REVUE DE PRESSE
SEPT 2020 / MARS 2021

Revue de presse de l'actualité RGPD et Cyber de septembre 2020 à mars 2021

DPO Consulting
Your personal data protection officer
Bourgogne Franche-Comté

La Covid a largement stimulé l'activité cybermalveillante **qui a coûté 1 000 milliards de dollars à l'économie mondiale en 2020** selon France tv info. Une étude réalisée par Tanium affiche le constat que 93% des entreprises françaises ont connu une hausse des cyberattaques depuis la survenance du virus. En tête des menaces, les ransomwares ; d'après Zdnet, **« *les incidents liés aux rançons représentent 41 % des demandes d'assurances cyber déposées au cours du premier semestre 2020* »** et touchent tous les secteurs d'activité :

- Le BTP s'est vu une nouvelle fois impacté par un ransomware. Après Rabot Dutilleul et Bouygues Construction, c'est Leon Grosse qui a été touché par un cryptovirus. Le groupe a réussi à limiter les dégâts et restaurer progressivement ses services informatiques. Le Monde Informatique
- Le groupe Atlantic, spécialisé dans les solutions thermiques, a été victime d'un ransomware ralentissant largement l'activité de ses entreprises. Les cyberattaquants auraient volé certaines données et les auraient publiées après avoir essuyé un refus concernant le paiement de la rançon. Larep
- Des pirates ont réussi à s'infiltrer dans les serveurs de l'horloger Swatch au mois de septembre. RTS
- Le bailleur social Paris Habitat a subi une paralysie de son activité le 27 octobre par suite d'une attaque par rançongiciel. La situation a été rétablie en restaurant les systèmes informatiques sur la base de sauvegardes saines qui ont permis d'éviter le paiement de la rançon. Zdnet
- L'un des leaders mondiaux de la fabrication d'ordinateurs portables, Compal, a fait face à un ransomware en novembre. C'est la troisième grande entreprise Taïwanaise à avoir subi ce type d'attaque en 2020. Zdnet
- Les chambres de l'agriculture du Centre-Val de Loire et de Nouvelle-Aquitaine, placées sous tutelle de l'Etat, ont été interdites de payer la rançon. Les systèmes informatiques ont été remplacés par le papier-crayon le temps de rétablir la situation. Terre-net
- Les serveurs de SFR, Bouygues et une dizaine d'autres FAI européens ont subi une violente attaque par déni de service (DDoS). Selon 01net, il pourrait s'agir d'une attaque d'ampleur mondiale.
- La coopérative Cérèsia, embauchant 650 salariés, a subi une cyberattaque très sévère l'obligeant à déconnecter la totalité de ses systèmes informatiques au mois de décembre. L'Union
- Le ransomware Egregor a touché Randstad. L'entreprise d'intérim n'a pas subi d'interruption d'activité et a lancé une enquête sur l'incident. La Revue du Digital

Industrie-techno rappelle les 3 mesures principales sur lesquelles insiste l'ANSSI pour se défendre contre un rançongiciel dans un article en date du 7 septembre 2020 :

- **Déconnecter du réseau les systèmes d'information infectés ainsi que les supports de sauvegarde non touchés,**
- **Ne pas payer la rançon,**
- **Restaurer les systèmes sur la base de sauvegardes saines, antérieures à la compromission.**

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Les collectivités territoriales, victimes de cyberattaques

Le Grand Besançon, la mairie de Vincennes, d'Evreux, Alfortville, Bayonne, Bondy, Pantin, Aulnoye-Aymeries, Marseille, Charleville-Mézières, Annecy et La Rochelle ont comme point commun d'avoir subi les foudres d'une cyberattaque récemment, ce qui a considérablement ralenti leurs services. Face à cette situation, le **groupe d'intérêt public Acyma**, via sa plateforme cybermalveillance.gouv.fr, **est l'interlocuteur référent à contacter pour les collectivités et les TPE/PME**. Zdnet

