REVUE DE PRESSE MAI 2020

Revue de presse de l'actualité Cyber et RGPD des mois d'avril et mai 2020

DPO Consulting
Your personal data protection officer
Bourgogne Franche-Comté

Les Cyberattaques continuent

L'actualité a été rythmée une nouvelle fois par les nombreuses cyberattaques touchant à la fois de nombreuses organisations publiques et privées en France.

En février dernier, l'entreprise Bouygues Construction avait été frappée par un logiciel malveillant. Ce fut au tour de l'entreprise régionale Roger Martin d'être visée par un rançonlogiciel comme le revèle Le Parisien dans son édition du 7 mai.

Le secteur de l'agro-alimentaire a été également touché avec la coopérative bretonne Cooperl basée dans les Côtes d'Armor comme le souligne l'hebdomadaire du groupe Ouest France.

Du côté des administrations publiques, l'AFPA, la métropole de Toulouse, les villes de Marseille et de Martigues ainsi que la métropole Aix-Marseille-Provence ont été la cible d'attaques. Une attaque que l'Agence Nationale de la Sécurité des Systèmes d'Information décrit dans Le Monde Informatique.

Toujours selon Le Monde Informatique, plusieurs semaines après l'attaque, les systèmes d'information de la ville de Marseille ne pouvaient pas fournir les données relatives aux décès liés à la crise du Covid.

Plus à l'Est de la France, ce sont les boîtes mails de Charleville-Mézières et Ardenne Métropole qui ont été également paralysées par une cyberattaque comme le rapporte Capital.

De nombreux médias ont relayé l'attaque de grande ampleur dont a été victime la compagnie aérienne britannique EasyJet. Ce sont les données personnelles de plus de 9 millions de clients qui ont été dérobés par les cyberattaquants. Parmi les 2 208 personnes ayant été victimes de vols de leurs données bancaires, plus de 300 français seraient concernés.

Des bases de données non sécurisées

Du côté du Figaro, la société de sécurité informatique Safety Detective mettait à jour une importante base de données laissée sans protection comme le révèle Le Monde.

La société Britannique Virgin Media a été également concernée par une fuite de données personnelles suite à la mauvaise configuration d'une base de données sur laquelle figuraient des données personnelles de 900 000 personnes.

La Crise du Covid, prétexte à de nombreuses attaques

Dans Le Figaro du 30 mars 2020, la société Thalès a pu souligner le lien entre la crise du Covid et les menaces Cyber. D'une manière générale, *« il semble que l'écosystème de la menace cyber suive la propagation géographique du Covid-19 avec des attaques d'abord en Asie, puis en Europe de l'Est et maintenant en Europe de l'Ouest. Le territoire français présente donc un risque d'attaques accru ».*

Le site Cubic fait état de 18 millions de mails de phishing ou contenant des malwares par jour. « *Des campagnes de mails frauduleux exploitent la peur et la confusion liées à la pandémie pour piéger les internautes ».*

Les chiffres des noms de domaines liés au Covid sont vertigineux. La société américaine de cybersécurité Domain Tools a ainsi recensé plus de 100 000 adresses déposées entre janvier et début mai avec les termes "coronavirus", "covid-19", "covid", ou encore "SarsCov2"

Le site CNET France révèle dans son article du 7 mai 2020 que *« les URL autour du coronavirus, achetées pour quelques euros aux débuts de la pandémie, sont remises en vente entre 5 000 et 10 000 euros, en moyenne ».*

Éric **CUENOT** / Président & Data Privacy Officer / Certificat Sciences Po Paris / Franchisé Bourgogne Franche-Comté
Espace Besançon - 25115 POUILLEY-LES-VIGNES **06 65 91 28 76** eric.cuenot@dpo-consulting.com

