14 novembre 2024 pour étudier un unique dossier, une session dont notre confrère Bruno Rasle a fait un compte rendu sur Agora. Dans cette affaire, une entreprise est mise en cause pour une surveillance disproportionnée de ses employés (notamment via un logiciel installé en mode « silencieux » destiné à surveiller la productivité des salariés). Bien que l'entreprise ait coopéré et corrigé rapidement les manquements, la CNIL a proposé une amende de

75 000 euros et la publication de la décision, attendue pour la fin de l'année. Bruno a complété le compte rendu par une série de commentaires, et attire l'attention des membres de l'AFCDP sur les risques que soulève l'utilisation du logiciel « Time Doctor », à l'origine de l'affaire.

### **Lunettes connectées : la CNIL enquête**

[Le site Tech&Co de BFM TV a indiqué le 30 octobre 2024](#), qu'après à une première plainte actuellement en instruction, la CNIL se penche sur la légalité de l'utilisation des lunettes connectées Meta Ray-Ban, commercialisées en partenariat avec EssilorLuxottica. Intégrant une caméra dans leur branche, ces lunettes permettent la captation vidéo continue et la diffusion en direct sur les réseaux sociaux Facebook et Instagram, soulevant d'importantes questions juridiques relatives à la protection de la vie privée. Cette innovation technologique se trouve à la croisée de plusieurs cadres réglementaires, notamment le droit à l'image, le Code de la sécurité intérieure concernant la vidéosurveillance sur la voie publique, et la protection des données personnelles sous l'égide du RGPD. La CNIL devra spécifiquement se prononcer sur la conformité de ces dispositifs au regard de la réglementation sur les données personnelles, dans un contexte où la frontière entre innovation technologique et respect des libertés individuelles devient de plus en plus ténue. La décision de l'autorité pourrait ainsi créer un précédent important pour l'encadrement des dispositifs de capture vidéo portables en France.

### **Protection des consommateurs et des données personnelles : la CNIL et la DGCCRF renforcent leur coopération**

Le 18 novembre 2024, [la DGCCRF et la CNIL ont conclu un nouveau protocole de coopération](#) qui modernise leur convention initiale de 2011, renforçant significativement leur collaboration dans la régulation de l'économie numérique. Ce protocole prévoit notamment un approfondissement des échanges d'informations sur les infractions au droit de la consommation et à la protection des données personnelles, incluant désormais explicitement les dossiers traités au niveau européen. Les deux autorités s'engagent à établir des analyses communes sur les législations, avec un focus particulier sur l'harmonisation des interprétations juridiques, notamment concernant la définition des dark patterns, et prévoient une mutualisation de leurs expertises techniques en matière d'outils et de méthodologies d'enquête. Cette coopération renforcée s'inscrit dans le cadre plus large de la loi SREN et vient compléter la convention tripartite signée avec l'Arcom en juin 2024, consolidant ainsi l'écosystème réglementaire français du numérique. Selon l'annonce de la CNIL, cette initiative marque une avancée majeure dans la coordination des régulateurs français du numérique, établissant un cadre opérationnel pour une meilleure protection des droits des consommateurs dans l'environnement digital, notamment en matière de transparence algorithmique et de lutte contre les pratiques commerciales abusives.

### **Reconnaissance faciale par la police : LFI saisit la justice**

Le groupe LFI à l'Assemblée nationale [a saisi la justice le 19 novembre 2024](#) concernant l'utilisation présumée illégale du logiciel de reconnaissance faciale Briefcam par la police française entre 2015 et 2023. Ce logiciel israélien qui permet l'exploitation d'images de vidéosurveillance via une intelligence artificielle, aurait été déployé sans l'autorisation préalable de la CNIL et hors de tout cadre légal, selon le député Aurélien Saintoul qui met en cause plusieurs ministres de l'Intérieur successifs. Bien qu'un rapport des inspections générales publié le 28 octobre 2024 ne relève qu'un « cas unique d'utilisation illégale de la reconnaissance faciale sur près de 600 exploitations du logiciel », les députés LFI contestent cette version et soulignent que même la vidéosurveillance algorithmique sans reconnaissance faciale n'était pas autorisée avant la loi de 2023 sur la sécurisation des JO.

