AVRIL 2022 : #13

L'ACTUALITÉ RGPD

By Tchérylène MAIRET - DPO PRO ARCHIVES SYSTEMES

L'EDITO DU DPO

Le 3 mars 2022, l'Union européenne a lancé la procédure d'examen de la demande d'adhésion de la Moldavie, la Géorgie et l'Ukraine. Voici le sens de l'histoire après l'invasion de l'Ukraine par la Russie : la protection de l'Europe est sollicitée. Qu'il est loin le temps des doutes au retrait du drapeau britannique du hall d'honneur du Parlement européen !
Or, en parallèle de cette guerre conventionnelle, les enjeux de sécurité numérique se font pressants : la France redouble de vigilance quant aux répercussions de ce conflit et les dommages collatéraux dans le cyberespace à l'image des *dommages irréversibles* sur les milliers de modems français des box attachées au service Viasat.

L'ANSSI, par la voix du CERT-FR publie un bulletin quasi hebdomadaire sur les cybermenaces et entend également lutter contre les contenus non-vérifiés. La Toile a frémi dès l'apparition le 23 février 2022 d'un nouveaux Malware de type Wipper baptisé « TrojanKilldisk ». L'ANSII considère à ce jour que l'impact en France est limité sans pour autant négliger les tentatives « d'indisponibilité de ressources sensibles ou porter atteinte à l'image d'institutions publiques ou privées ».

Et si, comme le suggère le site « *Le Vent Se Lève* » l'Union Européenne était en train de mesurer l'impact de sa dépendance aux infrastructures Web et logiciels américains dans ce conflit ? Alors que l'Union européenne étudie les options de sa souveraineté numérique, la Chine et la Russie prennent l'initiative de délimiter leur territoire dans le cyberespace : c'est le déploiement du *Splinternet*. *«La Chine a inauguré une balkanisation de l'internet en créant son «grand pare-feu», visant à lui assurer une souveraineté numérique»*. Quant à la Russie, la loi de 2019 sur « l'internet souverain » l'autorisait à se détacher architecturalement de l'infrastructure mondiale d'internet. Plusieurs rumeurs font état d'essais de déconnexion de la part de la Russie, visant à tester sa possible indépendance numérique » grâce au réseau RuNet ?

A l'image de *l'accord surprise* et polémique pour le transfert des données personnelles vers les USA en lieu et place du Privacy Shield invalidé, la situation diplomatique de l'Union européenne rappelle que les datas sont une source de profits qui survivra aux énergies fossiles.

EN BREF

CYBERATTAQUE ET PAIEMENT D'UNE RANÇON PAR L'ASSURANCE : PLAINTE PRÉALABLE OBLIGATOIRE

Le Gouvernement a déposé à l'Assemblée nationale le 16 mars 2022, son projet de loi d'orientation du ministère de l'Intérieur. Ce projet propose à l' *article 5* d'encadrer « *les clauses de remboursement des rançongiciels par les assurances, en conditionnant ce remboursement au dépôt rapide d'une plainte par la victime, afin d'améliorer l'information des forces de sécurité et de l'autorité judiciaire et de casser le modèle de rentabilité des cyber-attaquants* ».