Détournement d'aides publiques

Le Covid a été également à l'origine d'arnaques de grandes ampleurs comme en Allemagne où des dizaines de millions d'euros ont été détournés comme le décrit l'Usine Digitale du 21 avril 2020 : *« Concrètement, les individus malveillants ont d'abord réalisé une copie du site officiel servant à formuler les demandes d'indemnisation. Ils ont ensuite procédé à l'envoi massif de mails trompeurs aux publics concernés par l'aide gouvernementale. Les hackers ont alors pu collecter les données de ces sociétés et travailleurs indépendants, bernés par le réalisme du faux site web. Ils ont ensuite réclamé sur le site web officiel l'aide financière au nom de ces personnes morales, tout en demandant un virement vers leur propre compte bancaire. Cette arnaque a duré près de trois semaines, jusqu'au jeudi 9 avril 2020, avant d'être repérée par les autorités locales. Ces dernières ont alors suspendu tous les versements le temps que la copie du site officiel soit mise hors ligne. Dans ce laps de temps, la police a indiqué avoir comptabilisé 576 plaintes pour escroquerie. Le montant des aides subtilisées à chaque victime de l'arnaque étant compris entre 9 000 et 25 000 euros, le détournement pourrait coûter au gouvernement une somme comprise entre 31 et 100 millions d'euros ».*

Bilan du Commandant de la cyberdéfense

Le 6 mars dernier, le Commandant de la cyberdéfense, le général de division aérienne Didier Tisseyre a été reçu par la Commission de la défense nationale et des forces armées de l'Assemblée nationale. Un compte-rendu de cette audition dont on peut retrouver des passages sur le site opex360 avec les prochains enjeux du cyberespace *« Je vous assure que, dans le cyberespace, [...] nous ne sommes pas dans un temps de paix : il y a de nombreuses crises, et, d'une certaine manière, la guerre cyber a déjà commencé. Certains déploient leurs outils et se prépositionnent pour pouvoir le jour J, au moment où ils appuieront sur la touche «Enter», déclencher immédiatement les éléments. Or une fois qu'on est paralysé, il est trop tard pour réagir »*, a souligné le général Tisseyre. Le Commandant affirme que *« la France est aujourd'hui la nation la plus forte dans l'Union Européenne en matière de cyberdéfense ».*

Vidéo

La période de confinement a rimé avec visio. De nombreux outils ont été utilisés par les Français et notamment l'application Zoom décriée dans de nombreux articles pour ses failles de sécurité, ses transferts de données «par accident» à la Chine comme le révèle le Big Data.fr ou encore avec plus de 530 000 données en vente sur le dark Web selon Le Figaro *« qui contiennent non seulement les e-mails et les mots de passe, mais aussi les URL de réunion personnelle et les codes d'administration. Chacun des comptes ne coûte pas plus d'un centime, et certains sont même «offerts» pour favoriser le zoombombing, cette pratique qui consiste à s'introduire dans une conversation privée et à harceler ses membres, en partageant par exemple des contenus pornographiques ».*

Devant la pression médiatique, la société a décidé de racheter *« la société Keybase, dont l'expertise en matière de chiffrement permettra à Zoom de mettre en place le chiffrement de bout en bout ».* Comme le rapporte le site PresseCitron.

Ce large succès de Zoom a eu pour conséquence une recrudescence des noms de domaines en lien avec Zoom comme le précise là encore PresseCitron *« en l'espace de trois semaines, 2 449 noms de domaine en lien avec Zoom ont été enregistrés. Check Point Research aurait déjà identifié 32 de ces noms de domaine comme étant « malicieuses » et 320 comme étant « suspects ». En d'autres termes, lorsque vous recevez un message sur Zoom, Google Meet ou Microsoft Teams, vérifiez bien que ces messages ont été envoyés par ces entreprises, et non par des hackers qui essaient de voler des mots de passe ou des données sur votre compte bancaire ».*

Derrière les solutions détenues par les GAFAM, le logiciel de visioconférence libre Jitsi Meet est mis en avant par les journalistes du Monde. comme une alternative.

Vidéo : la mise en garde du site Cybermalveillance.gouv

Le site gouvernemental qui avait fait peau neuve en février dernier a publié un long **communiqué** en avril dernier sur la recrudescence des chantages à la vidéo suite à des prétendues images prises à votre insu via votre webcam.

Un nouveau label gouvernemental

Cybermalveillance.gouv.fr lance un label ExpertCyber ouvert *« aux entreprises de service informatique de toute taille, justifiant d'une expertise en sécurité numérique, adressant une cible professionnelle et assurant des prestations d'installation, de maintenance et d'assistance ».*

Amende record Facebook

La sanction est tombée. Un juge américain a confirmé le 23 avril dernier l'amende de 5 milliards de dollars infligée par l'agence américaine de protection des consommateurs (la FTC) à Facebook en 2019. Cette amende fait suite aux nombreux scandales sur l'utilisation des données personnelles de ses utilisateurs par Facebook. Comme le rapporte le site Stratégie, *"c'est une décision « historique », a estimé vendredi 24 avril le président de cette agence, Joe Simons, en soulignant que la FTC n'avait jamais infligé une amende aussi importante."*

Le conseil d'État contre l'utilisation des drônes.