## **Une suite numérique souveraine pour la sphère publique ?**

Autour d'une authentification unique, [la DSI de l'État poursuit ses travaux pour mettre à disposition une suite d'outils collaboratifs en open source](#) (sur certains points en mutualisant ses efforts avec l'Allemagne). Pour ce faire, la Dinum s'est appuyée sur AgentConnect (une version de France Connect permettant aux agents de l'administration de s'authentifier sur des systèmes d'information), et sur son évolution vers ProConnect, qui étend ce principe aux partenaires de l'administration centrale, comme la fonction publique hospitalière et les collectivités avant de s'étendre à l'ensemble de la sphère publique et des professionnels partenaires. Parmi les prochaines cibles, l'envoi ou la récupération de fichiers sur le drive de la Suite numérique depuis n'importe quelle application connectée ou encore la capacité à basculer en un clic du calendrier à la visioconférence. Dans le cadre d'un PIA réalisé sur un projet envisageant d'utiliser des solutions proposées par les GAFAM, il conviendra donc d'expliquer pourquoi elles ont été préférées à cette suite souveraine. (Merci à Bruno Rasle)

## **D'où proviennent les données qui ont fuitées ?**

Comme le rappelle [ce billet](#), il arrive que les pirates se contentent de proposer à la vente des données personnelles qu'ils n'ont jamais exfiltrées... mais se limitent à « rhabiller » des données accessibles librement ou volées par d'autres dans le passé. Certaines critiques à l'égard de responsables de traitement accusés de « cacher » des violations de données perdraient alors de leur pertinence. Cela pose aussi la question de l'utilisation possible de ces données pour nuire à un responsable de traitement, par exemple en publiant anonymement des données anciennes pour prétendre à une nouvelle violation que le RT a l'obligation de déclarer.

## **Microsoft utilise vos données pour entraîner son IA**

[Microsoft a semble-t-il discrètement introduit](#) une fonctionnalité nommée « Connected experiences » dans ses applications Office 365, permettant l'analyse automatique et l'utilisation des contenus des utilisateurs pour l'entraînement de ses modèles d'IA. Cette fonctionnalité, [exposée en détail sur le site de l'éditeur](#), est activée par défaut, et s'appuie sur une clause contractuelle accordant à Microsoft une licence mondiale et gratuite pour exploiter, copier, transmettre et redistribuer le contenu des utilisateurs. Les personnes utilisant Microsoft 365, notamment sur Word, Excel, PowerPoint et Outlook, sont potentiellement concernées, avec environ 345 millions d'utilisateurs impactés par ce paramétrage. Les utilisateurs peuvent désactiver cette fonctionnalité, mais la procédure suit un parcours de sept étapes dans les paramètres de confidentialité de leurs applications Office, détaillés par un spécialiste dans [un article sur X/Twitter](#).

## **La CEDH valide l'usage par la CAF de l'adresse IP pour lutter contre la fraude**

Dans [un arrêt du 5 novembre 2024](#), la Cour européenne des Droits de l'Homme a jugé licite la collecte et l'utilisation de l'adresse IP dans le cadre de la répression de la fraude aux allocations sociales. Un allocataire de la CAF s'était vu suspendre son RSA après enquête. Il utilisait un VPN qui produisait une adresse IP identifiée comme « hors de France », alors qu'il résidait bien en France, mais une anomalie dans sa déclaration de résidence rendait impossible le contrôle de sa situation. La CEDH a considéré que la collecte de l'adresse IP, par ailleurs minimisée et collectée pour le seul contrôle du lieu de résidence, reposait bien sur une base légale, et était permise « eu égard à l'appréciation accordée aux autorités dans le domaine de la répression de la fraude aux allocations sociales » et « ne portait manifestement pas une atteinte disproportionnée au droit du requérant au respect de sa vie privée. »

