JUILLET - AOÛT 2022 : #14

L'ACTUALITÉ RGPD

By Tchérylène MAIRET - DPO AGS RECORDS MANAGEMENT

L'EDITO DU DPO

Saint-Isidore à l'épreuve des neurosciences

En 2018, la mise en place du RGPD a engendré une période de confusion palpable où la Conformité a trop été réduite à une affaire de cybersécurité. Saupoudrer d'anti-virus son SI sur les conseils d'experts de pacotille a surtout permis d'alléger le portefeuille des dirigeants d'entreprise qui – pour certains - choisissaient d'y croire – pour d'autres – souhaitaient gagner du temps en attendant une meilleure approche. Or les cyberattaques n'ont cessé de proliférer, gagnant en complexité, en ingéniosité et en malveillance. Par ailleurs, l'un des meilleurs algorithme de chiffrement au monde vient de tomber. Prier Saint-Isidore-de-Séville – saint patron des informaticiens – pour que la taille de l'entreprise et ses SI constituent un enjeu trop faible pour un cyberattaquant ou supposer qu'une commune ne constituerait pas une cible « *parce qu'elle ne traite aucune donnée de valeur [bancaire]* » constitue un risque inconsidéré.

Bien entendu, le RGPD exige que l'Organisation sécurise les données à l'état de l'art.

Par ailleurs, l'Intelligence Artificielle est-elle venue renforcer les dispositifs permettant de bloquer des attaques comme les compromissions d'emails. L'intelligence artificielle est également efficace contre le camouflage et l'encapsulation automatique de logiciels malveillants. Mais pour les cyberattaques par ingénierie sociale qui misent sur les faiblesses de l'âme humaine l'intelligence artificielle est d'une efficacité très relative. Et seuls 3% des salariés sont capables de détecter toutes les arnaques aux e-mails frauduleux. Si toutes ces attaques étaient déjouées par des algorithmes nous n'aurions pas à déplorer cette croissance exponentielle des cyberattaques.

Une approche pour faire face à cette complexité est de recourir aux principes de la psychologie cognitive. « *Traiter les cyberattaques par ingénierie sociale comme un type particulier d'attaque « psychologique », nous ouvre de nouvelles perspectives en sciences cognitives et nous permet de dresser les bases d'un domaine que l'on pourrait appeler « l'approche cognitive de la cybersécurité » : elle étend et adapte les principes des sciences cognitives et notamment de la psychologie cognitive au champ d'application de la cybersécurité. Formation et éducation à l'approche cognitive de la cybersécurité doivent devenir des priorités nationales. Former les salariés du public et du privé à la compréhension des mécanismes psychologiques qui structurent et sous-tendent notre exposition et notre vulnérabilité à la cyberdélinquance et à la cybercriminalité est vital dans une société numérique hyperconnectée.* » *European scientist*

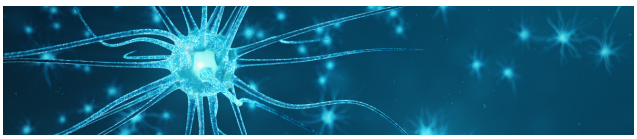
La mission du DPO inclut la sensibilisation des collaborateurs au respect de la vie privée des personnes concernées et les risques induits par les traitements mis en œuvre. Cette approche cognitive de la cybersécurité semble une approche innovante et prometteuse.

EN BREF

LE CEPD NE DIGÈRE PAS LA MODIFICATION DU RÈGLEMENT EUROPOL

Dans son communiqué de presse, du 27 juin 2022 le super-gendarme des données personnelles européen fulmine contre le règlement modifié de Europol et son impact sur les données personnelles de citoyens allant jusqu'à douter de sa légalité. Le CEPD prend acte qu'Europol « est désormais autorisé, dans des cas spécifiques, à traiter de grands ensembles de données, ce qui entraîne une augmentation substantielle du volume de données à caractère personnel des individus traitées et stockées par l'Agence. Par conséquent, les données relatives aux personnes qui n'ont pas de lien établi avec une activité criminelle seront traitées de la même manière que les données personnelles des personnes ayant un lien avec une activité criminelle. » À cette occasion, il « regrette que l'expansion du mandat d'Europol n'ait pas été compensée par des garanties solides en matière de protection des données qui permettraient un contrôle efficace des nouveaux pouvoirs de l'agence ».

