Revue de presse de l'actualité RGPD et Cyber d'avril à juillet 2021

Dans un rapport publié le 19 avril, l'assureur Hiscox indiquait que près d'une entreprise française sur deux (49%) avait été la cible d'une cyberattaque durant l'année 2020, contre 34% l'année précédente (New Assurance Pro). Dans le même temps, Canalys, cabinet d'analyse du marché mondial des technologies, a relevé que 30 milliards de données avaient été volées. Courrier international

Cette augmentation du cybercrime, et notamment du ransomware, a été facilitée par la crise sanitaire et le recours au télétravail. Elle l'a également été par les paiements trop nombreux des rançons demandées par les pirates. Le rapport d'Hiscox relève en effet que 58% des entreprises ciblées dans le monde ont cédé au chantage. L'explosion du nombre de cyberattaques **devrait coûter 6 000 milliards de dollars à l'économie mondiale en 2021** indique Europe 1 et la liste des victimes des derniers mois dans le monde conforte cette expectative :

- Le spécialiste de l'informatique Acer a été confronté à une demande record de rançon. Le montant s'élevait à 50 millions d'euros. Le Mag IT fait état des négociations entreprises entre la société et les pirates, sans en donner l'issue.
- L'université de Montpellier a été ciblée par un ransomware le 1er avril, paralysant le fonctionnement de certains services informatiques. Le Mag IT
- Le 11 avril, In Extenso déplorait une cyberattaque paralysant une partie de son informatique. Le groupe, qui compte plus de 100 000 TPE/PME parmi ses clients, n'a pas subi de fuite de données, rapporte Le Mag IT.
- Le groupe d'édition La Martinière a également connu une marche au ralenti suite à une attaque survenue le 13 avril paralysant ses services en ligne. Le Mag IT
- Le 20 avril, l'organisme de formation Cegos annonçait avoir subi une cyberattaque susceptible d'avoir compromis les données personnelles qu'il détenait et invitait les personnes concernées à faire preuve de vigilance quant à l'identité de leurs interlocuteurs.
- Un escape game situé à Castres proposant une activité en ligne pour faire face à la crise sanitaire a également été confronté à un ransomware. La Dépêche
- Même peine pour UniLaSalle, une école d'ingénieurs, qui a fait face à la même menace le 21 avril, la contraignant à suspendre tous les services pendant une quinzaine d'heures avant de reprendre les cours en distanciel. Le Mag IT
- Après la détection d'une intrusion dans son système informatique, Laurent Perrier a dû déconnecter ses serveurs pour rétablir son activité progressivement de manière sécurisée. Le titre perdait 1% à la Bourse de Paris le 26 avril suite à cette annonce. BFM Bourse
- Le 7 mai, un ransomware a fait beaucoup de bruit en touchant l'américain Colonial Pipeline, l'opérateur d'oléoducs. 4,4 millions de dollars ont été versés aux pirates informe Le Monde. Au vu de la cible, on s'attendait à ce qu'une puissance étatique soit derrière cette attaque. Le groupe DarkSide à l'origine de l'incident n'est pourtant affilié à aucun pays et a agi pour ses intérêts, rapporte Futura Sciences. En réaction, le gouvernement américain compte dorénavant **traiter ces attaques avec la même rigueur que les infractions liées au terrorisme**. L'Usine Digitale
- Après l'attaque contre le géant de l'agroalimentaire JBS au début du mois de juin, le groupe cybercriminel REvil a réalisé **« une des plus grandes attaques rançongiciel de tous les temps »** en exploitant, le 2 juillet, une vulnérabilité présente dans un logiciel édité par Kaseya, explique François Manens de chez Cyberguerre. Le nombre d'infections est encore inconnu… tandis que les hackers proposent le paiement d'une somme globale de 70 millions de dollars pour rétablir les systèmes.