## **Reconnaissance faciale : un rapport dénonce l'usage illégal du logiciel BriefCam par la police en 2023**

[Le 14 novembre 2023, Disclose](#) publie une enquête dévoilant l'utilisation illégale d'un logiciel de reconnaissance faciale par les services de police français depuis 2015. Un an plus tard, [le rapport ministériel du 28 octobre 2024](#) approfondit ces révélations. Le logiciel israélien BriefCam, outil d'analyse vidéo aux capacités algorithmiques avancées, a été déployé dans un contexte de flou juridique. Capable de compresser des heures de séquences en minutes, de détecter des mouvements et de générer des vignettes, il intègre une fonctionnalité de reconnaissance faciale introduite en novembre 2018. Suite à la publication de Disclose, le ministre de l'Intérieur a commandé une enquête interne confiée à l'Inspection générale de l'administration, de la police nationale et de la gendarmerie nationale. Le rapport pointe un usage unique dans des conditions illégales survenu lors des émeutes de l'été 2023.

## **L'Arcom marque un tournant dans la protection des mineurs**

Chaque mois, 2,3 millions de jeunes internautes se retrouvent exposés à des contenus pornographiques, malgré l'interdiction légale. Face à ce constat alarmant, [l'Arcom et la CNIL](#) déploient un dispositif inédit de protection. Le 26 septembre 2024, la CNIL valide un [référentiel](#) technique ambitieux, fruit de la loi SREN du 21 mai. L'objectif est ainsi de contraindre les sites à mettre en place un système de vérification d'âge robuste et respectueux de la vie privée. Adopté le 9 octobre 2024, le nouveau cadre réglementaire impose un délai de trois mois aux plateformes pour se conformer. Les sites devront désormais faire appel à un tiers vérificateur indépendant, garantissant un double anonymat. Une période transitoire permettra une mise en œuvre progressive via la vérification par carte bancaire. Au-delà de la technique, l'Arcom appelle à une stratégie globale de protection numérique des mineurs, suggérant le développement d'outils de parentalité numérique innovants.

## **Malakoff Humanis met en place une stratégie de purge des données**

Lors de Big Data & IA Paris, [Malakoff Humanis](#) a présenté un dispositif conçu pour identifier et supprimer les informations devenues obsolètes, s'appuyant sur une méthodologie rigoureuse et des outils adaptés à cette tâche complexe. Le projet prévoit deux types de purges, locales pour des périmètres ciblés et chaînées pour les systèmes connectés. L'entreprise a d'abord identifié les données concernées, les applicatifs impliqués et les durées de conservation avant de définir les règles de suppression. Ces processus concernent actuellement 30 applications et s'étendent progressivement. Pour centraliser et documenter ces opérations, Malakoff Humanis utilise une version adaptée de la plateforme Datagalaxy. Celle-ci permet de cartographier les données, structurer les règles de purge et visualiser les flux pour garantir la cohérence des suppressions. Une gouvernance dédiée a été mise en place, impliquant une trentaine de collaborateurs issus des domaines métier, technique, juridique et data.

## **La CNIL clôture la procédure contre la commune de Kourou après la désignation d'un DPO**

La CNIL a annoncé [la clôture](#) de la procédure engagée à l'encontre de la commune de Kourou, suite à sa mise en conformité avec l'obligation de désignation d'un DPO. La collectivité territoriale avait fait l'objet d'une mise en demeure en juillet 2023 pour non-respect de l'article 37 du RGPD, qui impose aux autorités publiques la désignation d'un DPO. Face à cette injonction, la commune a entrepris les démarches nécessaires et désigné officiellement un délégué à la protection des données en septembre 2023.