MISE À JOUR DU RÉFÉRENTIEL POUR LES FOURNISSEURS DE SERVICE CLOUD

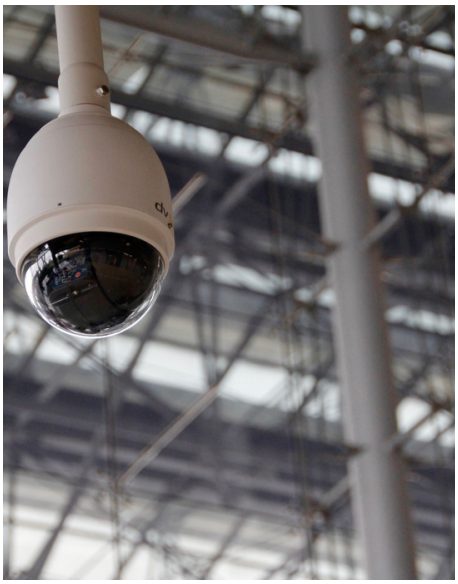
l'ANSSI a publié le 8 mars 2022 la version 3.2 du référentiel d'exigences applicables aux prestataires de services cloud. Cette qualification atteste de la qualité et de la robustesse de la prestation, de la compétence du prestataire ainsi que de la confiance pouvant lui être accordée.
La version 3.2 de SecNumCloud explicite des critères de protection vis-à-vis des lois extra-européennes. Ces exigences garantissent ainsi que le fournisseur de services cloud et les données qu'il traite ne peuvent être soumis à des lois non européennes. SecNumCloud 3.2 intègre également le retour d'expérience des premières évaluations et précise l'exigence relative à la mise en œuvre de tests d'intrusion tout au long du cycle de vie de la qualification. Concernant les solutions déjà qualifiées SecNumCloud, elles conservent leur Visa de sécurité et l'ANSSI accompagnera si nécessaire les entreprises concernées pour assurer la transition.

RÉUTILISATION DE DONNÉES RELATIVES À LA RELIGION PAR UN CANDIDAT DU 1ER TOUR : LA CNIL EST SAISIE

La Cnil est saisie d'un signalement concernant la réutilisation de données en ligne ciblant des destinataires de confession juive pour des diffusions de messages à finalité électorale par le candidat de Reconquête au 1er tour de l'élection présidentielle française. L'entourage du candidat explique : « Ce démarchage politique a été mis en place à l'aide d'un courtier en données personnelles – data broker – qui achète des bases de données récoltées sur des blogs, des sites d'information ou des newsletters ayant trait au sujet de l'antisémitisme en France. »
Or le consentement préalable des personnes concernées n'aurait pas été recueilli, à la fois s'agissant de données sensibles sur la religion et/ou une opinion politique d'une part, et d'autre part sur la réutilisation à des fins de démarchage politique.

La note du DPO

Ce cas de figure éclaire sur les conséquences de l'acceptation des cookies sur les sites consultés en termes de profilage
Par ailleurs, le candidat est Responsable de traitement et son courtier un sous-traitant. C'est donc au Responsable de traitement de s'assurer que toutes les données collectées et le traitement sont licites. Enfin, le recueil du consentement doit être un acte positif. C'est la raison pour laquelle la doctrine de la Cnil recommande une case à cocher et une information explicite sur la réutilisation des données.



LES FRANÇAIS FRILEUX CONCERNANT LA VIDÉOSURVEILLANCE INTELLIGENTE DANS LES COMMERCES

Les acteurs de la distribution et leurs fournisseurs réunis autour de préoccupations de sécurité et d'innovation technologique via la fédération Perifem, ont commandité un sondage sur la perception des Français sur la vidéosurveillance dans les commerces.

Il montre qu'une très large majorité de Français (77 %) y est favorable lorsqu'il s'agit de sécurité. L'accueil positif monte à plus de 90 % lorsqu'il s'agit de la sécurité dans les gares et aéroports, les parkings ou les transports en commun. Pour autant, une technologie IA appliquée à l'analyse du parcours client et comportements d'achats à des fins marketing est refusée à 65% par les français.

La note du DPO

Dans ce contexte les résultats du *projet de position de la CNIL* sur la « vidéosurveillance intelligente » (associée à l'IA et au Big Data) encore interdite est attendue par ces professionnels.

Voir les résultats de l'enquête

UN RÈGLEMENT EUROPÉEN IMMINENT POUR LA VALORISATION LES DONNÉES DE SANTÉ

La Commission européenne souhaite favoriser la réutilisation des données de santé et s'apprêterait à présenter en avril 2022 un projet de règlement afin d'améliorer les échanges et l'accès aux données de santé, pour soutenir l'offre de soins, la recherche en santé, et l'élaboration de politiques dans le domaine de la santé. Pour encadrer ces usages, la Commission prévoit l'institution d'une nouvelle autorité, l'European Digital and Health Data Board (Conseil européen du numérique et des données de santé). Par ailleurs, le programme EU4Health soutiendra la plateforme MyHealth@EU et le projet pilote visant à développer la nouvelle infrastructure décentralisée de l'UE pour une utilisation secondaire des données de santé dès 2022.

