FÉVRIER 2022 : #12

L'ACTUALITÉ RGPD

By Tchérylène MAIRET - DPO PRO ARCHIVES SYSTEMES

L'EDITO DU DPO

L'effet ciseaux

L'invalidation du Privacy Shield, aura posé un jalon d' avertissement par la politique européenne de protection et de transfert des données - notamment sensibles – vers des pays extracommunautaires dont les bases de données sont soumises à des injonctions de juridictions ou autorités administratives tiers les obligeant à une rupture de la confidentialité des données.

Si un sentiment de flottement ou d'impatience anime parfois les usagers européens en particulier français qui se demandent ce que le RGPD a changé au quotidien dans le respect de leur vie privée, la réponse arrive tel un rouleau compresseur de « dispositions » en Règlements venant compléter notre arsenal. C'est l'effet ciseaux.

Le Digital Service Act (DSA) adopté par le Parlement européen le 20 janvier 2022 vient renforcer certaines dispositions du RGPD sur l'interdiction de réaliser du profilage sur les mineurs, l'orientation politique et sexuelle et pose la responsabilité des GAFAM sur les moyens mis en œuvre pour la modération des contenus. Le projet d'un DNS européen pour l'accès à Internet bloquera les sites malveillants et des sites d'apologie du terrorisme ou de pédopornographie. Un des axes de La Présidence de la France de l'Union européenne est la souveraineté numérique et la coordination de la cybersécurité à l'échelle européenne. Le référentiel de la Cnil relatif aux entrepôts de données de santé pose le principe de la territorialité européenne ET exclut un transfert vers des pays non-adéquats comme les USA. Un vent de rébellion souffle contre Google Analytics qui pourrait aboutir à une disposition contraignante du CEPD. Enfin, le Règlement européen sur l'Intelligence Artificielle est examiné par le Parlement. Déjà, les effets se font ressentir sur les Gafam avec la potentielle décision de Marc Zuckerberg de fermer Facebook et Instagram aux utilisateurs Européens dans l'incapacité de se mettre en conformité avec la protection des données personnelles de l'Europe.

Néanmoins cet éparpillement de dispositions sonnera-t-il le glas du Règlement e-Privacy qui n'a toujours pas été adopté ?

EN BREF

UNE PUBLICITÉ AFFICHÉE DANS UNE BOITE E-MAIL PEUT ÊTRE ASSIMILÉE À UN COURRIEL DE PROSPECTION

Un arrêt de la Cour de justice de l'UE du 25 novembre 2021 donne une interprétation large à la notion « d'utilisation de courrier électronique à des fins de prospection directe » prévue par la directive ePrivacy. L'affaire concerne le service de messagerie électronique T-Online gratuit, financé par la publicité. Le fait que des messages publicitaires s'affichent, parmi les courriels légitimes, suffit pour les considérer comme des courriers électroniques. De fait le consentement préalable de l'utilisateur du service de courrier électronique est obligatoire.

La note du DPO

Cet arrêt de la CJEU est à suivre puisqu'il impacte le modèle économique de la plupart des messageries grand public gratuites.

UN FICHIER POUR LUTTER CONTRE LES RANÇONGICIELS

Par un arrêté du 22 décembre 2021, le Ministère de l'Intérieur est autorisé à mettre en œuvre un traitement des données personnelles relatives aux cyberattaques. Bizarrement dénommé « MISP-PJ », le fichier contiendra les noms et prénoms des personnes victimes des agressions informatiques contre rançon, les adresses IP des systèmes attaquées, la date, la nature et les circonstances des faits et les données sur l'auteur de l'attaque, comme la demande de rançon ou l'adresse de portefeuille de monnaie virtuelle (bitcoin). Ces données seront conservées six ans.

CLAP DE FIN POUR DATAJUST, L'ALGORITHME D'ÉVALUATION DES PRÉJUDICES CORPORELS

Selon les informations de ActeursPublics.fr, le Ministère de la Justice a acté le 13 janvier 2022 l'abandon du projet DataJust issu d'une expérimentation de deux ans de traitement de données visant à établir un référentiel fiable et officiel de l'indemnisation des victimes de préjudices corporels. L'idée était que les justiciables puissent estimer le montant d'une éventuelle indemnisation pour dommage corporel avant de se lancer dans une procédure.
L'enjeu était donc de s'appuyer sur l'intelligence artificielle pour désengorger des tribunaux en espérant qu'elle favoriserait le règlement à l'amiable des litiges.
La base de données sur laquelle l'IA a travaillé était biaisée car incomplète, en l'absence des décisions de première instance.

