



## ***Lettre AFCDP n°144 - L'Actualité des données personnelles – Décembre 2018***

*Le Conseil d'administration et toute l'équipe de permanents de l'AFCDP vous souhaite d'excellentes Fêtes de fin d'année !*

### **Vie de l'Association**

#### **Université AFCDP 2019 : plus aucune place !**

Bien que nous ayons négocié avec la Maison de la Chimie l'extension au maximum de leur capacité d'accueil, nous sommes dans l'obligation de refuser des inscriptions pour la plus ancienne et plus grande conférence en France sur la conformité Informatique et Libertés. Pour mémoire, comme après les douze éditions précédentes, l'intégralité des supports visuels et des comptes-rendus seront mis à disposition des membres dans le réseau social privé qui leur est réservé.

#### **Création d'un nouveau groupe AFCDP dédié aux banques**

Le première réunion du nouveau groupe de travail AFCDP « Banque & Finances » s'est tenue le [lundi 3 décembre 2018](#) chez Neuflyze OBC, en présence d'une trentaine de DPO d'acteurs concernés. Les thèmes qui vont faire l'objet de travaux et de réflexion ont été identifiés : Identification (s'il y en a) des contradictions entre le RGPD et les réglementations nationales et européennes applicables au secteur Banque, Portabilité RGPD vs Open Banking, Conformité RGPD des traitements de LAB, Conformité RGPD des traitements comportant des informations sur des infractions/condamnations pénales (ou autres données dites "sensibles"), Détermination et gestion des durées de conservation spécifiques au monde bancaire, Gestion de la trésorerie, etc.

#### **Bravo au groupe AFCDP Méditerranée !**

La conférence AFCDP qui s'est tenu le 23 novembre à Nice [à l'initiative du groupe AFCDP Méditerranée](#) a rencontré un vrai succès. Les supports de présentation et les comptes-rendus vont être déposés dans AGORA AFCDP très prochainement. Nous travaillons également sur un projet de conférence AFCDP qui se tiendra à Lyon, à l'initiative du groupe AFCDP "Lyon +".

#### **Succès de la première réunion AFCDP à Fort-De-France**

Une quinzaine de DPO martiniquais étaient réunis le 27 novembre à l'Espace Sonate (Fort-De-France) pour faire connaissance et pour déterminer, ensemble, quel va être leur plan d'action (fréquence des réunions, thèmes qui vont être étudiés, etc.). Ils ont bénéficié d'une intervention qui avait pour thème [la gestion des notifications des violations de données](#).

#### **DPO externes**

Le 26 novembre s'est tenue une nouvelle réunion, passionnante, dédiée aux DPO externes (un compte-rendu va être prochainement posté). [Y ont été listés quelques-uns des sujets que les membres concernés pensent traiter lors des réunions suivantes](#) : Livrables : quels critères pour évaluer la qualité plutôt que la quantité ? Contrat type : les clauses incontournables pour un DPO externe ; Justifier des compétences pour la fonction, la Certification des compétences du DPO est-elle la seule solution ? Comment entretenir le lien de confiance dans le temps avec le

client malgré la distance ? Comment être impliqué par le *privacy by design* ou *privacy by default* lorsqu'on n'est pas en interne ? Des travaux à suivre !

### **Les lignes directrices du CEPD en un seul recueil !**

Long et complexe, le RGPD nécessite d'être éclairé et complété par des éléments de doctrine. Au premier rang de ceux-ci figurent les lignes directrices formalisées par le Comité européen de la protection des données (CEPD), qui a remplacé le G29 le 25 mai 2018. Après avoir proposé le RGPD en version indexée et annotée, l'AFCDP met à disposition des DPO les lignes directrices du CEPD, en français, [regroupées dans un seul document](#).

Et toujours...

[Le job board dédié au DPO](#)

[La place de marché RGPD \(modalités d'utilisation\)](#)

[La Charte de déontologie du DPO](#)

### **Agenda des prochaines réunions de l'AFCDP**

◆ 11 décembre - Paris - [La Nuit du DPO](#)

◆ 14 décembre - Toulouse - [Réunion du groupe AFCDP « Toulouse »](#)

◆ 16 janvier - Paris - [13e Université AFCDP des DPO](#)

### **Thèmes récemment abordés dans AGORA AFCDP (réservés aux membres)**

Archivage papier de données de santé : faut-il être HDS ?