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 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

Les secteurs les plus touchés sur 2020

Le rapport d'activité de 2020 publié le 10 juin par l'ANSSI constate que **les établissements de santé, les collectivités territoriales et le secteur de l'industrie ont été les principales victimes de ransomwares** l'année dernière et cette tendance se poursuit en 2021. Le fonctionnement de l'hôpital de Saint-Gaudens[1], les cliniques du Grésivaudan[2] et des Cadrans Solaires[3], ou encore le centre de vaccination de Berck-sur-Mer[4] et le laboratoire pharmaceutique Pierre Fabre[5] ont été touchés au cours du mois d'avril.

Dans le même temps, des ransomwares ont atteint les villes de l'Isle-sur-la-Sorgue[6], de Morières-lès-Avignon[7] et de Douai[8], provoquant des perturbations dans les services.

Du côté des industriels, leurs installations sont de plus en plus connectées, ce qui emmène son lot de vulnérabilités. Ces systèmes industriels impliquent des efforts encore trop méconnus concernant la cybersécurité (différente de celle afférente à l'informatique « généraliste »). Interrogé par L'Usine Nouvelle, Danny BREN, spécialiste de la cybersécurité des systèmes industriels, alerte sur la méconnaissance des enjeux. La France est une cible privilégiée compte tenu de sa place mondiale parmi les centres industriels et de son retard sur ces sujets.

La cybersécurité, un enjeu de taille pour les entreprises

Les tentatives de phishing ont augmenté de 400% depuis mars 2020. Dans le même temps, le nombre d'attaques par ransomware a été multiplié par 4, rappelle LesEchos dans un article du 4 avril. Le coût des actes de cybercriminalité varie entre 80 et 100 millions d'euros par an aux entreprises françaises (BFMTV), alors que le montant des préjudices avoisinerait le milliard. Par manque de sensibilisation et de budget, la protection des réseaux et des données professionnelles est aussi mise à mal par l'explosion du télétravail suite à la pandémie. L'usage des smartphones a également monté en flèche. « *45% des entreprises ont vu au moins un de leurs salariés télécharger une application mobile malveillante au cours de l'année 2020* » rapporte Presse Citron. Une vulnérabilité supplémentaire à surveiller au sein des organisations.

Le 10 juin, la délégation aux entreprises du Sénat publiait un rapport d'information traitant de la cybersécurité des entreprises axé sur 3 thèmes (résilience des entreprises, alerte/formation sur les cyber risques et protection des TPE-PME) et contenant une vingtaine de propositions. Vie publique

Réseaux sociaux et données personnelles

Les données présentes sur les réseaux sociaux nourrissent de nombreuses bases de données en vente sur le darkweb. Bien souvent, **il s'agit d'informations publiées par les utilisateurs eux-mêmes**, qui sont simplement aspirées par des tiers pour constituer une base de données exploitable. Ainsi, ZDNet indiquait le 30 juin que les données personnelles de 700 millions d'utilisateurs LinkedIn étaient en vente sur Internet (en avril déjà, 500 millions d'utilisateurs du réseau social ont fait l'objet d'une vente de leurs données personnelles) tandis que Le Big Data évoquait la mise en ligne des données d'1,3 million d'utilisateurs de ClubHouse, le réseau social audio lancé en 2020. Facebook ne fait pas exception ; plus de 500 millions d'utilisateurs ont vu leurs données personnelles publiées sur un forum de cybercriminels suite à une fuite ayant eu lieu en 2019. La CNIL Irlandaise a d'ailleurs ouvert une enquête en avril. Le Monde Informatique

Parmi ces données, on retrouve le nom, adresse mails, numéro de téléphone, voire adresse du lieu de vie des utilisateurs. Autant d'informations utiles aux cybercriminels pour mener des campagnes de phishing efficaces ou usurper l'identité d'une personne.