La Préfecture de Police avait eu recours à l'utilisation de drônes pour surveiller le respect des consignes du confinement. Suite à une première plainte de l'association « La Quadrature du net » et de la Ligue des Droits de l'Homme devant le Tribunal de Paris, l'association a décidé de faire un appel auprès du Conseil d'État le 2 mai dernier.

Le 18 mai dernier, le juge des référés du Conseil d'État est venu infirmer la décision rendue par le Tribunal Administratif de Paris en ordonnant à *« l'État de cesser, sans délai, de procéder aux mesures de surveillance par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement »*

Le juge des référés précisant *« qu'il résulte de l'instruction que les appareils en cause qui sont dotés d'un zoom optique et qui peuvent voler à une distance inférieure à celle fixée par la note du 14 mai 2020 sont susceptibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire, au bénéfice d'un autre usage que celui actuellement pratiqué, à rendre les personnes auxquelles elles se rapportent identifiables. Dans ces conditions, les données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel ».*

La CNIL se prononcera prochainement sur ces pratiques observées dans d'autres villes en France.

Fronde contre la surveillance en ligne des examens

France Inter détaille les raisons qui ont poussé les étudiants d'HEC de protester contre l'utilisation de logiciels de surveillance en ligne dans le cadre leur examen à distance.
Dans une lettre ouverte, ils dénoncent à la fois des problèmes d'égalité des chances et de respect de la vie privée.
La CNIL a rappelé le 20 mai dernier que *« la mise en œuvre d'un système de surveillance d'examens organisés à distance constitue un traitement de données personnelles, quelle que soit la technologie utilisée : vidéo continue ou prise de photographies aléatoires, télésurveillance en temps réel ou à postériori, avec ou sans recours à des algorithmes de détection de la fraude, utilisation d'un outil permettant à un superviseur de prendre la main à distance sur l'ordinateur de l'étudiant afin de surveiller l'activité de celui-ci pendant la réalisation de l'examen, notamment en vérifiant l'accès aux boîtes mails et réseaux sociaux, etc. Les établissements doivent respecter le RGPD et la loi Informatique et Libertés ».*

La CNIL lève la mise en demeure à l'encontre de la société AERO

Initiée en novembre 2019, la procédure de mise en demeure de la société Aero a été levée en 6 avril 2020. On peut lire sur le site Legifrance.gouv les explications de la Présidente de la CNIL *« Au regard des éléments de réponse apportés pour satisfaire au second palier de la mise en demeure et des mesures prises quant à la tenue d'un registre des activités de traitement, à l'information des salariés relative au dispositif de vidéosurveillance et à la conclusion d'un contrat avec vos sous-traitants, je vous informe que j'ai décidé de procéder à la clôture de votre dossier ».*

Les axes de contrôle de la CNIL pour 2020

C'est quelques jours avant le début du confinement, que la CNIL avait dévoilé ses 3 thématiques de contrôles pour 2020 : la sécurité des données de santé, mobilités et services de proximité, les nouveaux usages des données de géolocalisation, le respect des dispositions applicables aux cookies et autres traceurs. La CNIL indiquait *« qu'elle laissera un délai de 6 mois aux organismes, à compter de la publication de cette recommandation, pour se mettre en conformité sur les obligations nouvelles résultant du RGPD. Les contrôles, sur ces obligations nouvelles, démarreront ainsi à l'automne 2020 et se poursuivront en 2021 ».*

Application Stop Covid

L'application **Stop Covid** qui sera lancée le 2 juin prochain a suscité beaucoup d'interrogations sur le plan du respect de la vie privée et des libertés individuelles et de la sécurisation des données collectées. Le club des Juristes s'est penché sur cette initiative au regard de l'avis rendu par la CNIL sur cette application et dans le contexte du Règlement Général sur la Protection des Données. 472 spécialistes en cryptologie et sécurité informatique et universitaires ont publié une lettre « Mise en garde contre les applications de traçage » sur le site **attention-stopcovid.fr.** et soulignent que *« Toutes ces applications induisent en fait des risques très importants quant au respect de la vie privée et des libertés individuelles. L'un d'entre eux est la surveillance de masse par des acteurs privés ou publics, contre laquelle l'Association Internationale de Recherche en Cryptologie (IACR) s'est engagée à travers la résolution de Copenhague ».*

L'article paru dans sur le site de France Info met en perspective cette application Stop Covid avec la initiatives prises dans d'autres pays comme à Singapour, Taiwan, la Corée du Sud et bien sûr en Chine.