Gestion des courriers : comment gérez-vous les droits de leurs auteurs ?

Champ application RGPD hors UE : nos établissements situés à l'étranger y sont-ils soumis ?

"Cartographie des données" : Quelles sont les informations à recenser ?

Gestion d'activités périscolaire dans le Cloud avec données de santé : que faire ?

Organismes de formation : Responsable de traitement ou Sous-traitant ?

Pouvons-nous publier le nom de notre chauffeur/conducteur impliqué dans un accident ?

Quelle est la responsabilité des agents qui assistent les publics en difficulté ou fragiles ?

AIVP : à quel moment la faire ? Avant ou après l'appel d'offre ?

Qui est responsable de traitement dans une couveuse d'entreprises ?

Collecte de données personnelles lors d'interviews : pouvons-nous les conserver pour des raisons historiques ?

Le DPO peut-il accéder aux données personnelles ?

Changement de Délégué : Que devons-nous faire ?

Report sanctions pécuniaires pour les organismes publics : info ou intox ?

Vol d'ordinateur professionnel : qui doit déclarer auprès de la police ?

Quelle procédure d'accès au dossier usager dans le secteur médico-social ?

Faut-il anonymiser les données dupliquées dans un outil décisionnel ?

Intervention d'un journaliste dans une école : quelles autorisations (droit à l'image) et quelle préparation ?

Réponse à une demande de droit d'accès aux données : faut-il détailler toutes les recherches même infructueuses ?

Un salarié peut-il s'opposer à ce que ses données RH se retrouvent dans un outil collaboratif en ligne ?

Utilisation de la liste électorale : détournement de finalité ?

Missions de contrôle et d'audit du DPO (art. 39.1.b) : êtes-vous prêts ?

Media - Libre antenne : quelles pratiques concernant l'enregistrement des appels téléphoniques ?

Borne à selfies (avec le Père Noël) : qui est responsable du traitement ?

Une entreprise peut-elle utiliser l'adresse LinkedIn d'un salarié pour un usage professionnel ?  
Que faire après avoir déterminé la durée de conservation des données ?  
Quel hébergeur de site web recommandez-vous ?  
Personne vulnérable + traitements RH = AIPD ?  
Documentation interne « registre des violations » : à quoi ressemble-t-elle ?  
La SACEM est-elle un "tiers autorisé" ?  
A quoi correspond la notion de « communication électronique » dans les AIPD ?  
Quels sont vos conseils pour la rédaction d'une charte informatique ?  
Accidentologie et outils de géolocalisation des véhicules : les données collectées vous paraissent-elles proportionnées ?  
Tour opérateur et réseau d'agences : RT-ST, ST-RT ou RT-RT ?  
Un DPD Mutualisé peut-il être en même temps sous-traitant ?  
Dans le cadre du RGPD : pouvons-nous utiliser Outlook ?  
Lettre RGPD : une escroquerie ?  
Demande de communication de coordonnées par un avocat : Faut-il y faire droit ?  
Gestion des congés payés et modulation du temps de travail : un traitement "à part" ?  
Quelles sont les exceptions à la réalisation d'une DPIA ?  
Communication de la liste du personnel aux syndicats (élections CSE) : autorisée ?  
Obligation de vigilance Travailleurs étrangers : une attestation générale de travail non dissimulé peut-elle suffire ?  
Comment lister les applications mobiles dans le registre de traitement ?  
Statistiques de données de santé via Google Analytics : les dérogations liées à l'article 89 du RGPD s'appliquent-elles ?  
Absence prolongée et non prévisible de notre DPO : que faire ?  
Insérer une mention d'information dans les contrats ?  
Casier judiciaire : Peut-on garder le bulletin n°3 ?  
Les salariés expatriés hors Union européenne sont-ils soumis au RGPD ?  
Notre prestataire "courrier", qui considère qu'il ne traite pas de données personnelles, peut-il refuser de signer l'avenant RGPD ?  
Collaborateur d'une filiale hors UE (Serbie) : Des BCR pour deux utilisateurs ?  
Guide Sécurité : quelle référence ?  
Interface entre applicatifs d'un même établissement : une seule finalité ou plusieurs ?  
Accès messagerie en l'absence d'un salarié : quelles sont les règles ?  
Quelles garanties demander à un Hébergeur ?  
Vidéosurveillance d'un immeuble regroupant plusieurs sociétés : qui doit informer ?  
CE/CSE utilisant des outils informatiques de l'entreprise : contrat de sous-traitance ? Que pensez-vous de certaines clauses du "Data Processing Agreement for Oracle Cloud Services" ?  
Déclaration URSSAF: licéité exécution d'un contrat ou obligation légale ?  
Comment qualifiez-vous les différents destinataires de données RH ?  
Avez-vous déjà évoqué ces questions relatives au DPO ?  
Doit-on obtenir le consentement du candidat à un emploi lors d'une procédure de recrutement ?  
Quand déclencher une analyse d'impact relative à la protection des données ?  
Lien vidéo France-USA semi-permanent : quelles précautions prendre ?