Le secteur de la santé, une cible privilégiée

L'Usine Nouvelle fait état de la cyberattaque qui a mis à l'arrêt les usines du fabricant pharmaceutique Fareva. Global Security Mag rapporte de son côté que L'OMS est la cible d'une campagne de phishing par un groupe de cybercriminels Chinois. L'agence Européenne des médicaments a également été victime d'une cyberattaque au mois de décembre (BFM TV). Aux Etats-Unis, le ransomware Ryuk a compliqué la prise en charge de certains patients chez le géant hospitalier UHS, Le Monde Informatique indique que 4 personnes seraient décédées suite à cette prise en charge tardive. En 2020, les hôpitaux français représentaient 11% de toutes les cyberattaques recensées. Le Huffington Post indique que chaque semaine, un hôpital est la cible d'une cyberattaque ; le dernier en date est celui d'Oloron Sainte-Marie, contraint de travailler au « papier crayon » depuis le 8 mars. La rançon demandée s'élève à 50 000 dollars en bitcoins. **En réaction, Emmanuel Macron a déclaré vouloir renforcer sa stratégie en matière de cybersécurité notamment dans le domaine de la santé. Un milliard d'euros seront donc investis dans le secteur de la cybersécurité, dont les effectifs devraient doubler d'ici 2025**. LesEchos

Partenariat entre le ministère des Armées et le GIP Acyma

Florence Parly, ministre des Armées, fait le constat peu réjouissant de la multiplication par quatre du nombre de cyberattaques en un an. Toujours dans cette optique de fortifier la stratégie nationale cyber, la ministre souhaite « *renforcer les liens et les synergies entre les acteurs de la filière pour fédérer l'écosystème de la cybersécurité* ». Une convention a donc été signée entre le ministère et le groupement d'intérêt public (GIP) Acyma qui prévoit la mise à disposition à plein temps d'un officier de la Direction du renseignement et de la sécurité de défense (DRSD) au service du GIP. L'Usine Digitale

Actes de cyber espionnage

Le 6 mars dernier, Le Monde faisait état de l'attaque qu'a subi Microsoft, notamment le piratage du service de messagerie Exchange qui aurait touché plus de 30 000 organisations. **L'exploitation des failles du logiciel a permis aux pirates de voler les e-mails et d'installer des malwares facilitant l'accès au reste de l'environnement informatique** ; des correctifs ont été apportés depuis et les utilisateurs sont tenus de procéder aux mises à jour. L'Usine Digitale indiquait le 8 mars que l'Autorité Bancaire Européenne faisait partie des victimes, sans relever de vol de données personnelles.

Alors que la Russie est suspectée d'être derrière l'affaire SolarWinds (l'attaque très sophistiquée ayant permis d'espionner le gouvernement américain), Microsoft indique que les deux piratages ne sont pas liés. Au travers du groupe de hackers nommé Hafnium, la Chine est pointée du doigt.

Le télétravail, facteur de vulnérabilités

Guillaume POUPARD, directeur de l'ANSSI, avoue être préoccupé par les dispositifs de télétravail. **Public Sénat a relaté ses préoccupations** : « *on est quand même assez inquiets sur toutes les brèches que ça a pu ouvrir dans les systèmes d'information, le risque est que l'on s'en rende compte dans quelques mois* ». La transition digitale précipitée des PME et TPE n'a pas échappé aux hackers. Le site de France Info rappelle les bonnes pratiques à adopter pour pouvoir télétravailler en sécurité.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Les incidents de sécurité cyberphysique directement imputables aux PDG ?

Les incidents cyberphysiques qui peuvent causer des dommages directement aux personnes, aux biens et à l'environnement deviendraient directement imputables aux PDG et non plus aux entreprises, selon Gartner. Une étude réalisée par le cabinet d'analyses prévoit qu'ils deviendraient les premières causes d'incidents informatiques et concerneraient 75% des responsables d'entreprise d'ici 2024. « ***Les PDG ne pourront plus plaider l'ignorance ou se retrancher derrière les polices d'assurance*** » alors que l'impact financier pourrait atteindre 50 milliards de dollars d'ici deux ans. Zdnet

Les gamers fortement touchés par les cyberattaques

Le secteur du jeu vidéo est en plein essor et en raison des mesures sanitaires, il a attiré énormément de joueurs en ligne non sensibilisés aux cyber risques. Une étude réalisée par Akamai démontre que ce n'est pas une préoccupation pour les gamers ; « *seulement un cinquième des joueurs interrogés par Akamai se sont dit inquiets de voir leurs comptes de jeu compromis* ». Presse Citron relate pourtant qu'ils sont très ciblés par les attaquants, notamment ceux qui réalisent des attaques par déni de service.

Focus sur les fuites de données

Les fuites de données peuvent coûter très cher aux entreprises (le site efl.fr fait état d'une étude détaillée sur l'impact financier) et rapporter beaucoup aux revendeurs. C'est un marché juteux dont le prix de la donnée peut varier de 20$ à 200$ selon la rareté de l'information, rapporte BFM TV. **Zataz propose un service très intéressant de veille individualisée qui vous alerte quand il repère une fuite d'informations personnelles vous concernant dans les espaces pirates ou une fuite au sein d'une entreprise**, vous permettant de réagir en conséquence très rapidement.