Have I Been Pwned, un site d'intérêt public

Pour savoir si vos données personnelles sont concernées par une fuite de données, le seul site recommandé est haveibeenpwned.com qui jouit d'une réputation et d'une confiance à l'internationale. En atteste la base de données de 4,3 millions d'adresses emails et informations correspondantes détenue par le FBI après le démantèlement du malware Emotet. Celle-ci a été transmise à Troy Hunt, le créateur du site, afin d'alerter les victimes du botnet. Journal du Geek

1 Le Parisien
2 Actu.fr
3 Actu.fr
4 BFM TV
5 Le Figaro
6 Le Dauphiné
7 Le Dauphiné
8 La Voix du Nord

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

Usurpation d'identité

L'étude annuelle du FBI relatif à la cybersécurité place la France dans le top 10 des pays les plus touchés avec, en tête des menaces, les attaques par phishing. Au cours des 12 derniers mois, 18 millions de Français ont été victimes de la cybercriminalité, relate L'Usine Digitale. La principale inquiétude des personnes concernées réside, dans les risques d'usurpation d'identité. 64% des Français se sentiraient désarmés et ne sauraient pas quelles démarches entreprendre si cela leur arrivait.

Il est pourtant primordial que les utilisateurs soient éclairés sur ces risques et l'importance d'être vigilant sur l'identité des interlocuteurs lorsqu'ils confient leurs données. L'usurpation d'identité place les victimes dans des situations très délicates et rétablir la situation peut s'avérer extrêmement compliqué. C'est ce qu'illustre le cas d'un auditeur de RTL, fiché à la Banque de France à son insu. L'usurpation sert également à la création de garages fantômes par des faussaires qui achètent et immatriculent des véhicules sous une identité volée en ligne, servant ensuite à la commission d'infractions. LCI a recueilli le témoignage d'une victime qui vit un cauchemar depuis plus de quatre ans. Le 23 juin, Courrier Picard relatait le cas d'un étudiant en STAPS ayant reçu plusieurs amendes d'un total de 2 750€ pour infractions au code de la route alors qu'il ne possède pas de véhicule personnel.

Attention également aux usurpations d'identité des organismes publics ou privés. L'attaque informatique qu'a connu le Grand Besançon en septembre 2020 permet aujourd'hui d'envoyer des courriels crédibles contenant des pièces jointes vérolées sous l'identité de la Ville de Besançon et Grand Besançon Métropole, informe L'Est Républicain. En Martinique, une campagne de phishing prenait l'identité de l'ARS locale pour récupérer frauduleusement les données personnelles des victimes, selon Radio Caraïbes International.

Données personnelles exposées

L'attaque perpétrée fin avril sur Veja, la marque de baskets écolos, a permis aux assaillants de mettre la main sur les adresses mails des clients et des inscrits à la newsletter de l'entreprise, indique L'Usigne Digitale. Les données bancaires et mots de passe ont par chance été épargnés.

Le 9 mars, VPNmentor découvrait l'exposition de près de 8% des salariés de Decathlon sur le plan mondial. Elle concerne les noms, prénoms, adresses email, villes de résidence de 7 883 employés et trouve son origine dans une mauvaise configuration du service AWS S3. Le Monde Informatique

Le 19 mai, La Gazette des Communes évoquait la diffusion des données personnelles de plusieurs agents de la commune d'Annecy qui avait fait l'objet d'une cyberattaque 6 mois plus tôt.

Le 12 juin, 120 000 demandeurs d'emploi français ont vu leur données personnelles (nom, âge, numéro de téléphone…) être publiées par un hacker, suite à une fuite chez Pôle Emploi, mentionne Le Figaro. L'organisme a lancé une enquête tandis que la CNIL a attesté qu'une « *notification de violation de données était en cours d'instruction* », informe L'Express. Le hacker a depuis retiré les données qu'il avait publiées.

La menace des phishings

Entre les données scrapées sur les réseaux sociaux, celles qui fuitent après une cyberattaque ou encore celles que vous transmettez directement via des formulaires frauduleux à l'apparence légitime, les moyens d'obtenir une adresse pour vous contacter et vous faire cliquer sur un lien malveillant, grâce à une communication finement rodée, ne manquent pas. Une étude mentionnée par Libre Eco indique que l'hameçonnage a dérobé 34 millions d'euros aux Belges en 2020 alors que 75% des virements frauduleux ont été détectés par les banques et inversés à temps.