## **Véhicules de transport : la CNIL précise les règles d'usage des dispositifs de vidéosurveillance augmentée**

[La CNIL a publié le 19 novembre des précisions](#) concernant l'installation de caméras augmentées dans les habitacles des véhicules de transport de marchandises. Ces dispositifs, combinant captation vidéo et analyse algorithmique, doivent répondre à des finalités strictement définies : la sécurité des biens et des personnes, la formation des conducteurs, ou encore l'amélioration de la conduite. La CNIL souligne que leur déploiement nécessite une analyse d'impact préalable et exige la mise en place de garanties spécifiques pour protéger les droits des conducteurs. Le traitement des données biométriques est particulièrement encadré, étant soumis au principe de minimisation et à des conditions de conservation limitée. L'autorité insiste également sur l'obligation d'information transparente des conducteurs et la nécessité d'obtenir l'avis des instances représentatives du personnel avant tout déploiement.

### **Les entreprises françaises face à une multiplication des incidents de cybersécurité**

Une [étude publiée](#) en novembre par la [société de cybersécurité Kaspersky](#) révèle que les entreprises françaises ont été confrontées à une moyenne de 14 incidents de cybersécurité sur l'année écoulée, témoignant d'une intensification significative des menaces numériques. Cette analyse, s'appuyant sur les retours d'expérience de 53 entreprises, met en lumière que les incidents majeurs, nécessitant l'intervention d'experts en cybersécurité, représentent 30 % des cas. L'étude souligne particulièrement la vulnérabilité des entreprises aux attaques par rançongiciel, avec 19 % des organisations touchées ayant subi au moins une attaque aboutie. Face à cette situation, les entreprises renforcent leurs dispositifs de défense, notamment en déployant des solutions d'authentification multi-facteurs et en augmentant leurs investissements en cybersécurité, qui s'élèvent en moyenne à 4,1 % du budget informatique global.

## **L'actualité des données personnelles (Belgique)**

### **Quand l'information du public prime sur la protection des données**

[Le site GDPRHub de Noyb a signalé](#) une [décision du 14 août 2024](#) par laquelle l'autorité de contrôle belge (APD) a tranché en faveur d'un site Web privé qui republiait des informations sur les mandats et rémunérations d'une dirigeante d'entreprise publique, malgré sa demande d'effacement basée sur l'article 17 du RGPD. L'APD a considéré que le droit à l'effacement n'était pas applicable dans ce cas, s'appuyant sur l'exception prévue à l'article 17(3)(a) du RGPD relative à la liberté d'expression et d'information, même si le responsable du traitement n'était pas un journaliste professionnel. Cette décision s'inscrit dans la lignée de la jurisprudence de la CJUE et de la CEDH, reconnaissant que le rôle de « chien de garde public » traditionnellement dévolu à la presse peut également être exercé par des citoyens ou entités privées. Le caractère déjà public des informations et le statut de « personnage public » de la plaignante ont pesé dans la balance des intérêts effectuée par l'APD, qui a estimé que l'objectif de transparence sur l'utilisation des fonds publics justifiait le maintien de la publication. Cette affaire avait été initialement portée devant la CNIL française puis transférée à l'APD belge en vertu de l'article 56(1) du RGPD. Elle illustre l'articulation entre protection des données personnelles et droit à l'information du public dans le contexte de la transparence administrative.

## **L'actualité des données personnelles (Europe)**

### **Pour l'application du RIA, l'Irlande désigne neuf autorités en charge de l'IA**

Dans [un communiqué du 30 octobre 2024](#), le Gouvernement irlandais a annoncé, en application du Règlement sur l'IA (RIA), la désignation de neuf autorités publiques

nationales chargées de la protection des droits fondamentaux. Ces autorités, incluant notamment la Commission de Protection des Données, la Commission des Médias et la Commission irlandaise des Droits de l'Homme et de l'Égalité, se verront attribuer des pouvoirs supplémentaires à partir du 2 août 2026 pour examiner la documentation des développeurs et déployeurs de systèmes d'IA à haut risque. Le communiqué rappelle que cette désignation, qui doit être notifiée à la Commission européenne avant le 2 août 2025, représente la première obligation nationale de l'Irlande dans le cadre du RIA. Cette liste des autorités désignées restera sous revue ministérielle et pourra être mise à jour à tout moment, reflétant ainsi la nature évolutive de la régulation de l'IA dans le cadre d'une mise en œuvre progressive sur 36 mois des dispositions du RIA.