Quels risques pour les personnes concernées par les fuites de données ?

Si votre nom, adresse électronique ou numéro de téléphone ont fuité, les pirates pourront facilement vous contacter en se faisant passer pour un organisme public ou privé légitime et ainsi gagner votre confiance. Sous couvert de leur fausse identité, ils peuvent vous demander de remplir un faux formulaire afin de collecter vos données ; « *ces informations sont ensuite utilisées pour accéder, par exemple, à des comptes sécurisés et effectuer des opérations sous l'identité de la victime* » indique la CNIL. **En quelques clics, les pirates peuvent modifier les accès aux différents services, par exemple bancaires**, grâces aux données personnelles récoltées ; s'en suit une éprouvante aventure afin d'arriver à prouver votre identité et récupérer vos accès.

L'histoire d'un professeur d'université de 42 ans, relatée par Orange, victime d'un réseau d'escrocs ayant usurpé son identité pour lui attribuer 400 voitures immatriculées à son nom, témoigne du calvaire subit par la victime. L'affaire traîne depuis 2018 et sa situation s'empire ; le Trésor public lui réclame 300 000€ d'amende pour les infractions commises par ses voitures qui ne lui appartiennent pas, alors que rien ne bouge du côté administratif pour rectifier sa situation.

Le 3 mars dernier, Capital mettait en garde contre l'explosion des arnaques sur les épargnes par usurpation d'identité. « *Les signalements d'épargnants victimes d'arnaque financière liée à des usurpations représentent 44% des montants déclarés perdus en 2020* » indique l'AMF. Le préjudice est évalué à 45 000€ par personne lésée. Les cibles sont incitées à saisir les offres au plus vite par ces organismes à l'apparence légitime. L'occasion de rappeler l'importance de prendre le temps de vérifier l'identité de vos interlocuteurs.

Fuite de données chez Spotify

D'après un article du site 20minutes publié le 12 décembre dernier, les partenaires commerciaux de Spotify ont pu consulter les données personnelles de nombreux utilisateurs par suite d'une faille de sécurité tardivement corrigée. Ce n'est pas la première fuite que connaît la plateforme de musique.

DPO Consulting
Your personal data protection officer
DPO **Consulting** franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric **CUENOT** / Président & Data Privacy Officer **06 65 91 28 76** eric.cuenot@dpo-consulting.com
Stéphanie **BROGGINI** / Data Privacy Officer **06 85 06 11 43** stephanie.broggini@dpo-consulting.com

Fuite de données à l'Université de Franche-Comté

Près de 6 000 personnes ont été contactées le 10 mars par l'Université de Franche-Comté, pour les informer que leur adresse mail ainsi que leur mot de passe universitaires se sont retrouvés sur le darkweb. L'Université a fait partie des cibles touchées par la fuite Cit0Day qui comptabilise près de 23 000 bases de données volées selon MaCommune.info. Si la présidente de l'Université indique que les mots de passe compromis sont chiffrés, donc illisibles dans la base de données, « *elle conseille "fortement" de changer ce mot de passe partout où il a été utilisé* » pour éviter tout risque tel que l'usurpation d'identité. Cette fuite a fait l'objet d'un signalement auprès de la CNIL.

Un haut responsable de Cdiscount mis en examen

Dans un article du 8 février dernier, L'Usine Digitale faisait état de 33 millions de données clients volées et mises en vente sur le darknet par le directeur du site Cdiscount à Cestas, près de Bordeaux. Aucune donnée bancaire ne serait concernée mais les noms, prénoms, adresses électroniques et montant total des commandes sur les deux dernières années sont compromis.

Quatre villes mises en demeure par la CNIL

Le dispositif de lecture automatisée des plaques d'immatriculation (LAPI), utilisée par certaines polices municipales pour contrôler les stationnements gênants voire dangereux, a amené quatre mises en demeure adressées par la CNIL contre les villes de Marseille, Brest, Pau et Kremlin-Bicêtre. Caradisiac

Les applications éducatives et les données personnelles

Les applications éducatives qui proposent des enseignements et un apprentissage à distance permettent d'assurer une continuité pédagogique pendant la crise sanitaire. Une enquête réalisée par l'IDAC révèle qu'elles comporteraient de nombreuses faiblesses tenant à la confidentialité et la sécurité des données. Les défauts résideraient dans la collecte excessive des données des utilisateurs et le partage de ces données avec des tiers. L'Opinion

Usage de caméras thermiques dans des lycées

La CNIL n'est pas favorable à l'utilisation des caméras intelligentes. Pourtant, le Conseil d'Etat la tolère tant que les personnes concernées **peuvent refuser de s'y soumettre sans se voir refuser l'accès à l'établissement**. C'est ainsi que trois lycées de la région Auvergne Rhône-Alpes se sont équipés de ce dispositif qui ne conserve aucune donnée personnelle et qui permet de minimiser les risques sanitaires. L'Usine Digitale

Les données de performance sportive, soumises à consentement ?