La note du DPO

Fraîchement accueilli par l'ensemble des professionnels de justice, DataJust traitait une quantité colossale de données personnelles sensibles contraire au principe de proportionnalité du RGPD et ne garantissait pas une anonymisation sans possibilité de réidentifier les personnes concernées. Voulu au service des justiciables, DataJust aiguisait particulièrement l'intérêt des assureurs. Mal inspiré, DataJust rappelle certaines pratiques étasuniennes où 80% des litiges sont conclus par un accord entre parties sans déboucher sur un procès.

En savoir +

GOOGLE ANALYTICS DANS LE COLLIMATEUR DU RÉGULATEUR AUTRICHIEN

L'autorité autrichienne de la violation des données estime que l'utilisation de Google Analytics permet le transfert de données vers les Etats-Unis, ce qui constitue une violation du droit européen.
Google Analystics aurait partiellement ignoré l'annulation du Privacy Shield par la Cour de Justice de L'Union européenne en 2020. Comme toutes les données sont hébergées aux Etats-Unis, les utilisateurs sont impactés par cette collecte de données.

Des décisions similaires sont attendues dans d'autres états membres.

La note du DPO

Le Comité Européen à la protection des données (CEPD) pourrait prendre des dispositions applicables sur l'ensemble du territoire. Ce volet est à surveiller du fait de son impact sur les traceurs.

En savoir +

LA CNIL RE(N)CADRE R.I.F.I.

La Recherche sur Internet de Fuites d'Informations (RIFI) a pour objectif de détecter, au plus tôt, une fuite de données. Les organismes qui souhaitent y recourir, ainsi que les prestataires de RIFI eux-mêmes, doivent respecter certaines règles, notamment le RGPD et le code pénal.
Une opération de RIFI consiste à analyser le web de manière automatisée, afin de vérifier si des informations, préalablement identifiées par le biais de mots-clés, ont été rendues publiques. Cela revient, pour un organisme, à rechercher dans le vaste océan du web, les données qui ont fuité. Cela implique donc d'analyser un important volume de données, y compris, des données personnelles.

La note du DPO

Cette méthode pose le problème de la proportionnalité de la collecte car il y a un risque non négligeable de faire remonter des données personnelles non pertinentes si les mots-clefs de la recherche sont mal paramétrés. Bien entendu, seules les informations accessibles sans contournement de sécurité doivent être collectées. Enfin, le RIFI est susceptible d'être mis en œuvre en dernier recours. D'autres méthodes moins invasives doivent être examinées.

Lire l'article

LE DSA RENFORCE L'ARSENAL JURIDIQUE FACE AU GAFAM

Le Digital Service Act (DSA) adopté par le Parlement européen le 20 janvier 2022 vient renforcer certaines dispositions du RGPD.
Aussi les publicités ciblées issues d'un traitement par segmentation comportementale sur les mineurs, relatives à l'orientation sexuelle et la religion seront interdites.
Les dark patterns ou interfaces truquées reposant sur les biais cognitifs seront interdites.
Si une plateforme promeut délibérément du contenu blessant, un utilisateur qui se sent attaqué pourra réclamer une réparation.
Les plateformes et réseaux sociaux devront proposer la désactivation manuelle des traceurs lors de la navigation sur leurs services.

La note du DPO

La pression mise sur les contenus abusifs et blessants impose désormais aux GAFAM de déployer de vrais moyens pour la modération de leurs services.

En savoir +

VIDÉOSURVEILLANCE : UNE PREUVE ILLICITE PEUT ÊTRE RETENUE

Mettre en œuvre un traitement de données personnelles issues de la vidéosurveillance des salariés sans information préalable des personnes concernées et du comité d'entreprise est illicite. Cependant, les preuves recueillies par ce traitement ne sont pas nécessairement exclues d'un débat judiciaire. Dans un arrêt du 10 novembre 2021 de la Cour de Cassation, il appartient au juge d'apprécier si une telle preuve peut porter atteinte au caractère équitable de la procédure, en mettant en balance le droit de la preuve et le droit au respect de la vie personnelle du salarié, dont l'atteinte doit rester strictement proportionnée au but poursuivi.

La note du DPO

Et puisqu'il appartient au Tribunal de trancher la recevabilité de certaines pièces, cet arrêt n'invalide aucune disposition applicable sur la licéité d'un traitement de données relatif au suivi du temps de travail du salarié.