### **Frontex cherche un nouveau DPO**

Frontex, l'agence européenne de contrôle des frontières a annoncé être à la recherche d'un nouveau DPO. Si les candidatures sont closes depuis le 29 novembre 2024, l'annonce indique que [le poste est basé en Pologne](#). Cela pourrait avoir un rapport avec [le blâme](#) que le CEPD/EDPS avait adressé à Frontex en avril 2022 pour avoir migré vers le Cloud (Microsoft 365, Microsoft Azure, AWS) sans évaluation appropriée de la protection des données. Le CEPD/EDPS reprochait (entre autres) à Frontex de ne pas avoir démontré une recherche réelle de solutions alternatives moins intrusives, et exigeait que le PIA soit revu et amendé (un document que l'on aurait aimé lire). (Merci à Bruno Rasle)

### **Données non purgées ? 900 000 € de sanction**

Un prestataire de services basé à Hambourg conservait des données à caractère personnel jusqu'à cinq ans après la date prévue. L'Autorité locale [inflige une amende de 900 000 euros](#). Pour cette autorité, « Il n'est pas acceptable que les acteurs travaillant dans les secteurs numériques n'aient pas développé de procédure de suppression cohérente. » (Merci à Bruno Rasle)

### **Grande-Bretagne : le régulateur défavorable aux grosses sanctions contre les géants du numérique**

Dans [une interview au Times le 18 novembre 2024](#), le commissaire à l'information britannique John Edwards (le patron de la CNIL locale) remet en question l'efficacité des amendes massives contre les géants technologiques, arguant que des sanctions de centaines de millions de livres ne feraient que bloquer son bureau dans des litiges interminables. Contrairement aux régulateurs européens qui ont infligé des amendes de 3,2 milliards d'euros depuis 2018, l'ICO britannique préfère collaborer avec l'industrie technologique pour assurer la conformité aux lois, comme le Code pour Enfants qui régule la gestion des données des jeunes. Edwards souligne qu'infliger une amende de 10 milliards d'euros à Meta ne les pousserait pas à effectuer les changements demandés et les engagerait plutôt dans des procédures judiciaires longues et coûteuses. Cependant, certains experts comme Ben Rapp de Securys estiment que le régulateur britannique devrait adopter une approche plus stricte pour protéger les droits et libertés des citoyens. (Merci à Bruno Rasle)

### **Allemagne : Meta jugé responsable de « préjudice moral »**

Selon [le site The Media Leader](#), la Cour fédérale de justice allemande a déclaré Meta responsable de « préjudice moral » suite à une fuite massive de données personnelles de 533 millions d'utilisateurs en 2019. La décision, potentiellement déterminante pour des milliers de recours, établit qu'une simple perte de contrôle des données personnelles constitue un préjudice juridiquement réparable, même sans utilisation abusive effective. Meta, qui conteste la décision, pourrait être condamné à verser des dommages et intérêts, s'inscrivant dans une série de sanctions européennes récentes pour manquement à la protection des données. Toutefois, avant que l'affaire ne soit à nouveau jugée par la Cour

d'appel de Cologne, Meta a fait part de son désaccord avec la Cour fédérale de justice concernant les dommages-intérêts, dont l'entreprise estime qu'ils ne sont pas conformes aux récents arrêts de la Cour de justice de l'UE, des demandes similaires ayant déjà été rejetées plus de 6 000 fois par les tribunaux allemands.

### **L'usage des algorithmes pour détecter la fraude et ses dérives discriminatoires**

Aux Pays-Bas, l'utilisation [d'algorithmes par les organismes publics](#) vient d'essuyer une critique sévère. Le Dienst Uitvoering Onderwijs (DUO), l'organisme national de l'éducation, s'est vu condamner par l'autorité de protection des données (AP) pour une méthode discriminatoire de détection de fraude de la bourse locale étudiante. Le mécanisme reposait sur un système de notation calculant un « score de risque » à partir de critères non objectivés : type d'études, proximité géographique familiale et tranche d'âge. Entre 2013 et 2022, 21 500 étudiants ont subi des investigations ciblées, avec un biais manifeste envers les populations migrantes.