Les données de performance des sportifs sont traitées par les clubs, les jeux vidéo et les sociétés de paris sportifs. Certains estiment qu'il s'agit de données publiques puisqu'elles sont collectées au cours de compétitions regardées par un public et analysées par les médias. Plus de 400 footballers anglais revendiquent au contraire des traitements de données personnelles auxquels ils n'ont pas consenti. « *Si la justice leur donne raison, certains joueurs pourraient exiger des dizaines de milliers d'euros d'indemnisation pour l'exploitation non autorisée de leurs données au cours des dix dernières années* ». Slate

Le droit à l'effacement et les personnes mineures

Un article des éditions Francis Lefebvre est venu indiquer qu'**un mineur, même s'il n'a pas acquis la majorité numérique de 15 ans, peut demander à un site Internet d'effacer les données collectées sur lui sans que le consentement des détenteurs de l'autorité parentale ne soit requis**. Cet article fait suite à un rapport parlementaire rendant compte des nombreuses situations dans lesquelles les parents sont à l'origine de la diffusion des données du mineur et trouve un intérêt financier à leur mise en ligne.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Les craintes face aux assistants vocaux

En septembre dernier, la CNIL a publié un livre blanc préventif pour encadrer les assistants vocaux et anticiper les menaces qui pourraient en découler. Elle recommande une meilleure transparence sur l'utilisation des informations personnelles et préconise un traitement local, techniquement possible très bientôt, plutôt qu'un traitement sur des serveurs distants. Francetvinfo.fr

Les « badgeuses photo » ne sont pas conformes au RGPD

La CNIL, qui a reçu six plaintes provenant d'employés dénonçant l'instauration de « badgeuses photo » au sein de leur structure, a publié un communiqué dans lequel elle indique que la prise de photographie à chaque pointage est excessive au regard du principe de minimisation. Elle met donc en demeure ces organismes de se conformer au RGPD. Villes-internet

Wi-Fi gratuit : des patrons de bar en garde à vue

Ouvrir sa box Internet à ses clients fait de vous un fournisseur d'accès à Internet. À ce titre, il vous incombe de respecter certaines règles en matière de conservation des données de connexion. **Certains patrons de bars grenoblois ont méconnu ces règles et se sont retrouvés en garde à vue**. L'occasion de rappeler qu'il est préférable, pour ces questions de rétention de données, de passer par un partenaire proposant un Hotspot Wi-Fi respectant ces règles. Zdnet

Données de connexion : recadrage de la CJUE

Le 6 octobre 2020, la CJUE a interdit la conservation généralisée et indifférenciée des données de connexion par les FAI. Une conservation généralisée pourra être mise en œuvre dans le cas où l'Etat fait face à une menace grave pour la sécurité nationale à condition d'être encadrée par un magistrat et temporellement limitée. La France devra donc se conformer à la position de la CJUE puisqu'à ce jour, la loi prévoit que les FAI et autres intermédiaires techniques sont tenus de conserver toutes les métadonnées pendant une durée d'un an afin d'être en mesure de les communiquer aux autorités judiciaires. Zdnet

Rachat de Fitbit par Google approuvé sous conditions

Numerama rapporte que le rachat de Fitbit (entreprise qui commercialise des objets connectés) par Google a été approuvé par la Commission Européenne sous certaines conditions relatives à l'exploitation des données personnelles. Google devra respecter ses engagements pendant une période d'au moins 10 ans.

Télétravail et surveillance

La loi autorise les employeurs à surveiller leurs salariés qui télétravaillent en respectant quelques conditions. Le contrôle doit être justifié, proportionné et doit respecter le RGPD. ***« Aucune information concernant personnellement un salarié ne peut-être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. ».*** Le site Slate relate les façons dont certains employeurs excèdent le champ légal et espionnent véritablement leurs employés.