*Vous voulez rejoindre l'AFCDP ? Nul besoin d'être DPO ! Les adhésions agréées par le Conseil d'administration à partir du 1<sup>er</sup> octobre de l'année en cours s'étendent jusqu'au 31 décembre de l'année suivante. Visitez sans attendre les pages « [Comment adhérer ?](#) »,*

« [Témoignages](#) », « [Qui sont les Membres de l'AFCDP ?](#) » et « [Valeur rendues aux Membres](#) ». Pour tout complément, n'hésitez pas à contacter le Délégué général.

*« Le DPO est souvent un peu seul. Les travaux de l'AFCDP permettent de pallier cet inconvénient en dégagant des « bonnes pratiques ». Cette association est donc indispensable pour qui veut remplir avec professionnalisme sa mission. » Marie Eymond, DPO – Groupe Randstad France*

## **L'actualité des Données personnelles (France) :**

### **Finalités soumises à PIA : voici enfin la liste**

Par [ses délibérations n° 2018-326 et 2018-327 du 11 octobre 2018](#), la CNIL donne la liste des cas où une analyse d'impact relative à la protection des données (AIPD) est requise.

### **Atelier de la CNIL sur le RGPD**

Le 13 novembre, la CNIL a organisé en ses locaux un Atelier dédié au RGPD. Merci à Albine Vincent, Cheffe du service des DPO, de nous permettre de partager le support visuel utilisé lors de cette session (réservé aux membres).

### **Gestion des activités commerciales et Gestion des impayés**

La CNIL ouvre, jusqu'au 11 janvier 2019, une consultation publique sur deux de ses futurs référentiels. La première, issue principalement de l'ancienne NS 48, porte sur la "[Gestion des activités commerciales](#)". La seconde porte sur la "[Gestion des impayés](#)". La CNIL, dans un esprit de co-construction de la régulation, est particulièrement intéressés de connaître vos observations et commentaires sur ces textes.

### **Le 11 décembre : la Nuit du DPO**

L'AFCDP est associée à l'évènement organisé par Le JDN et [destiné à récompenser les meilleurs DPO de France](#). Le Jury remettra les trophées suivants : le DPO le plus Fédérateur, le DPO le plus Innovant, le DPO le plus Ambitieux, le prix spécial du Jury. Dans cette attente, prenez connaissance des interviews des nominés.

### **Une nouvelle formation DPO en région**

Enfin ! Les Universités en régions commencent à proposer des formations longues qui préparent à notre métier. Après Lyon et Lille, [c'est au tour de l'UFR de droit de Caen de proposer un DU Data privacy officer](#). Nous mettons donc à jour notre liste qui recense toutes les formations longues.

### **La barre des 1.000 notifications de violations de données a été franchie**

Mais Mme Albine Vincent, Cheffe du service des DPO, [nous a indiqué que l'ICO en a enregistré 6.000 dans le même temps](#) (il lui semble que les pays du Nord de l'Europe enregistre bien plus de notifications que les pays du sud). Elle précise également que, parmi les 15 000 DPO désignés auprès de la CNIL, 550 sont des personnes morales, ce qui traduit l'explosion du nombre de DPO externes. Enfin elle rappelle qu'il ne faut pas parler de "certification du DPO", mais de "certification des compétences du DPO" (le référentiel n'ayant pas pour ambition de vérifier si la personne détient le savoir-faire et le savoir être, mais uniquement le savoir). Lors des échanges avec la salle, un DPO qui a été invité par un organisme certificateur d'être membre de l'un de ses jurys a fait part d'un témoignage troublant : on lui aurait demandé de "remonter" sa note afin de permettre aux candidats d'obtenir leur certification. La CNIL a pris soigneusement note.