### **Ciblage ou paiement : Meta cède à la demande européenne et lance la publicité contextuelle**

Sous la pression des régulateurs européens, [Meta](#) bouleverse son modèle publicitaire. L'entreprise proposera une option gratuite de publicité contextuelle moins invasive, répondant aux critiques sur l'exploitation des données personnelles. Cette transformation fait suite au système controversé « ciblage ou paiement » instauré fin 2023. En parallèle, Meta réduit de 40 % le tarif de l'abonnement sans publicité ciblée, atténuant les reproches des défenseurs des consommateurs. L'entreprise maintient néanmoins une posture défensive face aux exigences de la Commission européenne, qu'elle estime dépassant le cadre réglementaire.

### **L'EDPB émet des réserves sur l'extension du régime de conservation des données**

Dans une [déclaration publiée le 4 novembre](#), le Comité européen de la protection des données (EDPB) exprime ses inquiétudes concernant les 42 recommandations émises par le groupe de haut niveau de la Commission et du Conseil de l'UE sur l'accès aux données par les forces de l'ordre. Si l'EDPB approuve le principe d'une harmonisation du régime de conservation des données, il souligne que son extension à l'ensemble des gestionnaires de données contreviendrait à la jurisprudence établie. Les régulateurs pointent l'absence de preuves objectives étayant ces recommandations et alertent sur les risques d'atteinte aux droits fondamentaux en matière de protection des données et de vie privée. Par ailleurs, l'EDPB défend fermement le chiffrement, considéré dans les recommandations comme un obstacle à surmonter. Face à ces enjeux, le Comité exhorte les instances européennes à conduire une évaluation rigoureuse de la faisabilité juridique, dans le strict respect du cadre réglementaire de protection des données.

### **IA générative : le MEDEF identifie les données privées comme avantage stratégique européen**

Dans un [rapport conjoint](#) avec le think tank Digital New Deal, le MEDEF met en lumière l'importance stratégique des données privées pour la compétitivité européenne dans le domaine de [l'intelligence artificielle générative](#). Face à la domination américaine dans les infrastructures et technologies de l'IA, l'organisation patronale identifie les données privées comme l'ultime levier de différenciation pour les entreprises européennes. Le rapport préconise la création d'espaces sectoriels de partage de données privées, s'inscrivant dans la stratégie européenne des données, pour constituer un véritable marché unique. Cette mutualisation permettrait d'alimenter des modèles d'IA générative européens et représenterait une alternative à la captation des données par les géants technologiques américains. Le MEDEF souligne l'urgence de cette démarche collaborative, établissant un

parallèle avec les occasions manquées lors de l'émergence du Web dans les années 1990-2000.

### **Data Privacy Framework : l'EDPB salue les avancées mais appelle à renforcer la mise en œuvre**

L'EDPB a publié son premier [rapport d'évaluation du Data Privacy Framework \(DPF\)](#), soulignant les progrès significatifs réalisés dans la mise en œuvre du mécanisme de transfert de données UE-États-Unis. Le Comité reconnaît notamment les efforts du Département du Commerce américain dans le déploiement du processus de certification des entreprises. Toutefois, plusieurs points d'attention émergent de cette analyse : le faible nombre de plaintes reçues durant la première année d'application, la nécessité de clarifier les exigences relatives aux transferts ultérieurs de données et la définition des « données relatives aux ressources humaines ». Concernant l'accès des autorités publiques américaines aux données, l'EDPB salue les garanties introduites par le décret 14086, tout en appelant à une meilleure démonstration de l'application des principes de nécessité et de proportionnalité. Si les mécanismes de recours ont été substantiellement améliorés, notamment grâce aux prérogatives de la Cour de révision de la protection des données, le Comité recommande d'en faire une priorité lors des prochaines évaluations, qu'il souhaite voir intervenir dans un délai inférieur à quatre ans.