Concernant l'activation des caméras au cours des visioconférences, il n'est pas possible de l'imposer de manière généralisée. Il est cependant possible de l'exiger de manière ponctuelle si vous démontrez que l'usage de la caméra est justifié et proportionné au regard de l'objectif de la conférence.

Amazon abuse-t-il de sa position dominante ?

Le site RTL indique qu'Amazon espionnerait et volerait les données clients de ses concurrents présents sur son marché en ligne. Il rappelle que Google Shopping a déjà été condamné par la Commission Européenne à payer une amende de 2 milliards et demi d'euros pour des raisons similaires en 2017.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Case pré cochée : défaut de consentement

La Cours de cassation rappelle, dans son arrêt du 11 novembre 2020, qu'une case pré cochée figurant dans un contrat ne constitue pas un recueil valable du consentement à un traitement de données personnelles. Dalloz-actualite

Données personnelles et preuve prud'homale

Un employeur a retrouvé l'auteur d'une faute commise par un de ses salariés en retrouvant l'adresse IP fautive collectée irrégulièrement en vertu des règles antérieures au RGPD, dans un fichier de journalisation. Le salarié, remercié pour faute grave, a contesté son licenciement fondé sur une preuve illicite. La Cour de cassation, dans son arrêt du 25 novembre, considère que **le droit à la preuve de l'employeur « *peut justifier la production d'éléments portant atteinte à la vie personnelle d'un salarié* » à condition qu'elle soit nécessaire et proportionnée.** Nextinpact

Surveillance par drone

La préfecture de police de Paris, après une première tentative échouée d'utiliser les drones pour contrôler le respect des règles sanitaires en mai dernier, a remis le couvert en mettant en place un dispositif de surveillance des manifestations par drone. Malgré l'effort de flouter les images avant l'envoi en poste de commandement, l'absence de texte venant autoriser et fixer les modalités de ce dispositif fait dire au Conseil d'État qu'il existe de sérieux doutes quant à la légalité de ce dispositif. Il a enjoint au Préfet de police de faire cesser ces mesures de surveillance. Zdnet

L'application TaData validée par la CNIL

L'application propose aux jeunes âgés entre 15 et 25 ans de gagner de l'argent en vendant directement leurs données personnelles. **« *Cette start-up est la première à permettre aux internautes de tirer profit de leurs données plutôt que de laisser les GAFAM les exploiter* »** explique le site Challenges. Après quelques aménagements sur le recueil de consentement et sur le droit d'opposition, la CNIL a donné son feu vert à ce nouveau concept.

Réservations d'hôtel en ligne : 10 millions de données exposées

La société espagnole Prestige Software propose une plateforme utilisée par les plus grands sites de réservation d'hôtel en ligne tel qu'Expedia, Booking ou encore Hotel.com. Le Journal du Geek indique que 10 millions de données confidentielles ont été exposées en ligne à la suite d'une faille de sécurité, sans que l'on sache si des cybercriminels ont eu le temps de mettre la main dessus. Pour l'heure, les risques de phishing ou de fraude à la carte bancaire planent à la suite de cette exposition.

Violations au RGPD : les amendes tombent en Europe

Alors que le Siècle Digital annonce qu'en 2022, de nouvelles règles européennes viendront faciliter les recours collectifs pour violation des données, les manquements au RGPD sont d'ores et déjà lourdement sanctionnés. En première ligne, British Airways qui n'a pas détecté l'attaque informatique qu'elle subissait et qui a permis la fuite de données de plus de 400 000 clients, a écopé d'une amende prononcée par la CNIL Anglaise (ICO) de 20 millions de livres sterling.

Même sentence pour Mariott qui récolte une amende de 18,4 millions de livres sterling pour ne pas avoir suffisamment sécurisé les données. Le Monde indique que la fuite de données concerne ici 339 millions de personnes.

En Allemagne, le groupe de prêt-à-porter H&M a écopé d'une amende de 35 M€ pour avoir collecté et conservé illégalement les données personnelles de leurs employés entre 2014 et 2019. L'Usine Digitale

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Carrefour réprimandé en France

Carrefour France et Carrefour Banque ont fait l'objet d'une sanction prononcée par la CNIL de 3 millions d'euros pour divers manquements au RGPD détaillés par L'Informaticien. En premier lieu, une atteinte au principe de transparence exigeant que les personnes concernées soient informées de façon claire et compréhensible du traitement de leurs données dans un document facile d'accès. En l'espèce, l'accès aux politiques relatives aux données personnelles était compliqué et leurs mentions peu compréhensibles. Les durées de conservation des données ont été jugées excessives et l'ineffectivité des droits des personnes concernées ont conduit la CNIL a prononcé une sanction de 2,2 M€ à Carrefour et 800 000€ à sa filiale Carrefour Banque.