Les ransomwares encouragés par les assurances ?

La facilité qu'ont les victimes à payer les rançons demandées par les pirates encouragent ces activités malveillantes et les ransomwares prolifèrent. Les assureurs préfèrent bien souvent démarcher un négociateur et payer la rançon que de dédommager une perte d'exploitation prolongée et autres dommages prévus dans la police d'assurance qui leur coûteraient plus cher. Si cette garantie n'est pour l'instant pas interdite, le parquet de Paris et le directeur de l'ANSSI ont pointé du doigt cette pratique lors d'une audition au Sénat en avril. L'assureur AXA France a pris les devants début mai en suspendant sa garantie « cyber rançonnage ». BFM TV

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

Le cyberespace exploité par les États-nations

L'Usine Digitale fait état d'une étude menée par le criminologue Mike McGuire relevant une explosion des attaques menées par les États. Ces derniers investissent toujours plus « *de temps et de ressources à l'obtention d'avantages stratégiques cyber pour promouvoir leurs intérêts nationaux, leurs capacités de collecte de renseignements, et leur puissance militaire par l'espionnage et le vol* ». Les incidents cyber liés à un État ont doublé en trois ans, d'après cette étude.

Alors que le 19 mars, les renseignements Finlandais accusaient le gouvernement Chinois d'être impliqué dans une cyberattaque subie par son Parlement en décembre (Le Figaro), la course aux renseignements complique la conclusion d'un traité à portée internationale en matière cyber.

Un gestionnaire de mots de passe compromis

Le 26 avril, Les Numériques publiait un article indiquant que le système de mise à jour du gestionnaire de mots de passe Passwordstate avait été corrompu. L'attaque, qui a duré deux jours, aurait extrait les données de 29 000 clients vers un serveur détenu par les cybercriminels. Le site rappelle que **« lorsque la sécurité du gestionnaire de mots de passe est elle-même défaillante, c'est tout le château de cartes qui peut s'effondrer »** et préconise d'activer l'authentification à deux facteurs. Les gestionnaires de mots de passe constituent une proie de choix pour les cybercriminels du fait de leur contenu.

Objets connectés

Phonandroid relatait le 14 avril la découverte de 9 failles de sécurité qui concernent plus de cent millions d'objets connectés à travers le monde. Si les menaces pèsent sur les particuliers qui utilisent ces objets, cette découverte met en lumière la vulnérabilité des objets connectés de manière générale et les risques qui pèsent sur les organismes utilisant ces objets, comme les hôpitaux ou les industries.

Il est donc primordial d'être attentif à l'utilisation des objets connectés par vos salariés (*nous préparons un sujet sur la charte informatique pour septembre !*)

Achat/vente d'un appareil d'occasion

Le 20 avril, ZDNet faisait le point sur les bonnes pratiques en cas de vente ou d'achat d'un appareil de seconde main. Pour le vendeur : réinitialiser l'appareil et s'assurer que toutes les données soient bien effacées (photos, contacts, mots de passe, wifi, message…). Côté acheteur, il conviendra de s'assurer d'acheter un modèle toujours visé par le déploiement des mises à jour du fabricant. Il est conseillé de réinitialiser également l'appareil avant toute utilisation.

Les bonnes pratiques de la CNIL

La CNIL propose tout un panel de tutos pour utiliser les différents outils numériques en préservant les données personnelles. De la configuration de votre téléphone et ordinateur aux réflexes à adopter lorsque vous naviguez sur Internet, en passant par l'utilisation des réseaux sociaux ; la CNIL vous rend incollable quant aux différents moyens de protéger vos données.