## **RGPD et marchés publics**

La direction des affaires juridiques (DAJ) du ministère de l'Économie et des Finances [a publié une fiche sur « l'impact du RGPD sur le droit de la commande publique »](#). Ce document transpose les termes (le "responsable de traitement" est l'acheteur, le « sous-traitant » est le titulaire du marché, tandis que le "sous-traitant du sous-traitant" au sens du RGPD est le simple sous-traitant au sens du droit de la commande publique. Pour les marchés publics ne faisant pas référence à un CCAG, les dispositions issues du RGPD étant d'application immédiate aux contrats en cours d'exécution, la DAJ recommande « vivement » de conclure des avenants afin de prendre en considération le RGPD.

## **Comment intéresser les Députés au RGPD ?**

[Notre membre Thiébaud Meyer, DPO de l'Assemblée nationale](#), présente au JDN le chantier majeur qu'il a conduit en 2018 concernant le RGPD.

## **Le Ministère de la justice cherche un expert RGPD de haut niveau**

Le secrétariat général du ministère de la justice cherche un expert de haut niveau, [chargé des fonctions de DPO](#) qui mettra en œuvre les mesures nécessaires à la conformité des traitements de données du ministère au règlement européen sur la protection des données (RGPD) et à la loi « Informatique et Libertés ».

## **Votre ordinateur est-il unique ?**

Vous connaissiez sans doute le site Panopticlic. Les chercheurs de l'INRIA ont développé un service similaire, [Am I Unique?](#), mais qui met en œuvre les techniques les plus récentes de prise d'empreintes digitales, dont webGL et [canvas](#). Le site vous indique si votre ordinateur peut être distingué (donc pisté) par les sites web même si vous refusez ou supprimez les cookies (grâce à la technique du [Fingerprinting](#), dont nous vous parlions dès... 2011).

## **Notification de violation et communication de crise**

À la suite de la publication d'un article de ZATAZ concernant la fuite de données ayant visé l'espace "JOB" des restaurants Flunch, l'enseigne du groupe Mulliez a communiqué en toute transparence [via son DPO](#).

## **La CNIL épingle aussi Vectaury**

La Commission met en demeure une start-up spécialisée dans le ciblage publicitaire, lui reprochant d'exploiter des données d'utilisateurs de smartphones sans accord clair de leur part. La société concernée, Vectaury, est la quatrième de ce type visée par la CNIL depuis l'entrée en application du RGPD. Vectaury a trois mois pour se mettre en conformité dans le recueil des consentements et [mais aussi pour supprimer les millions de données indûment collectées](#).

## **Colloque TIC Santé 2019**

L'association FORMATIC Santé organise à Paris, les 6 et 7 février 2019, son colloque annuel. Notons la présence (à confirmer), dans la table ronde "[Le numérique - quelle valeur ajoutée pour les institutions de santé ? Chance ou menace ?](#)", de Thomas Dautieu, Directeur adjoint de la conformité à la CNIL

## **Le RGPD dévoyé par les géants du profilage publicitaire ?**

Ce papier dénonce les agissements de certains géants américains de la publicité qui ont réussi à instrumentaliser le nouvel environnement réglementaire [en imposant leurs propres règles contractuelles au nom du RGPD](#). Comme l'indique l'auteur, il ne faudrait pas que l'instrumentalisation abusive du RGPD ne se développe au profit du plus fort et non du plus

sincère.

### **Bercy va tester la surveillance des réseaux sociaux**

C'est ce qu'a dévoilé le Ministre de l'Action et des Comptes publics lors d'une émission télévisée : "[Il s'agira de vérifier que le niveau de vie affiché par les contribuables sur les photos qu'ils publient sur Facebook, Twitter, Instagram ou Snapchat correspond bien aux déclarations de revenus envoyées au fisc](#). L'administration pourra « constater que si vous vous faites prendre en photo manifestement de nombreuses fois avec une voiture de luxe alors que vous n'avez pas les moyens pour le faire, peut-être que c'est votre cousin ou votre copine qui vous l'a prêtée, ou peut-être pas ». Les services de Bercy précisent "Il s'agit seulement d'une expérimentation, réalisée avec l'accord de la CNIL".