Sanction record en France contre Google

Le 4 mars, le Conseil d'État a validé la **sanction record d'une amende de 100 M€** prononcée par la CNIL à l'encontre de Google. **L'autorité de contrôle reproche le dépôt automatique de cookies publicitaires sur le site google.fr sans consentement et sans information pour l'utilisateur**. La CNIL avait laissé à Google trois mois pour se mettre en conformité avec les principes de la directive ePrivacy et 100 000€ d'astreinte à payer par jour de retard. La société reprochait le montant trop élevé de l'astreinte et considérait que ce délai laissé était beaucoup trop court. La compétence de la CNIL était également interrogée. L'autorité de contrôle a été appuyée par le Conseil d'État, indique L'Usine Digitale. Pour ces mêmes raisons, le géant Amazon a écopé d'une amende de 35 M€.

Sanction de la prospection sans consentement

La société Nestor, spécialisée dans la livraison de repas, a été sanctionnée d'une amende de 20 000€ pour avoir envoyé des emails de prospection sur la base d'informations recueillies sur internet sans consentement ni information préalable. Selon La Revue du Digital, cela concernerait plus de 600 000 prospects. Les contrôles de la CNIL révèlent également que le site web de l'entreprise n'est pas conforme au RGPD et que les droits des personnes concernées ne sont pas effectifs, notamment le droit d'information et d'accès aux données que l'entreprise détient sur les personnes qui la sollicitent.

Une mise en conformité ardue pour l'annuaire de l'ICANN

L'annuaire des noms de domaine Whois peine à se conformer au RGPD. Le Monde Informatique précise que l'annuaire a été fermé le temps de trouver une solution mais que des alternatives conformes existent.

Plaintes pénales en cours

Dans un article du 8 mars, L'Equipe faisait état d'une affaire de violations de données venues bouleverser les élections à la présidence de la Fédération Française d'Équitation. Cette dernière a porté plainte pour « *divulgation illégale volontaire de données à caractère personnel, détournement de la finalité d'un traitement de données à caractère personnel et extraction frauduleuse de données contenues dans un système de traitement automatisé* » contre une cadre technique du Ministère de l'Éducation nationale, de la Jeunesse et des Sports mise à la disposition de la FFE. La mise en cause aurait fait une utilisation suspecte d'identifiants de la Fédération pour consulter des informations personnelles des licenciés et l'historique des licences. Ces agissements répondraient à une demande émanant d'une candidate à l'élection et viseraient à contrôler les critères d'éligibilité d'autres candidats.

Plainte déposée devant la CNIL

Le 9 mars, L'Usine Digitale indiquait que l'association France Digitale, représentant près de 1 800 start-up, a déposé une plainte devant la CNIL contre Apple. La mise à jour iOS 14 prévoirait un ciblage publicitaire par défaut sur certaines applications Apple, un manquement au recueil du consentement éclairé et univoque imposé par le RGPD. Cette pratique a fait naître un sentiment d'injustice pour les « petits » acteurs français, soucieux et contraints de rentrer dans les clous du RGPD.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Bug de l'application mobile LCL : La CNIL enquête

Le 23 février dernier, entre 17h40 et 18h40, l'application mobile LCL a rencontré un bug permettant aux clients d'avoir accès non pas à leurs comptes bancaires, mais aux comptes d'un autre utilisateur ainsi que ses dernières opérations. Il ne s'agissait non pas d'un acte malveillant mais bien d'un bug technique comme le rapporte BFM TV. La CNIL va donc enquêter sur l'affaire et prononcera peut-être une sanction pour violation au RGPD.

Deux sites de téléconsultations condamnés

En novembre dernier, le Tribunal judiciaire de Paris a condamné les dérives de deux sites de téléconsultations spécialisés dans les arrêts maladies. Il leur est reproché de créer un marché de la prescription et de ne pas stocker les données qu'ils traitent chez des hébergeurs agréés, comme l'oblige le Code de la santé publique. Le Tribunal a donc prononcé la fermeture définitive de ces plateformes sous 24h. L'Usine Digitale

Deux médecins sanctionnés par la CNIL

Le 7 décembre dernier, la CNIL a retenu un manquement à l'obligation de sécuriser les données et de lui notifier toute violation de celles-ci contre deux médecins libéraux qui écopent de 3 000€ et 6 000€ d'amende. Il leur est reproché d'avoir mal configuré leurs réseaux informatiques, ce qui a conduit à rendre les données librement accessibles sur Internet. La CNIL relève également un défaut de chiffrement des données hébergées sur leurs serveurs. Les images médicales de leurs patients se sont retrouvées librement accessibles sur Internet sans que les deux médecins ne l'aient notifié à la CNIL après en avoir eu connaissance.