Lire l'article

DÉCRET 2022-372 DU 16 MARS 2022 : LE CALCUL DE LA DURÉE DE CONSERVATION DES DMST FACILITÉ

Le décret 2022-372 du 16 mars 2022 modifie l'article R 4624-28-2 du Code du Travail et dispose que l'employeur doit informer le Service de Prévention et de Santé au Travail de la fin de l'exposition à un risque professionnel de son salarié.
La précision n'est pas anodine parce qu'elle offre – enfin – la possibilité aux SPST de calculer avec finesse la durée de conservation des dossiers médicaux de santé au travail.
La durée de conservation des données étant un point de conformité majeur impactant au regard du RGPD, le paramétrage des métadonnées des DMST numériques à l'instar des DMST papier permettra d'en faciliter le calcul.

Voir le décret

DÉCRET 2022-395 DU 18 MARS 2022 : DURÉE DE CONSERVATION DU DOCUMENT UNIQUE D'ÉVALUATION DES RISQUES

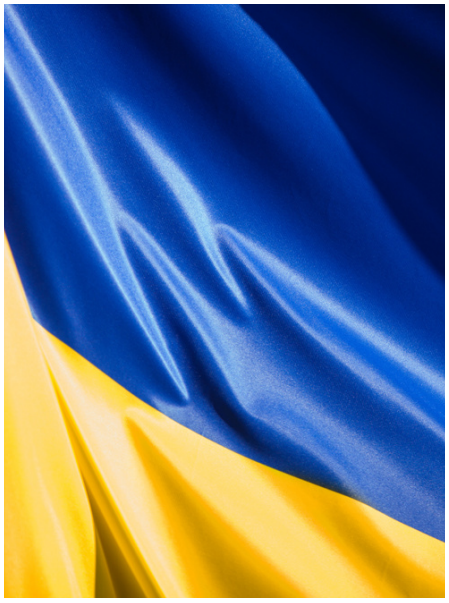
Décret 2022-395 du 18 mars 2022 modifie l'article R. 4121-4 du Code du Travail et dispose que le document unique d'évaluation des risques professionnels et ses versions antérieures sont tenus, pendant une durée de 40 ans à compter de leur élaboration. Une telle durée de conservation est cohérente avec les durées de conservation des DMST en fonction des expositions à un risque déclarées par l'employeur.

En savoir +

ACTU CNIL : PUBLICATION D'UN RÉFÉRENTIEL DE PROTECTION DE L'ENFANCE DES MINEURS ET MAJEURS DE MOINS DE 21 ANS

Comme tout organisme qui manipule des données personnelles, les organismes publics et privés qui proposent un accompagnement social et médico-social des mineurs et des jeunes majeurs de moins de 21 ans doivent respecter le RGPD.
Afin de les aider à être en conformité, la CNIL a adopté un nouveau référentiel à la suite d'une consultation publique.

En savoir +



LE CERT-FR PUBLIE UN RAPPORT HEBDOMADAIRE DE L'ÉTAT DES CYBERMENACES DEPUIS L'INVASION DE L'UKRAINE

L'ANSSI, par l'intermédiaire du *Centre Gouvernemental de Veille, d'Alerte et de Réponses aux Attaques Informatiques* publie un bulletin qui centralise et diffuse les éléments d'intérêt cyber en lien avec le contexte actuel pour favoriser le renforcement du niveau de protection de l'ensemble des entités françaises. En effet les tensions internationales causées par l'invasion de l'Ukraine par la Russie s'accompagnent d'effets dans le cyberespace.