### **La CNIL pas tout à fait emballée...**

Suite aux annonces du Ministre Gérard Darmanin sur le projet de Bercy d'analyser les réseaux sociaux des Français pour pointer d'éventuelles discordances fiscales, [la CNIL se montre pour le moins réservée](#). Si « la lutte contre la fraude constitue en soi un objectif légitime, [...] un projet de ce type soulève, par nature, d'importantes questions de proportionnalité compte tenu de son caractère intrusif dans la vie privée des personnes et du caractère potentiellement massif de la collecte ».

### **Un jeu pour ne plus dire « oui » à n'importe qui**

[L'UFC-Que Choisir lance un \*serious game\*](#), ouvert à tous, permettant de sensibiliser de manière ludique aux enjeux et aux bons réflexes à acquérir en la matière. La mécanique de jeu est simple : elle consiste à prendre des décisions en faisant à chaque fois le meilleur choix parmi ceux qui sont proposés au fil de la narration. Mais attention : si certains choix n'empêchent pas le joueur de progresser dans l'histoire, d'autres ne pardonneront pas...

### **eMarketing et RGPD**

Dans le 4ème Baromètre Programmatique "Data, Insights & RGPD" de l'EBG (qui comprend un entretien avec Laure de Lataillade, du Geste) on apprend que, pour 64 % des professionnels interrogés, [le principal impact du RGPD est l'obligation d'être plus transparent et la nécessité de regagner la confiance des consommateurs](#), que 59 % des répondants pensent que le RGPD renforce la position des GAFAs et que 56 % parient sur la disparition de certains acteurs de la chaîne de valeur "à cause" du RGPD.

### **Facebook : Action de groupe en France**

L'association Internet Society France a lancé le 8 novembre 2018, [une action de groupe](#) contre Facebook, pour faire cesser des infractions. Elle appelle tous les utilisateurs du réseau social intéressés à se joindre à cette plainte collective et entend réclamer 1 000 euros par utilisateur; visant 100 000 usagers elle pense demander 100 millions d'euros de dommages et intérêts. Dans un premiers temps, elle donne 4 mois à Facebook pour répondre à sa [mise en demeure](#) qui énumère 7 manquements : protection insuffisante des données, information insuffisante sur la faille récente, cookies non conformes, CGU insatisfaisantes, collecte d'informations sensibles, consentement incorrect et maîtrise insuffisante de l'utilisateur sur les données collectées. L'association précise qu'elle a fait le choix d'une action devant la justice, et non auprès de la CNIL, dont elle trouverait le traitement des plaintes long et opaque.

### **Signature électronique**

La FNTC (Fédération des tiers de confiance du numérique) [publie un nouveau guide dédié à l'archivage des preuves de signature électronique à la volée](#). Le document comprend - entre



autres - un descriptif des risques et des contraintes liées à ce type de signature et des solutions à adopter pour assurer la validité et la pérennité de ce type de signature.

### **Un réseau d'une cinquantaine de DPO et correspondants**

A l'approche de la Nuit du *Data Protection Officer*, [le DPO de la Société Générale \(membre AFCDP\) revient sur la mise en place d'une gouvernance taillée pour le RGPD](#). Vous pouvez prendre connaissance [de l'intégralité des témoignages des DPO qui concourent cette année](#).

### **40 caméras de surveillance dans la commune ? Disproportionné**

La cour administrative de Nantes [a annulé](#) le 13 novembre dernier un arrêté du préfet du Morbihan, qui autorisait la ville de Ploërmel à déployer 40 caméras de surveillance sur la quasi-totalité des lieux de vie de la commune bretonne.

### **La mise en œuvre du RGPD dédramatisée au Congrès des maires**

« En décembre 2017, aucune ligne n'était prévue au budget pour la mise en œuvre du RGPD. [Nous n'en avons pas encore entendu parler](#). Le sujet est arrivé sur la table progressivement début 2018 ». Ces quelques mots de Jean-Claude Husson, maire de Saint-Arnoult-en-Yvelines, montrent l'une des raisons du retard qu'ont pris les collectivités dans la mise en œuvre du RGPD.