Fuite des données de santé : le début d'une grande affaire

Des données médicales en libre accès sur internet suite à la fuite émanant de laboratoires d'analyse médicale (dont le nom, le numéro de sécurité sociale, le groupe sanguin et bien d'autres informations sur les personnes) concerneraient 500 000 Français dont 300 000 bretons selon RTL. La CNIL s'était étonnée de n'avoir reçu aucune notification alors que la fuite proviendrait d'une trentaine de laboratoires d'analyse médicale. Numerama rapportait le 24 février qu'elle allait enquêter pour « *constater l'ampleur de l'incident et vérifier l'attitude des responsables en charge de la sécurisation de ces informations* ».
À ce jour, tous les laboratoires impliqués se seraient signalés et s'organisent pour contacter rapidement les personnes concernées par cette fuite de données sensibles. Les personnes auront alors la possibilité de déposer plainte, indique France Bleu.
Le piratage à l'origine de cette fuite fait l'objet d'investigations menées par l'ANSSI, le Ministère des Solidarités et de la Santé ainsi que la CNIL. La section cybercriminalité du parquet de Paris est également sur le coup, selon Ouest France.
En attendant, les autorités prennent toutes les mesures permettant de préserver ces données sensibles du mieux possible. Le 4 mars, le Tribunal judiciaire de Paris a ordonné à SFR, Bouygues, Orange et Free de bloquer immédiatement, et pour une durée de 18 mois, un site hébergeant ces données sensibles.
La fuite de tous ces numéros de sécurité sociale est très préoccupante du fait de la nature hautement personnelle de cette donnée qui révèle, à elle seule, énormément d'informations sur vous.
Elle peut devenir dramatique pour les personnes n'ayant pas encore créé de compte Ameli. Comme le relève Cyberguerre Numerama, ce compte détient des informations médicales qui peuvent servir aux hackers « *pour faire du chantage, ou pour effectuer des paiements de soin frauduleux.* » Il permet également de se connecter à différents services publics grâce au système FranceConnect et avoir accès à toute sorte de démarches administratives. La création de ce compte Ameli nécessite le numéro de sécurité sociale, le nom et le code postal. Toutes ces données se retrouvent dans la fuite.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

RGPD et responsabilité : responsable de traitement / sous-traitant

Le 27 janvier dernier, la CNIL a sanctionné un responsable de traitement et son sous-traitant d'une amende respective de 150 000€ et 75 000€ pour manquement à leur obligation de sécuriser les données personnelles de leurs clients. 40 000 données personnelles auraient fuité par suite d'une attaque par bourrage d'identifiants sur le site marchand en cause. **Cette décision démontre la nécessité de renforcer les liens contractuels entre le responsable de traitement et son sous-traitant pour éviter ces cas de coresponsabilité**. Retrouvez l'analyse complète de cette décision par notre juriste DPO, Stéphanie Broggini, sur LinkedIn.

Champs prioritaires de contrôle de la CNIL

Le 2 mars, la CNIL a fait savoir les trois grandes thématiques qu'elle priorisera en 2021 ;

- **Sécurité des sites web français** : elle contrôlera les formulaires recueillant les données personnelles, l'utilisation du protocole HTTPS, les politiques concernant les mots de passe et les stratégies adoptées pour éviter les rançongiciels.

- **Sécurité des données de santé** : elle vérifiera la « *gestion des accès au dossier patient informatisé au sein des établissements de santé, plateformes de prise de rendez-vous médicaux en ligne, gestion des violations de données personnelles* » et a pour ambition d'élever le niveau de sécurité de ces données.

- **L'utilisation des cookies** : elle vérifiera l'application des règles relatives au recueil du consentement détaillées par ses lignes directrices et sa recommandation en date du 1er octobre. Pour rappel, les sites web et applications mobiles avaient jusqu'au 31 mars pour y être conformes.

Transfert des données vers les Etats-Unis : où en est-on ?

Depuis l'invalidation du Privacy Shield décidée par la Cour de justice de l'Union Européenne en juillet dernier, la question du transfert des données vers les Etats-Unis est sensible. La CJUE tolère ce transfert en vertu des clauses contractuelles types si elles présentent un haut niveau de garantie contre la surveillance des services de renseignement américains.