En savoir +

LE 5ÈME ART DE LA GUERRE NE FAIT PAS DE PAUSE PENDANT LA PANDÉMIE.

De l'énergie en passant par l'hôpital, nombreux sont les secteurs d'activité touchés par des attaques informatiques en 2021, le plus souvent en échange de rançons. Mais d'autres cyberattaques ont lieu dans l'ombre car elles visent à récolter des informations stratégiques plutôt que de l'argent. Et elles n'obéissent pas à des groupes criminels, mais à des Etats.
De nombreux pays continuent en effet d'utiliser le cyberespace comme terrain de chasse, pour mener des opérations d'espionnage ou de sabotage. Sans avoir connu la même explosion que les attaques par rançongiciel, elles ont, elles aussi, profité de la pandémie de Covid-19 pour réaliser certaines des pires attaques informatiques de l'histoire. Et la France n'est pas épargnée.

La note du DPO

On appelle 5ème art de la guerre à partir de la hiérarchie de Sun Tzu, la référence à des batailles obscures dans le cyberespace.

Lire l'article

PRÉSIDENCE FRANÇAISE DE L'UNION EUROPÉENNE ET CYBERSÉCURITÉ

Pour sa présidence du Conseil de l'Union européenne, lors du premier semestre 2022, la France fait la cybersécurité l'un de ses axes de travail prioritaires. Les chantiers sont nombreux :

- Réviser la directive NIS sur les opérateurs de services essentiels,
- Éprouver la coopération entre les Etats membres en cas d'incidents cyber, notamment lors d'un exercice de Stress Test grandeur nature au sein de l'Union Européenne,
- Définir le contenu du schéma de certification pour le cloud,
- Consolider le tissu industriel.

« Nous nous inscrivons pleinement dans la ligne politique de promotion d'une souveraineté numérique européenne » déclare le sous-directeur stratégie de l'ANSSI Yves Verhoeven. La renégociation de la Directive NIS est également « un acte fondateur pour positionner l'Union européenne comme l'organisation internationale légitime pour la cybersécurité des infrastructures critiques en Europe, notamment vis-à-vis de l'OTAN. »

En savoir +

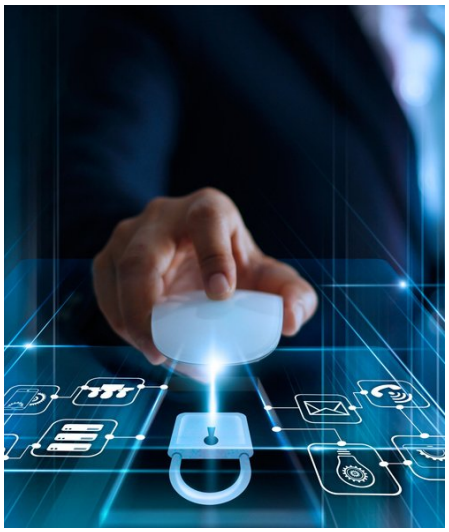
DNS FOR YOU (DNS4EU) OU LA PROMESSE D'UNE NAVIGATION WEB RGPD RESPONSABLE

Le 12 janvier 2022, la Commission Européenne a lancé un appel à projet pour offrir un service européen alternatif à Cloudflare de Google pour l'accès au Web mondial. « DNS4EU sera transparent, conforme aux normes et règles les plus récentes en matière de sécurité, de protection des données et de respect de la vie privée dès la conception et par défaut. »
DNS4EU

- Renforcera la protection contre les piratages,
- Bloquera les sites malveillants susceptibles de distribuer des malwares ou de procéder à du Phishing grâce à des filtres,
- Bloquera les sites jugés illégaux : apologie du terrorisme, pédopornographie, contrefaçons d'œuvres audiovisuelles etc.

En savoir +

SANCTIONS 2021 CNIL



BILAN DES SANCTIONS 2021 DE LA CNIL

2021 est une année sans précédent, tant par le nombre de mesures adoptées (18 sanctions et 135 mises en demeure) que par le montant cumulé des amendes, qui atteint plus de 214 millions d'euros.

Cette année, les décisions ont concerné des secteurs d'activité et des acteurs très divers. Parmi les manquements les plus fréquents figurent :

- Le défaut d'information des personnes,
- Des durées de conservation excessives.

Sur ces 18 sanctions, la moitié comporte un manquement en lien avec la sécurité des données personnelles.

Voir le bilan