### **Rendre la justice prédictive éthique ?**

Le comité éthique et scientifique de la justice prédictive [a adopté une charte éthique non contraignante](#) qui s'appliquera aux acteurs utilisant l'intelligence artificielle dans le monde du droit.

### **Démarchage : une entreprise se fait passer pour 60 Millions**

Comment éviter de se faire raccrocher au nez quand on est un démarcheur téléphonique ? En se faisant passer pour 60 Millions de consommateurs ! Depuis plusieurs semaines, [une entreprise usurpe l'identité du magazine pour glaner des informations personnelles](#). L'interlocuteur annonce réaliser une enquête sur la hausse des prix des mutuelles afin de berner les personnes appelées.

### **Signalement des violences à caractère sexuel et sexiste**

Un décret du 22 novembre autorise le ministre de l'intérieur à mettre en œuvre un traitement de données à caractère personnel destiné à permettre aux personnes victimes ou témoins de violences à caractère sexuel ou sexiste [d'entrer en relation et d'échanger en temps réel avec un personnel de la police nationale ou de la gendarmerie nationale et d'effectuer un signalement](#).

### **L'actualité des Données personnelles (Monde) :**

#### **Champ d'application territorial du RGPD**

Le projet de lignes directrices du CEPD sur le champ d'application territorial du RGPD a été publié. La consultation publique sur ce projet est ouverte jusqu'au 18 janvier. (Merci à Lorette Dubois)

#### **Le gouvernement néerlandais publie l'analyse d'impact qu'il a fait réaliser sur les offres Office**

Selon une analyse d'impact réalisée et publiée par le gouvernement néerlandais (plus de 300.000 ordinateurs de l'administration néerlandaise utilisent les logiciels Office), [les versions ProPlus d'Office 2016 et du service Office 365 proposées par Microsoft ne](#)

[respecteraient pas le RGPD](#). C'est la télémétrie associée à ces offres qui est en cause (comme elle l'avait été dans le cadre de la mise en demeure de la CNIL [au sujet de Windows 10](#)). On apprend ainsi que jusqu'à 25.000 types d'événements sont "remontés" sans aucune informations des clients ni contrôle de leur part, et seraient partagés entre trente équipes d'ingénieurs. Cela porte aussi sur du contenu, comme des objets d'email ou des phrases de documents, notamment en cas d'utilisation des outils de traduction ou de correction des applications.

### **Une sélection de TED Talks ayant pour sujet la "Privacy"**

*Pourquoi la protection de la vie privée est-elle importante ? Comment les entreprises de technologie vous trompent et vous poussent à renoncer à vos données et à votre vie privée, Vous croyez que vos email sont privés ? Réfléchissez encore, L'éthique de la collecte des données, etc.* Voici une sélection de TED talks sur nos sujets de prédilection (réservé aux membres). Si vous en connaissez d'autres, n'hésitez pas à les signaler en commentaire de cet article.

### **Vidéosurveillance sans autorisation**

Des employés de la Société des Bains de Mer et du Cercle des *Étrangers* avaient constaté que [le dispositif de vidéosurveillance n'avait fait l'objet d'aucune autorisation](#) et s'en était ému auprès de la CCIN. La Commission de contrôle des informations nominatives monégasque a prononcé un avertissement avec publication de la sanction.

### **Gestion des Habilitations**

Signalons l'intéressante délibération n° 2017-206 du 20 décembre 2017 de la CCIN monégasque sur la « [Gestion des Habilitations et des Accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information](#) ».

### **Bien sûr que je ne suis pas un robot ! Quoique...**

Découvrez comment Google parvient à récupérer les données personnelles de millions d'utilisateurs à travers le monde, [grâce au test reCaptcha](#), auquel l'internaute doit se soumettre pour prouver qu'il n'est pas un robot et accéder au contenu désiré. Pourtant, il existe des solutions tout aussi efficaces et qui permettent de respecter le RGPD.