Voir le communiqué



LE TOURNANT COGNITIF DE LA CYBERSÉCURITÉ

Dans son article publié dans European Scientist Bruno Teboul, co-auteur de « Les usages malveillants de l'intelligence artificielle au service de la cybercriminalité (Février-Mars 2022) déclare en conclusion de sa démonstration de l'apport des neurosciences à la cybersécurité : « La neuro-cybersécurité (ou cybersécurité cognitive) donnera naissance à de nouveaux outils, à de nouveaux produits, au bénéfice des acteurs de la sécurité informatique et aux services des organisations publiques et privées, cibles de toutes les attaques « psychologiques » dans le cyberespace. Elle engendrera de nouvelles vocations, de nouveaux débouchés pour cette industrie et créera de nouveaux métiers appliqués à la cybersécurité : « neuroscientist », « cognitive scientist », « neurocognitive analyst », dont les compétences et les expertises s'arracheront à prix d'or ! ».

STATISTIQUES ETHNIQUES ET AUTRES DONNÉES SENSIBLES : LE POINT SUR SON ENCADREMENT

Cela commence comme une histoire pour hanter les nuits d'un DPO : oui, on collecte et on épluche des données ethniques au Pays des Lumières !
Pourtant, cette catégorie de statistiques fait partie de l'activité de l'Insee. Dans son billet de blog intitulé « Insee Oui, la statistique publique produit des statistiques ethniques ; Panorama d'une pratique ancienne, encadrée et évolutive », l'Insee revient sur son encadrement, en particulier les contraintes liées à la conformité au RGPD ; l'occasion de faire le point sur les traitements de données sensible à des fins de recherche scientifique et les 10 recommandations de la Cnil publiées en 2007 relatives Mesure de la diversité.

La note du DPO

L'article 6 de la Loi I&L interdit la collecte et le traitement de données dites « sensibles » notamment celles relatives à l'origine ou à l'appartenance ethno-raciale réelle ou supposée des personnes. Mais conformément à l'article 89, paragraphe 1 du RGPD, sont ainsi autorisés des traitements « à des fins de recherche scientifique ou historique ou à des fins statistiques ». La base légale n'est pas le consentement.
Les personnes sont libres de refuser de répondre, ou de répondre qu'elles ne savent pas. Cette possibilité de ne pas répondre s'applique y compris aux enquêtes statistiques obligatoires au sens de l'article 1er bis de la loi du 7 juin 1951 sur l'obligation, la coordination et le secret statistique.

En savoir +

DÉTECTION DE LA FRAUDE : PÔLE EMPLOI PEUT COLLECTER CERTAINES DONNÉES PERSONNELLES

Un décret publié le 30 juin 2022 précise les modalités d'exercice du droit de communication dont bénéficient les agents chargés de la prévention des fraudes agréés et assermentés de Pôle emploi. Pour d'obtenir auprès de certains organismes et entreprises, notamment les établissements bancaires, les fournisseurs d'énergie et les opérateurs de téléphonie, les documents et informations nécessaires au contrôle de la sincérité et de l'exactitude des déclarations des demandeurs d'emploi (situation géographique, leur niveau d'activité et des ressources perçues, leur mode de paiement ou de rémunération), ainsi que de l'authenticité des pièces produites en vue de l'attribution et du paiement des allocations, des aides, ainsi que de toutes autres prestations servies par Pôle emploi. Ces demandes ne pouvant porter que sur une période de 18 mois au maximum.

La note du DPO

Le décret 2022-955 du 29 juin 2022 vient de compléter une disposition adoptée en décembre 2020 dans le cadre de la Loi de finances pour 2021.

46% DES FRANÇAIS CONTINUENT D'ACCEPTER LES COOKIES

Malgré le durcissement de l'utilisation des cookies dans les délibérations 2020-091 et 2020-092 de la Cnil qui renforce le contrôle aux utilisateurs pour qu'ils soient capables de refuser d'être suivis par des trackers, l'étude de NordVPN montre que cette politique est un échec.
Même si les français disent ne pas vouloir de cookies, ils les acceptent quand même. L'étude montre que seulement 6% des français refusent systématiquement les cookies de leur navigation web et que 46% les acceptent dans leur totalité.