Voitures et données personnelles

PressePortal rappelle que les voitures d'aujourd'hui contiennent beaucoup de données personnelles, allant des trajets enregistrés comme l'adresse du domicile au carnet d'adresses présent dans le smartphone, mais également les services musicaux qui nécessitent un code d'accès. Si des processus de suppression des données sont souvent mis en place lorsque le véhicule repasse par un garage, il est conseillé aux propriétaires d'effectuer eux-mêmes ces démarches avant de vendre leur voiture, surtout si l'acheteur est un particulier.

Audacity à l'écoute des données

Depuis son rachat par un groupe russe, le logiciel de montage audio Audacity récolte un certain nombre de données personnelles telles que l'adresse IP, le système d'exploitation et le processeur utilisé… D'autres encore sont collectées « *nécessaires à l'application de la loi, aux litiges et aux demandes des autorités* » sans plus de précision, avec un hébergement des données au sein de l'espace économique européen mais susceptible de transfert outre-Atlantique, indiquait Les Numériques le 5 juillet.

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 **07 55 58 02 80** stephanie.broggini@dpo-consulting.com

L'opposition des agriculteurs à la publication de leurs données

Une loi de 2015 impose aux greffiers des tribunaux de commerce de transmettre une copie des actes à l'INPI (Institut National de la Propriété Intellectuelle). Le problème étant que l'institut accorde des licences gratuites. En résulte la mise en ligne de données parfois très personnelles d'agriculteurs comme sur le site entreprise du Figaro, révèle France3. Une situation décriée par les agriculteurs et Pierre Venteau, député (LREM) de la Haute-Vienne.

Protection des données face au droit à l'information

Dans un jugement du 30 juin, le tribunal judiciaire de Paris a débouté un demandeur qui souhaitait la suppression ou l'anonymisation d'un article faisant état d'une condamnation pénale datant de plus de 10 ans en vertu du droit à l'oubli. Il a ainsi mis en lumière la primauté du droit fondamental à l'information. Legalis

Les sanctions RGPD au 1er trimestre 2021

Le 29 avril, Nextinpact faisait le point sur les sanctions RGPD prononcées au cours du premier trimestre de l'année. Le montant total européen s'élève à environ 34 millions d'euros d'amende. L'Autorité espagnole se place en tête du classement avec 15,7 millions d'euros pour 34 sanctions prononcées. L'Allemagne arrive deuxième avec 10,7 millions d'euros. Les deux pays représentent à eux deux près de 80% du montant total.

La CNIL surveille les cookies

Depuis le 1er avril, les règles en matière de cookies sont renforcées et IT Social indique que la CNIL va intensifier ses contrôles et alourdir les amendes en cas de manquement relevé. Elle a déjà adressé une vingtaine de mises en demeure à de grandes entreprises de l'économie numérique le 18 mai. Il leur était reproché de ne pas rendre aussi facile la possibilité de refuser les cookies que celle de les accepter. Au 29 juin, les sites concernés s'étaient tous mis en conformité. CNIL

Pour faire le point, un service gratuit nommé Inspecteur RGPD permet de tester les sites des entreprises pour évaluer leur conformité. Widoobiz

Côté particuliers, les Français ne sont toujours pas très éclairés en ce qui concernent les cookies : seulement 1 français sur 4 sait très concrètement ce qu'est un cookie. Concernant les nouvelles règles, seuls 46% en ont eu connaissance. En pratique, ils sont 85% à en constater les effets dans leur navigation quotidienne. CBnews

Manquements au RGPD : 500 000€ d'amende

Dans sa délibération du 14 juin 2021, la CNIL a sanctionné la société BRICO PRIVÉ pour le dépôt de cookies à des fins publicitaires sans le consentement des visiteurs et pour avoir réalisé des communications de prospection sans recueillir le consentement des personnes prospectées. Divers manquements au RGPD ont également fondé cette sanction de 500 000€, notamment l'irrespect des durées de conservation, le défaut d'information des personnes sur le site internet, la méconnaissance du respect du droit à l'effacement ainsi qu'un manquement à l'obligation de sécuriser les données par des moyens d'authentification jugées trop souples.