## **L'actualité des données personnelles (Monde)**

### **Surveillance de la localisation et des mouvements des employés**

L'étude « [Tracking Indoor Location, Movement and Desk Occupancy in the Workplace](#) » décrit les fonctionnalités que des fournisseurs, tels que Cisco ou Juniper, ont implémenté dans leurs solutions de réseau WiFi destinées aux entreprises et qui peuvent permettre, à tout moment, de « cybersurveiller » les salariés, y compris jusqu'aux toilettes. Cisco affirme ainsi avoir jusqu'à présent traité 17 200 milliards de « points de données de localisation » collectés via plus de trois-millions de points d'accès wifi installés dans 250 000 bâtiments de par le monde. Le document évoque plusieurs cas où les protestations des travailleurs ont finalement conduit à leur désactivation. (Merci à Bruno Rasle)

### **Le contrôle de l'utilisation des données personnelles dans l'IA : les régulateurs précisent leur position**

Dans une [déclaration conjointe](#) adoptée le 28 octobre, 16 autorités de protection des données actualisent leur position sur l'utilisation des données personnelles pour l'entraînement des modèles d'IA, approfondissant leur [première analyse](#) d'août 2023. Les régulateurs reconnaissent qu'aucune solution unique ne peut garantir une protection absolue contre le scraping illégal de données personnelles, préconisant plutôt une approche défensive multicouche et évolutive. La déclaration souligne particulièrement l'insuffisance des seules clauses contractuelles pour encadrer la collecte par des tiers, appelant à la mise en place de mécanismes de contrôle effectifs. Concernant les réseaux sociaux qui collectent des données sur leurs propres plateformes, les autorités rappellent simplement l'obligation de conformité tant aux réglementations existantes sur la protection des données qu'aux futures législations spécifiques à l'IA, illustrant ainsi les limites actuelles du cadre réglementaire face à ces nouveaux enjeux.

### **Cyberattaques financières : l'utilisation stratégique de LinkedIn par des pirates nord-coréens**

Microsoft vient d'alerter sur une campagne d'attaques menée par des acteurs malveillants nord-coréens, [exploitant LinkedIn à des fins frauduleuses](#). Ces cybercriminels, identifiés



comme appartenant au groupe Lazarus, créent de faux profils d'entreprises technologiques et de capital-risque pour cibler des sociétés de cryptomonnaies et des startups. Leur mode opératoire consiste à établir une relation de confiance avec leurs cibles via des échanges professionnels prolongés, avant de les inciter à installer des logiciels malveillants sous couvert d'opportunités d'investissement. Microsoft souligne que ces attaques ont déjà permis de dérober plusieurs millions de dollars, notamment en cryptomonnaies. Cette nouvelle forme d'ingénierie sociale sophistiquée illustre l'évolution des techniques exploitant les réseaux professionnels comme vecteur d'infiltration.

*Directeur de la publication : **Paul-Olivier Gibert**, Président de l'AFCDP.*

*Rédaction : **Nathalie Brunet, Marina Casas, Elizabeth Thomas, Patrick Blum.***

*Directeur de la publication : Paul-Olivier Gibert, Président de l'AFCDP. Afin que cette lettre soit à la fois un outil d'information, mais également d'échanges, vous pouvez contacter pour toute réaction, commentaire et contribution, la rédaction : Patrick Blum - <mailto:delegate.general@afcdp.net>*

*Si vous pensez que cette lettre peut intéresser des tiers, n'hésitez pas à leur signaler son existence.*

***Si vous ne souhaitez plus recevoir cette lettre d'informations, merci de le signaler par retour d'email (adresse <mailto:back-office@afcdp.net>).** Si vous recevez cette lettre électronique au format html, soyez informé qu'elle dispose d'indicateur permettant de s'assurer de sa bonne réception (webug) afin de mettre à jour la liste des destinataires, et de mesurer l'intérêt global pour les sujets abordés. Merci de vous reporter à la configuration de notre navigateur pour apporter les modifications ad hoc si vous ne souhaitez pas que cette information nous parvienne*