Ce n'est pas le cas des clauses que propose Facebook. La CNIL Irlandaise (DPC) lui a demandé de ne plus transférer les données depuis l'Europe vers les Etats Unis. Jugeant cette demande irréalisable, le réseau social menace de boycotter le marché Européen. Clubic

Le Comité Européen de la protection des données (CEPD) a rendu ses recommandations. Les clauses contractuelles types doivent être accompagnées d'une vérification quant au niveau de protection des données conféré par la législation étrangère, qui se doit d'être équivalente à la protection européenne. Des garanties supplémentaires doivent être adoptées en complément de ces clauses si le niveau de protection se révèle insuffisant.

Concernant les États-Unis, la loi américaine qui autorise la NSA à connaître des données étrangères stockées sur des serveurs américains fait obstacle au niveau de protection requis. « *Bruxelles attend de Washington des changements dans les procédures de surveillance. Reste à savoir si l'administration Biden serait encline à cette révision* » indique L'Usine Digitale. Le 11 mars, le même site relatait les inquiétudes de Washington concernant sa position d'État tiers non conforme aux exigences européennes de protection des données et les risques de rapatriement massif de ces données en Europe.

Le Parisien rapporte qu'une centaine de chauffeurs Uber ont saisi le Conseil d'Etat afin qu'Uber soit contraint à plus de transparence concernant des possibles transferts de données outre-Atlantique et démontre des garanties appropriées.

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com

Les conséquences sur le cloud

Alors que l'hébergement des données de santé de la plateforme Health Data Hub par Microsoft fait débat à la suite de l'invalidation du Privacy Shield, le Conseil d'État a estimé que le risque pour ces données sensibles était faible et n'a donc pas écarté Microsoft dans l'immédiat. Ce n'est pas la position prise par l'Assurance Maladie le 19 février, qui considère l'implication de l'entreprise américaine comme un problème. Numerama

Le 5 mars, France24 faisait état de la nouvelle inquiétude qui pèse sur les données de santé. L'entreprise Doctolib est impliquée dans la stratégie vaccinale adoptée par le gouvernement. Un recours a été déposé devant le Conseil d'État par des syndicats de médecins inquiets pour la protection des données car la plateforme utilise *Amazon web services*, un cloud également soumis au droit américain. Cette protection est « *intimement liée au secret médical qui est essentiel pour conserver la confiance des patients* », confie un syndicaliste. L'ordonnance rendue par le Conseil d'Etat le 12 mars 2021 valide pourtant ce partenariat. Il estime que des garanties sont en place pour faire face aux demandes d'accès éventuelles des autorités américaines. Numerama

La problématique n'est pas exclusive au secteur de la santé, Le Monde Informatique détaille ce qu'il faut analyser pour savoir si l'utilisation d'un service cloud américain est possible : « *Il est maintenant essentiel que les DSI agissent pour mettre en conformité avec le droit européen l'infrastructure cloud que leur entreprise utilise*. »

Il est à noter qu'une alliance entre OVH et Google est en train d'être scellée afin de proposer une solution d'hébergement purement européenne chez OVHcloud, tout en profitant des technologies avancées de Google. LesEchos

Cyber assurance de Google Cloud allié à Allianz et Muniche Re

Alors que les assurances cyber peinent encore à s'installer en entreprise, elles vont certainement se révéler cruciales dans un avenir proche. C'est pourquoi Google lance un outil proposé aux clients de Google Cloud, le « Risk Protection Program ». Ce programme réalise un diagnostic sur le niveau de sécurité de l'entreprise transmis à Allianz et Munich Re qui l'étudient pour proposer une police d'assurance adaptée en fonction du niveau de sécurité de l'entreprise : le *Cloud Protection +.*
L'Usine Digitale explique dans un article en date du 4 mars que « *plus le niveau de sécurité sera élevé et plus le prix de Cloud Protection + sera bas. Ce qui pousse finalement les personnes à mieux se protéger contre les cyberattaques.* »
L'outil est pour l'instant réservé aux utilisateurs américains mais devrait rapidement s'étendre au reste du monde.

Revue de presse réalisée avec le concours de
Florine GIACOMUZZI
Stagiaire étudiante Master II «Droit du numérique»
Université de Franche-Comté

DPO Consulting
Your personal data protection officer
DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC - Espace Besançon - 25115 POUILLEY-LES-VIGNES - RCS Besançon 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 06 85 06 11 43 stephanie.broggini@dpo-consulting.com