Google face à Schrems

Maximilien Schrems, l'autrichien à l'origine de l'invalidation du Privacy Shield l'été dernier, s'attaque aujourd'hui à Google devant la CNIL. Il reproche au géant du net de faire fi du consentement des utilisateurs du système Android. **Chaque smartphone concerné possède un AAID (Android Advertising Identifier), un identifiant unique qui collecte les préférences des utilisateurs pour afficher des publicités ciblées, actif par défaut sans en informer l'utilisateur.** L'Informaticien

Cette action intervient dans un contexte où Google prévoit pourtant de répondre aux attentes des utilisateurs Android en facilitant le contrôle qu'ils détiennent sur leurs données personnelles. Europe1
De son côté, l'association NOYB présidée par l'autrichien a mis au point un logiciel qui relève les manquements des sites internet à la règlementation relative aux cookies. 500 mises en demeure ont déjà été adressées. Siècle Digital

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

L'Allemagne s'oppose aux nouvelles CGU de Whatsapp

L'Autorité de régulation allemande a interdit pendant trois mois à Facebook de traiter les données venant de Whatsapp, comme prévu dans ses nouvelles conditions générales d'utilisation. En cause, un consentement loin d'être libre et éclairé comme l'impose le RGPD car l'utilisation de Whatsapp sera bientôt subordonnée au consentement de ces nouvelles stipulations rédigées de manière indigeste. Le CEPD sera appelé à se prononcer, rapporte Capital dans un article du 11 mai. L'Argentine, l'Inde, le Brésil et les États-Unis ont également pris des mesures pour s'opposer à ce partage de données, indique BFM TV. Le 1er juin, ZDNet annonçait le changement de direction de Whatsapp : l'utilisation de l'application sera sans restriction même si l'utilisateur refuse les nouvelles CGU.

Amazon au cœur de polémiques

Mi-avril, Numerama relatait les distorsions existantes entre Amazon et l'un de ses partenaires, le fabricant d'appareils domotiques connectés à l'assistant vocal d'Amazon, Ecobee. Pour protéger la vie privée de ses clients, ce dernier refuse de remonter des informations au géant du commerce en ligne lorsque son assistant vocal n'est pas invoqué. En réaction, Amazon menacerait l'entreprise de rompre le partenariat et de ne plus vendre ses produits sur son site.

Applications et partage de données

À la suite de l'introduction des étiquettes de confidentialité sur l'App Store, qui oblige les éditeurs à mentionner les données collectées par leur application et l'usage qui en est fait, Statista a publié un graphique le 24 mars, affichant les applis qui partagent le plus nos données personnelles avec des tiers. Instagram arrive largement en tête, suivi de Facebook. LinkedIn et Uber Eats se disputent la troisième place.

Dans un article du 18 juin, Siècle Digital alertait sur les applications de santé. D'après une étude, 88% d'entre elles collectent massivement les données personnelles (sensibles) et reposent sur un modèle économique de partage de ces données. Alors que 28% de ces apps n'ont pas mis à disposition de Google Play leur politique de confidentialité, l'étude constate que moins de la moitié (47%) des transmissions de données des utilisateurs étaient conformes à leur politique de confidentialité.

IQVIA et données de santé

Suite à l'émission du 21 mai de Cash Investigation, huit associations et organisations ont transmis un signalement à la CNIL. La nationalité américaine de la société IQVIA inquiète et les organisations souhaitent également améliorer l'effectivité des droits des personnes concernées, notamment le droit d'information et d'opposition. L'Usine Digitale

Pour rappel, IQVIA a été autorisée en 2018 par la CNIL à traiter les données de santé des patients visitant les pharmacies partenaires (14 000 officines concernées) à des fins de recherches scientifiques et répond donc à un motif d'intérêt public. La CNIL a d'ores et déjà annoncé qu'elle allait procéder à des contrôles. Le Monde Informatique

Point sur la troisième phase du déconfinement

Place au passe sanitaire et au QR code, dispositifs de gestion de sortie de crise sanitaire, depuis le 9 juin. Pour se rendre à l'intérieur des bars, restaurants et salles de sport, il faudra se soumettre au scan du QR code par le dispositif de TousAntiCovid, ou se faire inscrire sur les cahiers de rappel de ces établissements.