### **Agence e-santé du Luxembourg : "Notre projet de dossier de soins partagé vise 750 000 patients"**

Julien Sassella, le DPO du GIE luxembourgeois spécialisé dans le domaine de la santé évoque ses chantiers, dont le dossier de soins partagé (DSP), [actuellement à la fin de sa phase pilote avec 60 000 patients luxembourgeois](#), sur une population potentielle de 750 000 habitants, qui y sont inscrits de manière à la fois volontaire et avec l'accord de leur médecin référent.

### **Avec qui vivez-vous ?**

On vient d'apprendre que Facebook a déposé un brevet en 2017 [pour savoir qui partage votre foyer](#) et pour s'en servir pour du ciblage de contenus publicitaire. Le brevet évoque des technologies *Big data* et *machine learning* se basant sur les photos postées sur Facebook et Instagram, ainsi que sur d'autres informations partagées avec le réseau social. (Merci à Laurent Laurelut)

### **Deux bons exemples de Privacy by Default**

Deux nouveaux navigateurs bloquent par défaut les cookies tiers : [Brave](#) (qui se targue de



temps de réponse deux à huit fois meilleurs que Chrome) et [Cliqz](#), développé par des allemands ("A browser made for privacy").

### **Facebook pas fiable ?**

Le représentant démocrate américain David Cicilline, qui devrait devenir le prochain président du comité antitrust de la Commission judiciaire de la Chambre des représentants, a déclaré que Facebook ne peut pas être considéré comme un organisme de confiance pour s'auto-réglementer [et que le Congrès devrait prendre des mesures](#).

### **Données "non personnelles"**

Après le RGPD voici le RDNF (Règlement relatif aux données "non personnelles"), Règlement concernant un cadre applicable [à la libre circulation des données à caractère "non personnel" dans l'Union européenne](#). Eric Barbry commente ce projet. Avancée juridique ou usine à gaz réglementaire ?

### **La collecte massive de données personnelles d'enfants montrés du doigt**

La commission britannique de protection de l'enfance a publié un rapport pointant [les effets indésirables d'un trop grand nombre de données des enfants sur la Toile](#).

### **Droit à la portabilité : Oups !**

En avril 2018, Instagram mettait en place une fonctionnalité permettant la portabilité des données. [Or cet outil affiche dans certains cas le mot de passe dans l'URL de la page](#), ce qui est particulièrement gênant pour ceux et celles qui ont recours à cette fonctionnalité sur un ordinateur non personnel. De plus, cela prouve qu'Instagram a connaissance des mots de passe, ce qui est franche opposition avec la doctrine (ne doivent être conservées que des empreintes de mots de passe).

### **Les données des utilisateurs de Tinder à la vente sur Internet**

Selon une enquête de l'ONG Tactical Tech, [des données des utilisateurs de Tinder seraient en vente libre sur des sites de Data Brokers et à des prix abordables](#). Parmi les données proposées à la vente, on trouve les noms, adresse mail, genre, centre d'intérêts, caractéristiques physiques... mais aussi l'orientation sexuelle.

### **Objets connectés plus ou moins louches**

Mozilla publie sa liste annuelle d'objets connectés de son programme « [Privacy not included](#) ». Parmi les objets porteurs du bonnet d'âne, des webcams de surveillance d'enfants et les Cloud Security Cam ou les Echo et Dot d'Amazon.

### **Duplex**

Google lance avec grande précaution son agent conversationnel Duplex dans laquelle une IA est capable d'appeler un restaurant à votre place pour réserver une table... avec une qualité telle que le restaurateur est persuadé d'être appelé par un être humain. [Duplex ira jusqu'à insérer des "Hum" et des pauses dans l'appel pour en renforcer le réalisme](#). Lors de son annonce, en mai dernier, Google avait paru surpris par les réactions négatives, beaucoup se méfiant des potentielles dérives que le système pourrait permettre. C'est sans doute ce qui explique que le déploiement [s'adressera d'abord à un « petit groupe » d'utilisateurs](#). Pour rassurer les utilisateurs, Google avait publié un communiqué indiquant que Duplex, au début de l'appel, [s'annoncera comme étant un système automatisé](#) et non un être humain, de manière à ne pas tromper la personne à qui l'appel est destiné. Cela rappellera à certains les propos de Serge

Tisseron lors de son intervention à l'occasion de l'Université AFCDP des DPO de 2018 : « Si vous préférez parler à un humain, tapez sur la touche # ». (réservé aux membres)

### **Google accusé d'espionnage**

Sept organisations de défense des consommateurs issus de sept pays de l'Union européenne ont saisi des régulateurs nationaux [en reprochant à Google de manipuler ses utilisateurs pour "espionner" leurs mouvements](#) en violation le RGPD, a annoncé le Bureau européen des unions de consommateurs (BEUC).