Si les combats en Ukraine sont principalement conventionnels, l'ANSSI constate l'usage de cyberattaques dans le cadre du conflit. Dans un espace numérique sans frontières, ces cyberattaques peuvent affecter des entités françaises. Il convient sans céder à la panique de l'anticiper et de s'y préparer. Aussi, afin de réduire au maximum la probabilité de tels événements et d'en limiter les effets, l'ANSSI partage des bonnes pratiques de sécurité ainsi que des éléments sur la menace et invite l'ensemble des acteurs à s'en saisir.

Voir le rapport

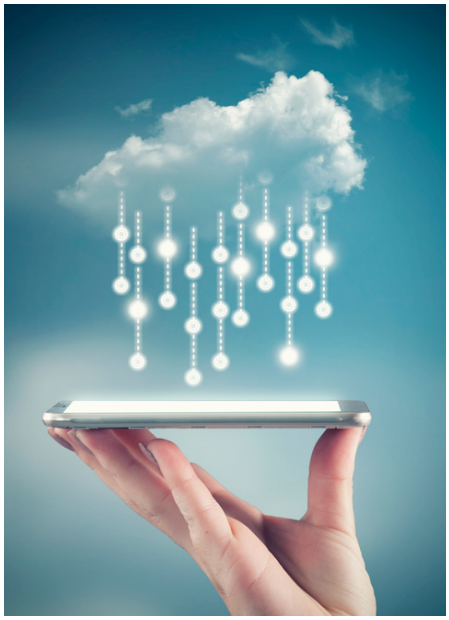
YANDEX : LES DONNÉES PERSONNELLES DES APPLICATIONS MOBILES PARTENT EN RUSSIE !

En effectuant l'audit d'une application mobile, un chercheur a constaté le comportement douteux d'un kit de développement proposé gratuitement par le géant russe Yandex, grand concurrent de Google.

Selon le Financial times, ce logiciel qui permet l'intégration de fonctions essentielles (cartographie, paiement...) est utilisé par plus d'un tiers des applications mobiles (IOS comme Android), mais il s'avère que les données qu'il collecte sont ensuite récupérées et stockées sur des serveurs en Russie et en Finlande.

La proximité présumée entre Yandex et le Kremlin ne fait qu'accroitre la préoccupation que soulève cette observation. Le chercheur californien continue à diffuser sur Twitter ses observations, et signale que 200 applis VPN seraient concernées.

En savoir +



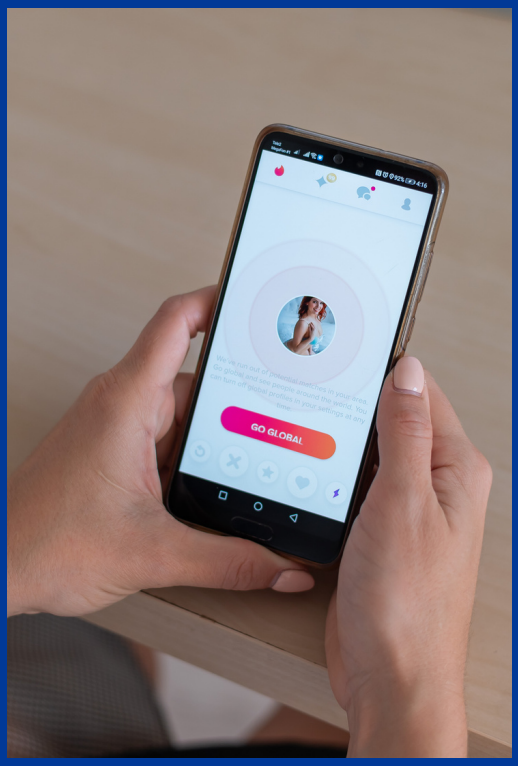
PRIVACY SHIELD V3 : LES USA ET L'UE TROUVENT UN ACCORD DE PRINCIPE POUR LE TRANSFERT DES DONNÉES PERSONNELLES

C'est en pleine guerre de l'invasion de l'Ukraine et la veille d'un accord de mise à disposition de 15 milliards de mètres cubes du gaz naturel liquéfié (DNL) américain pour palier la dépendance de l'EU au gaz russe que Ursula Von Der Leyen et Joe Biden signent un accord de principe pour remplacer le Privacy Shield invalidé par le 16 juillet 2020 par l'arrêt Shrem 2 de la Cour de Justice de l'Union Européenne.