Données de santé

Le Covid a placé la collecte de données de santé au coeur de la pandémie. Le Comité Européen de la Protection des Données (CEPD) a rendu une déclaration très attendue le 20 mars dernier détaillée sur le site Dalloz tant pour les organisations publiques que les employeurs.

La CNIL a précisé le 7 mai dernier les obligations tant du côté employeurs que salariés lors du passage au déconfinement avec des précisions sur les relevés de température *« En l'état du droit, et sauf à ce qu'un texte en prévoit expressément la possibilité, il est interdit aux employeurs de constituer des fichiers conservant des données de températures de leurs salariés. Il leur est de même interdit de mettre en place des outils de captation automatique de température (telles que des caméras thermiques). Les prises manuelles de température à l'entrée d'un site et sans constitution d'un fichier ni remontée d'information ne sont en revanche pas soumises à la réglementation sur la protection des données personnelles. La CNIL renvoie sur ce point aux recommandations de la direction générale du travail ».*

Télétravail

Cette crise sanitaire a rimé avec télétravail pour des millions de français. Là encore, les hackers ont profité de cette nouvelle organisation qu'il a fallu mettre sur pied en quelques heures ou quelques jours dans les organisations pour tenter de frapper au cœur des systèmes d'informations.

Didier Schreiber, directeur marketing chez Zscaler, un des leaders mondiaux de la surveillance et de protection des données affirme sur France Inter le 5 mai dernier que *« depuis janvier 2020, avec la crise du coronavirus, on a constaté une augmentation de plus de 30 000 % des attaques informatiques de type hameçonnage (fishing en anglais), des logiciels malveillants (malwares), des sites malicieux qui ciblent des utilisateurs à distance. En janvier, on avait constaté 1 200 attaques informatiques liées au Covid 19… et on en était à 380 000 cyberattaques début avril ! ».*

De nombreux experts en sécurité pointent du doigt, le retour des données sur le lieu de travail comme le précise Alain Bouillé sur France Info, délégué général du Cesin et RSSI du Groupe Caisse des Dépôts. *« Parfois, dans l'urgence et la précipitation, corollaires inamicaux de la nécessité, certaines entreprises n'ont pas hésité à demander à leurs salariés de travailler depuis la maison avec leur ordinateur personnel : c'est ce que l'on appelle le BYOD (Bring Your Own Device : "Apporte ton propre appareil"). "Procéder ainsi sans prétentions d'un point de vue sécurité, c'est une catastrophe", "Comment faire pour récupérer en toute sécurité deux mois de données stockées sur des ordinateurs personnels ?, C'est inenvisageable. Vous n'avez aucun contrôle sur les postes de travail : quelques uns de mes confrères s'arrachent en ce moment les cheveux pour tenter de récupérer cette situation…»*

Dans ce contexte de circonstances exceptionnelles, l'organisation du télétravail, posé dans l'article 1222-11 du Code du Travail, a pu se faire dans de nombreuses entreprises avec l'usage d'équipements informatiques personnels ou non.

On retiendra 3 formes de nomadisme avec chacune leurs avantages et inconvénients :

- **Le BYOD :** "Bring Your Own Device - Apportez Votre Equipement personnel de Communication". C'est l'usage d'équipements informatiques personnels (choisis et achetés par le salarié) dans un contexte professionnel
- **Le CYOD :** "Choose Your Own Device". La société propose à ses collaborateurs de choisir le matériel qu'ils souhaitent utiliser à des fins personnelles et professionnelles selon une liste établie par l'entreprise (DSI, RSSI). Le collaborateur achète le matériel et en reste ainsi le propriétaire
- **Le COPE :** "Corporate Own, Personnaly Enable". La société fournit à ses collaborateurs le matériel et laisse la possibilité aux salariés d'utiliser ce matériel à des fins personnelles

La Cnil a ainsi rappelé au cours des dernières semaines :

- les bonnes pratiques permettant de concilier sécurité des données de l'entreprise et protection de la vie privée du salarié connecté
- ses recommandations pour aider à la bonne sécurisation des données personnelles dans le cadre du télétravail

Il conviendra donc à l'entreprise de s'assurer que les conditions de la mise en œuvre du travail à distance respectent les dispositions du RGPD, notamment en matière de sécurité des données car l'accès à distance aux outils et systèmes informatiques de l'entreprise n'est pas sans risque en termes d'atteinte à leur sécurité.