### **Uber sanctionné**

[Uber Technologies a écopé d'amendes en Grande-Bretagne et aux Pays-Bas](#), ces deux pays accusant le géant américain des services de véhicules de transport avec chauffeur (VTC) de n'avoir pas suffisamment protégé les informations personnelles de ses clients lors d'un vol massif de données en 2016. La sanction totale est de 1 million d'Euros.

### **GAN : Generative Adversarial Networks**

Il s'agit d'un concept formulé en 2014 par le chercheur Ian Goodfellow, alors qu'il étudiait à l'Université de Montréal (Depuis, il a rejoint Google) : [Deux IA sont mises en opposition](#). L'une crée des images les plus réalistes possible, alors que la seconde tente d'en détecter l'aspect artificielle. C'est cette approche, dans laquelle l'humain est totalement exclu, qui permet de créer des photos d'hommes ou de femmes qui n'ont jamais existé ([cet article vous propose de deviner si les photos qui vous sont proposées sont artificielles ou réelles](#)). Bluffant... et inquiétant. (merci à Steven Adamson)

### **Il est inquiet**

Yoshua Bengio, l'un des fondateurs de l'apprentissage profond (*deep learning*) qui a réussi à résister aux chants des sirènes et n'a pas rejoint l'un des GAFAM, s'est exprimé sur les perspectives d'avenir de l'intelligence artificielle, lors d'un événement organisé par le MIT : ["Il est dangereux de laisser trop de pouvoir se concentrer entre les mains de quelques-uns"](#).

### **En Chine, le système de notations des individus va être renforcé**

Le gouvernement chinois souhaite renforcer les listes noires déjà existantes avec des critères plus développés. Selon l'« indice de confiance » de l'habitant, le gouvernement se donne ensuite le droit de limiter son accès au marché, aux services publics, mais aussi à l'emploi, par exemple. Récemment, [on apprenait que 11 millions de trajets aériens avaient été refusés à des individus qui présentaient un score trop faible](#). Pour Laurent Laurelut, notre membre (DPO du Sénat) qui nous signale cet article, il s'agit en fait d'une opération montée de toutes pièces par le gouvernement chinois pour nous montrer l'intérêt du RGPD et accessoirement de vivre dans une démocratie.

### **LinkedIn sous pression**

Le commissaire à la protection des données irlandais, Helen Dixon a fait réaliser une inspection de *LinkedIn Ireland Unlimited Company* (filiale de LinkedIn, appartenant à Microsoft) suite à une plainte qui lui a été notifiée par un utilisateur n'appartenant pas à LinkedIn. [L'enquête a révélé que LinkedIn Corporation avait traité des adresses de messagerie d'environ 18 millions de personnes qui ne figurent pas parmi les membres de LinkedIn](#) et avait ciblé ces personnes sur la plateforme Facebook. « Suite aux conclusions de notre audit de *LinkedIn Ireland*, en tant que responsable du traitement des données des utilisateurs de l'UE, a demandé à *LinkedIn Corp* de cesser le traitement pré-informatique et de supprimer toutes les données à caractère personnel associées à ce traitement avant le 25 mai

2018 », a rapporté la commissaire. Pour être en règle avec le RGPD, [LinkedIn a dû mener des actions correctives](#).

### **500 millions de clients concernés**

La chaîne d'hôtels Marriott (Sheraton, Westin, Méridien, etc.) enquête sur une violation de données qui affecterait [depuis au moins quatre ans](#) son système d'information et aurait exposé les numéros de cartes bancaires, références de documents d'identité, adresses postales et courriel, dates de naissance de plus de cinq cents millions de clients de par le Monde. A titre de comparaison, la violation d'Equifax l'an dernier ne touchait "que" 145 millions de personnes. Marriott a commencé à émettre des courriels vers les clients concernés.

*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 : Bruno Rasle - <mailto:delegue.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:delegue.general@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 (webbug) 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.*