Le 8 juin, LCI éclairait sur les modalités de traitement des données personnelles par le dispositif numérique. « *Vous ne serez ni tracé, ni identifié, mais seulement informé* » indiquait le Gouvernement, et ce grâce à un code correspondant à un identifiant chiffré, qui fait fi également de l'identité de l'établissement fréquenté. Le serveur central de l'application se charge de transmettre anonymement les QR codes scannés avec horodatage des endroits à risque, à charge pour les appareils disposant de l'application de faire la concordance avec les QR codes scannés par leurs utilisateurs.

Concernant le passe sanitaire nécessaire pour se rendre dans les endroits clos accueillant plus de 1 000 personnes ou pour faciliter le passage aux frontières, son contrôle ne révèlera que votre nom, prénom, date de naissance, ainsi que le fait que vous soyez immunisé après avoir contracté la maladie, que vous

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

soyez vacciné ou que vous avez un test PCR daté de moins de 48h. Les données de santé ne seront connues que des autorités sanitaires. À noter que la CNIL a émis, le 7 juin, quelques observations sur le dispositif tandis que le Conseil d'État refusait le 6 juillet de suspendre le dispositif, comme le demandait la Quadrature du Net. BFMTV

Données rendues publiques et contrôles fiscaux

Le 11 mai, legiFiscal indiquait que la loi de finances pour 2021, dans la prolongation de celle de 2020, autorise les administrations fiscales et douanières à collecter et exploiter les données rendues publiques par les utilisateurs sur les réseaux sociaux et autres plateformes en ligne afin de détecter les comportements frauduleux.

GendNotes, l'application critiquée de la gendarmerie

L'application GendNotes permettant aux forces de l'ordre de prendre des notes directement sur téléphone ou tablette, au cours de leurs enquêtes, a fait l'objet de nombreuses controverses. Le 13 avril, le Conseil d'État s'est prononcé sur la légalité de ce décret. Si l'application prévoit une zone de commentaire libre où peuvent être enregistrées des données personnelles sensibles telles que « *la prétendue origine raciale ou ethnique, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale, à la santé ou à la vie sexuelle ou l'orientation sexuelle* », c'est l'article relatif aux transferts de ces données vers d'autres fichiers qui a été censuré pour transgression à la loi informatique et libertés. ZDNet

Adresses IP et droit d'auteur

Dans un arrêt du 17 juin, la Cour de Justice de l'UE est venue indiquer que **l'upload de segments de fichier média protégé par le droit d'auteur dans un réseau peer-to-peer, constitue une communication au public** au sens de la directive européenne de 2001 portant sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. En outre, le traitement consistant pour le titulaire de droits de propriété ou un tiers agissant pour son compte d'enregistrer les adresses IP utilisées pour l'upload d'œuvre protégée ne contrevient pas au droit de l'UE, ni même le fait, pour un FAI, de communiquer les noms et adresses postales correspondantes permettant au titulaire des droits d'agir en indemnisation. Pour autant, il faut que les lois étatiques le permettent et que cela soit justifié, proportionné et non abusif. Dalloz Actualité

Nomination d'un fonctionnaire et données personnelles

La mise en ligne d'un arrêté portant sur la titularisation d'un fonctionnaire constitue un traitement de données personnelles au sens du RGPD, a indiqué le Conseil d'État dans un arrêt du 10 juin 2021. L'arrêté indique dans ses visas le décret appliqué lors du recrutement du fonctionnaire, à savoir celui relatif au recrutement des travailleurs handicapés dans la fonction publique. Le Conseil d'État considère qu'il ne révèle directement ni la nature, ni la gravité du handicap de la personne concernée, et donc ne saurait être considéré comme traitant des données de santé même s'il révèle indirectement que les personnes recrutées souffrent d'un handicap. Cependant, à l'issue du délai de recours contre cette nomination, les données traitées en ligne doivent être limitées à ce qui est nécessaire au regard de la finalité, si bien que le fondement de la titularisation révélant indirectement la situation de handicap du requérant doit être retiré.