Mais la mise en place du télétravail repose également sur un **encadrement juridique spécifique,** posé dans l'article 1222-9 du code du travail, qui doit reposer sur un des trois moyens juridiques suivants :

- **L'accord collectif :** certaines conventions de branche, accord d'entreprise, d'établissement ou de groupe peuvent prévoir les modalités dans lesquelles le dispositif de télétravail doit être mis en place.
- **La charte informatique élaborée** par l'employeur devra être soumise à l'avis du Comité Social Économique (CSE) s'il existe.
- **Un accord formé par tout moyen entre l'employeur et le salarié** en cas d'absence d'accord collectif ou de charte informatique.

L'opposabilité de la charte informatique aux salariés suppose qu'elle soit annexée au règlement intérieur de l'entreprise et qu'elle respecte la même procédure, notamment :

- la saisine pour avis du Comité Social et économique (CSE) (**article L.1321-4, alinéa 1er du Code du travail**),
- le dépôt au greffe du conseil de prud'hommes du ressort de l'entreprise ou de l'établissement concerné (**article R.1321-2 du Code du travail**),
- la communication à l'inspection du travail, jointe à l'avis du CSE (**article L.1321-4, alinéa 3 du Code du travail**)

Une fois le règlement intérieur dûment validé, il devra être porté à la connaissance des personnes ayant accès aux locaux par tout moyen (**article R.1321-1 du Code du travail**).

Télétravail généralisé ?

Dans un communiqué, Peugeot a été une des premières sociétés du CAC 40 à annoncer le 6 mai dernier sa volonté de faire du travail à distance la *« référence »* pour ses activités hors production (dans le tertiaire, le commercial et la recherche-développement) avec une présence *« d'une journée à une journée et demie par semaine, en moyenne »* pour les salariés. 20 minutes dans un article consacré à ce sujet relate le monde après-Covid qui s'ouvre comme en témoigne Jes Staley, le patron de la banque britannique Barclays… qui estime ainsi que *« mettre 7 000 personnes dans un immeuble pourrait être du passé. Nous trouverons des moyens pour opérer avec davantage de distances pendant longtemps ».*

DPO Consulting
Your personal data protection officer

vous accompagne dans votre projet de **mise en conformité RGPD**

Audit

Nous réalisons une cartographie de vos traitements de données, auditons votre structure ainsi que vos projets et vous fournissons les recommandations à mettre en place pour vous mettre en conformité.

Formation

Clé du maintien de votre mise en conformité et de votre réussite, nous proposons à vos équipes plusieurs niveaux de formation. Les formations conçues par DPO Consulting sont riches de nos expertises métier et terrain.

L'externalisation de la fonction de DPO/DPD

Désignés officiellement auprès de la CNIL, nous réalisons pour vous l'ensemble des missions du DPO (conseil, tenue du registre, point de contact des personnes concernées, gestion documentaire des preuves de votre conformité, mise à disposition de notre outil myDPO ...).

Assistance et support aux DPO

Nos experts accompagnent votre DPO dans l'exercice de ses missions. Nous lui fournissons des conseils personnalisés et adaptés à son cœur d'activité ainsi que les outils dont il aura besoin au quotidien.

La mise à disposition de myDPO

DPO Consulting a mis en place une solution logicielle, myDPO, pour faciliter la mise en œuvre des obligations imposées par le RGPD. Destiné à l'ensemble des secteurs, myDPO est également utilisé par nos consultants afin de gagner en productivité.

Réalisation de vos EIVP

Afin de vous faire gagner du temps, notre équipe d'expert réalise pour vous les études d'impact sur la vie privée.

DPO Consulting
Your personal data protection officer

Éric **CUENOT** / Président & Data Privacy Officer / Certificat Sciences Po Paris / Franchisé Bourgogne Franche-Comté
Espace Besançon - 25115 POUILLEY-LES-VIGNES **06 65 91 28 76** eric.cuenot@dpo-consulting.com