La note du DPO

Le DPO rappelle que le problème n'est pas la publicité (pour rémunérer un contenu) mais le profilage.

La publicité ciblée rémunère mieux l'éditeur qu'une publicité aléatoire susceptible de rater sa cible. En refusant les cookies vous refusez d'être le produit pour les annonceurs.

En savoir +

DES « DARK PATTERNS » DANS 97 % DES SITES ET APPLICATIONS EUROPÉENS LES PLUS POPULAIRES ?

Selon Bianca Schulz, responsable du Centre européen des consommateurs (CEC) France interrogée par le Journal du Net, le recours aux « dark patterns » (éléments graphiques trompeurs) s'est amplifié avec le développement des usages des consommateurs. On les trouve partout, en particulier sur les médias sociaux, les places de marché, comparateurs de prix, moteurs de recherche, plateformes de vidéo à la demande, sites d'e-commerce... Ils concernent 97 % des sites web et des applications les plus populaires en Europe. Si les grandes plateformes comme Amazon ont été pionnières, toutes les entreprises suivent, y compris les PME.

La note du DPO

Les dark patterns sont des interfaces piège-à-clic ou élaborées pour prolonger votre hésitation ou votre présence sur une page. Véritable fléau exploitant les biais cognitifs, savoir les identifier, c'est s'en préserver.
La Cnil par l'intermédiaire de son laboratoire Linc a publié un cahier intitulé « *la forme des choix* ».

Voir le cahier

RECEVABILITÉ DE LA SIGNATURE ÉLECTRONIQUE : QUE NOUS APPREND LA JURISPRUDENCE ?

A l'heure où l'utilisation de la signature électronique est un acte banalisé de la vie contractuelle, le contentieux autour de celle-ci se développe. Bonne nouvelle pour la sécurité juridique, la jurisprudence a su apporter des précisions et élargir le champ à de nouvelles perspectives. A travers des décisions récentes, cet article de l'Usine Digitale du 29 juillet 2022 résume les problématiques soulevées.

L'un des points majeurs quant à la recevabilité d'une signature électronique demeure la preuve de l'identité des signataires.

ACTUALITÉ CNIL : PUBLICATION D'UN RÉFÉRENTIEL DE LA COMMANDE PUBLIQUE

La CNIL publie un guide sur la responsabilité des acteurs dans le cadre de la commande publique.
Face aux difficultés soulevées par les professionnels du secteur de la commande publique dans l'identification de leurs responsabilités, la CNIL a publié un guide afin de clarifier les éléments à prendre en compte et les conséquences juridiques à tirer de la qualification de « responsable du traitement », de « sous-traitant » ou « responsable conjoint ». L'autorité précise notamment que cette qualification « doit intervenir le plus tôt possible et être effectuée au regard d'éléments factuels et en prenant en compte chaque contexte contractuel ».
Ainsi, ce guide devrait permettre aux professionnels concernés de « mieux caractériser l'existence et la portée de leurs obligations respectives en matière de protection des données, d'initier sur une base claire les démarches de mise en conformité au RGPD, et de renforcer ainsi leur sécurité juridique ».

Découvrir le guide

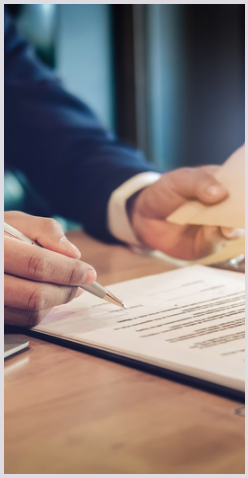
LE ROYAUME UNI RESTERA-T-IL UN PAYS ADÉQUAT ? UNE DÉGRADATION DES PROGRÈS DU RGPD REGRETTABLE