eCommerce et conservation des données bancaires

Suite à la pandémie et l'augmentation du commerce en ligne qui a suivi, le CEPD a adopté le 19 mai 2021 des recommandations concernant les bases légales permettant la conservation des données bancaires pour faciliter de futures transactions en ligne. L'article 6 du RGPD énonce les bases légales possibles pour traiter les données. Parmi elles, seules le recueil du consentement et l'intérêt légitime du responsable de traitement sont admis par le CEPD pour justifier de cette conservation, avec une défiance affichée concernant l'intérêt légitime. Au vu de la nature hautement personnelle de ces données et des risques encourus, l'intérêt légitime devra être habilement et solidement justifié. Recueillir le consentement du client reste la solution la plus simple et la plus sûre. Dalloz Actualité

Clouds américains face à l'invalidation du Privacy Shield

La fin des transferts des données personnelles européennes outre-Atlantique oblige notamment les clouds américains, leaders sur le marché, à adopter des mesures pour conserver leurs clients européens. Alors que des représentants des entreprises du numérique françaises appellent à l'adoption d'un nouvel accord entre l'Europe et les Etats Unis pour encadrer les transferts inéluctables de données (L'Usine Digitale), Microsoft a entrepris un chantier pour garantir le stockage et le traitement des données personnelles des européens sur le territoire du vieux continent. Numerama

Contester les demandes gouvernementales d'accès aux données personnelles des clients fondées sur le Cloud Act : c'est la promesse faite par Microsoft ainsi qu'Amazon et son cloud AWS, qui a décidé de renforcer ses clauses contractuelles. L'Usine Digitale

Si l'idée paraît séduisante, elle est loin d'être suffisante pour garantir la protection de nos données face au gouvernement américain et à la portée extraterritoriale des lois états-uniennes.

Un code de conduite adopté pour les services cloud

Le premier code de conduite (prévu à l'article 40 du RGPD) visant les services de cloud computing a été approuvé par le CEPD le 20 mai. Initié par CISPE (Cloud Infrastructure Services Providers in Europe), ce code permet aux clients IaaS d'être assuré de la conformité RGPD de leur fournisseur de cloud. Nextinpact

Dans un communiqué de la CNIL du 11 juin, elle informait de son approbation concernant ce premier code de conduite européen. Son effectivité prendra effet lorsque les organismes contrôlant la bonne application du code identifiés par CISPE auront été agréées par la CNIL.

Deux nouvelles clauses contractuelles types

Après l'invalidation du Privacy Shield, les clauses contractuelles types adoptées par la Commission européenne demeuraient un instrument valide permettant le transfert des données vers des pays tiers à conditions d'être accompagnées de mesures supplémentaires concernant les transferts outre-Atlantique. Le 4 juin, la Commission publiait deux nouveaux ensembles de clauses contractuelles types visant à encadrer ces transferts avec de nouvelles garanties en laissant 18 mois aux organisations utilisant les anciennes clauses contractuelles types pour se conformer aux nouvelles. L'Usine Digitale

Les transferts de données vers le Royaume Uni échappent à ces formalités malgré le Brexit. La Commission européenne a adopté le 28 juin deux décisions d'adéquation valables quatre ans reconnaissant un niveau de protection des données personnelles équivalent aux règles européennes facilitant les transferts de données personnelles. L'Usine Digitale

DPO Consulting
Your personal data protection officer
Bourgogne-Franche-Comté

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 **07 55 58 02 80** stephanie.broggini@dpo-consulting.com