Le Privacy Shield était supposé encadrer le transfert des données personnelles des citoyens européens vers les USA. Cependant, comme le souligne *Numerama*, « les USA n'ayant pas mené depuis 2020 les réformes juridiques adéquates pour satisfaire les règles du jeu européennes, il n'est pas besoin d'être devin pour supposer que cette troisième tentative échouera encore une fois. ».

Le Directeur du Centre de recherche français sur le renseignement Eric Denécé rappelle dans un entretien à France Soir que « les Américains peuvent piocher dans les données que nous leur transmettons comme ils le veulent en utilisant l'argument de la sécurité nationale, ce qui ouvre la porte à tous les abus. Or (...) Il n'y a pas de réciprocité des données avec les Américains. »

En savoir +



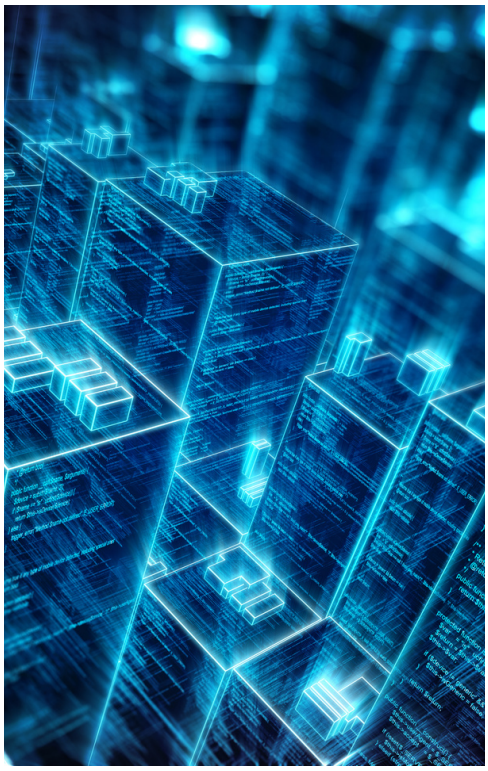
ÉTATS-UNIS : LES ANTÉCÉDENTS JUDICIAIRES DE VOS CONTACTS POTENTIELS VÉRIFIABLES SUR TINDER

La protection des données personnelles serait-elle irréconciliable des deux côtés de l'Atlantique ?

Aux États-Unis l'application Tinder va bientôt proposer de vérifier les antécédents judiciaires des matchs, suggérant qu'elle permet ainsi d'améliorer la sécurité de ses utilisateurs. Ce dispositif peut générer *« un faux sentiment de sécurité, les personnes malveillantes n'ayant généralement pas de casier judiciaire »*.

A cela s'ajoute les biais raciaux de la justice américaine qu'il convient de prendre en compte.

En savoir +



ANDROID : STOCKAGE DES DONNÉES TÉLÉPHONE ET MESSAGE PAR GOOGLE ?

Un professeur du Trinity College de Dublin a publié un article très approfondi intitulé : *« Quelles sont les données que les applications Téléphone et Messages sur Android envoient à Google ? »*.

Selon cette étude, il semble que lorsque l'on effectue un appel téléphonique, ou que l'on envoie un SMS, des données personnelles sont partagées sur des serveurs de Google, sans information préalable ni, à fortiori, consentement.

En particulier, le contenu des SMS serait transmis sous forme d'un hachage qui, s'agissant de messages courts, n'interdit pas la reconstitution du contenu.

De même que les données relatives aux appels (horodatage, durée) qui permettent de relier deux combinés impliqués dans un appel.

L'auteur de l'étude reproche aux deux applications de ne pas appliquer de règles de confidentialité, alors que Google les impose aux développeurs tiers.

Lire l'article