Le gouvernement Britannique entend s'éloigner du RGPD et proposer un nouvel encadrement du droit des données du citoyen. Dans un article du The Register, Peter Church, avocat au sein de l'équipe Linklaterson déclare que le gouvernement dans ce nouveau cadre entend remettre en question l'obligation de désigner un DPO, supprimer l'obligation de réaliser des Analyses d'Impacts et d'enregistrer les activités de traitement. Il est prévu de remplacer les exigences de consultation préalable obligatoire pour les activités de traitement des données à haut risque par un mécanisme volontaire, exclure l'obligation de consentement pour les cookies. Une « modernisation » de l'I.C.O. (Régulateur britannique) est envisagée.
Ce cadre qui s'annonce comme une dégradation des avancées du RGPD, pourrait bien remettre en question la décision d'adéquation octroyée par la Commission européenne pour la libre circulation des données entre l'UE et le Royaume-Uni.

La note du DPO

Il est assez stupéfiant d'observer que le Royaume Uni ne tire pas les leçons des déboires des USA relatives à l'invalidation du Privacy Shield. De fait, si le Royaume-Uni perd son statut de « pays adéquat » c'est-à-dire présentant les mêmes garanties pour la protection de la vie privée que l'UE alors, toute donnée hébergée par ou transférée au Royaume-Uni devra faire l'objet d'un encadrement juridique sous peine d'infraction au RGPD.

L'AUTORITÉ DE LA CONCURRENCE PLAIDE POUR UNE COOPÉRATION RENFORCÉE AVEC LA CNIL



A priori tout oppose ces deux autorités :

- L'une visant à protéger les utilisateurs contre toute collecte et exploitation préjudiciable de leurs données,
- L'autre visant à garantir les conditions d'une concurrence libre et non faussée entre les entreprises sur les marchés,

Les deux cadres de régulations présentent néanmoins une certaine convergence : le bénéfice des usagers et éviter des inégalités face à la concurrence. Dans ce contexte, le Président de l'Autorité de la concurrence a plaidé pour une « coopération accrue » entre les deux autorités dans un discours prononcé le 2 juin 2022 devant le collège de la CNIL, afin « *de s'assurer que les objectifs d'un des champs de régulation ne soient pas compromis par les mesures prises par l'autre régulateur* ». Cette coopération peut notamment passer par une demande d'avis de la CNIL par l'autorité de la concurrence dans le cadre du contrôle de concentration, ou vice versa, d'une sollicitation de l'autorité de la concurrence par la CNIL en cas de questionnement sur les impacts potentiels de ses décisions au regard du droit de la concurrence.

PÉDOPORNOGRAPHIE : PROTECTION DES MINEURS RESPECTUEUSE DES DONNÉES PERSONNELLES

Dans son avis du 3 juin 2021 la CNIL a déjà eu l'occasion de se pencher sur la vérification de l'âge pour l'accès aux sites pornographiques. Il y avait été recommandé le recours à un système respectueux de la vie privée, mis en place par un tiers vérificateur lors du processus de vérification d'âge par les sites. L'intérêt d'une telle solution réside notamment dans la mise en œuvre de mécanismes permettant d'empêcher, d'une part, que le tiers de confiance identifie le site ou l'application à l'origine d'une demande de vérification et, d'autre part, de limiter la capacité du site à l'origine de cette demande d'identifier l'individu concerné. Le Pôle d'Expertise de la Régulation Numérique (PEReN) a par ailleurs consacré le n°4 de sa collection Éclairage sur…à ce sujet (« Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? »).
Face à cet enjeu, le laboratoire LINC de la CNIL vient de publier un exemple de mise en œuvre d'un système de vérification d'âge pour permettre l'accès à certaines catégories de sites sans que ne soient partagées d'autres informations identifiantes.

La note du DPO

Pour l'heure, il n'existe pas de norme industrielle de vérification d'âge, ainsi chaque entreprise peut utiliser son propre système. Dans la plupart des cas, les plateformes demandent la date de naissance, or cette mesure est aisément contournable. Instagram (Meta) ayant annoncé le déploiement d'une fonctionnalité permettant de mieux contrôler l'accès des mineurs à certains types de contenus sur la base de la reconnaissance faciale, cette dernière pose inéluctablement une problématique pour la protection de la vie privée.