La CNIL face au compte à rebours de la nouvelle loi européenne

La CNIL face au compte à rebours de la nouvelle loi européenne

La Commission nationale de l'informatique et des libertés doit préparer l'application, en mai 2018, du nouveau règlement européen sur les données personnelles. Le temps presse.

De l'aveu de sa présidente, Isabelle Falque-Pierrotin, l'année 2016 a été *« intense »* pour la Commission nationale de l'informatique et des libertés (CNIL). La présidente de l'instance chargée de la protection des données personnelles en a donné la mesure, lundi 27 mars lors de la présentation de son rapport annuel, en égrenant les principaux dossiers qui ont concerné l'institution lors de l'année passée : adoption du nouveau règlement européen sur les données personnelles ; actions lancées contre plusieurs géants du Net ; débat sur le chiffrement ; loi pour la république numérique ; polémique autour du fichier biométrique TES ; début des processus électoraux…
Ce surcroît d'activité ne s'est cependant pas traduit dans le nombre de procédures traitées par la Commission. En 2016, elle a reçu plus de 7 703 plaintes, un peu moins que l'année précédente (7 908), procédé à 430 contrôles (501 en 2015), prononcé 82 mises en demeure (93 en 2015) et infligé 13 sanctions dont 4 financières (10 en 2015).
C'est plutôt du point de vue législatif que l'année 2016 a été chargée, marquée par l'adoption de *« trois textes qui bouleversent la protection des données personnelles »* dans le sens d'*« une plus grande maîtrise de leurs données par les individus »*, a expliqué Mme Falque-Pierrotin.

Le défi du règlement européen

La loi pour une république numérique a été publiée au *Journal officiel* le 7 octobre, et l'accord Privacy Shield est entré en vigueur, après de longues négociations, le 1er août. Mais c'est surtout l'adoption définitive, en mai, du nouveau règlement européen sur les données personnelles qui a constitué, selon Mme Falque-Pierrotin, *« une étape majeure pour la protection des données personnelles en Europe »*. Ce règlement institue notamment des sanctions plus importantes pour les entreprises, de nouveaux droits pour les citoyens et une meilleure coordination des autorités de protection des données. Il nécessite à la fois des adaptations de la part des entreprises, mais aussi un travail législatif au niveau français pour toiletter la loi informatique et libertés de 1978. Le temps presse : le règlement s'appliquera dès le 25 mai 2018.
« 2017, c'est la cote d'alerte », a ainsi prévenu Mme Falque-Pierrotin.
Les entreprises *« doivent se mettre en marche »* pour se conformer au règlement, a-t-elle expliqué, insistant sur le rôle d'accompagnement de la Commission. Consciente de l'effort requis, elle a tenté de rassurer : *« Nous sommes convaincus qu'il n'y a pas d'innovation sans protection des données personnelles »* : *« Il est possible d'innover et que, loin de la contraindre, la protection des données permet de développer l'innovation. »*
Autre obstacle de taille, législatif cette fois : pour être appliqué dès le mois de mai 2018, la nouvelle loi informatique et liberté *« devra être déposée en conseil des ministres avant l'été »*. *« Pour le moins délicat »*, a euphémisé Mme Falque-Pierrotin…[lire la suite]
Téléchargez le rapport annuel 2016

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

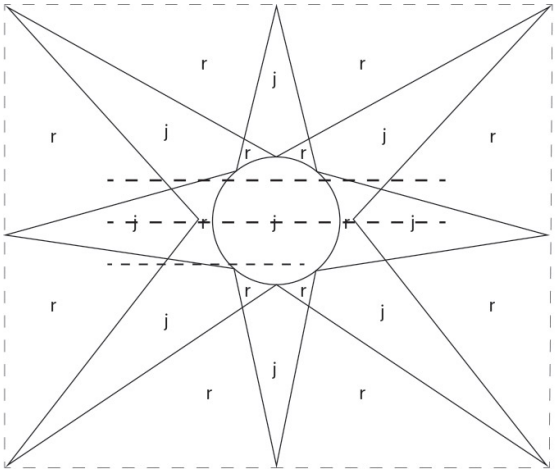
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *En 2017, la CNIL face au compte à rebours de la nouvelle loi européenne*

Cyber-harcèlement mortel avec un gif animé



j :
r :
--- : zone texte
v : vitesse j > r > j > r

Cyber-harcèlement mortel avec un gif animé

Un journaliste américain a été victime d'une très violente crise d'épilepsie en regardant une image animée envoyée, à dessein, par un troll. Le responsable, arrêté, risque dix ans de prison.

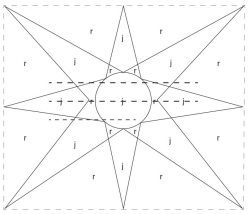
On connaissait le gif comme objet de plaisanterie web, il pourra désormais être aussi considéré comme une arme pouvant tuer. Le tribunal de Dallas s'apprête à juger John Rayne Rivello, utilisateur de Twitter et harceleur présumé du journaliste Kurt Eichenwald. L'arme du – presque – crime : une image animée envoyée à l'attention du reporter, provoquant une crise d'épilepsie qui aurait pu être mortelle.
Comme l'explique le blog Big Browser du *Monde*, le journaliste, collaborateur de *Newsweek* ou *Vanity Fair*, était connu pour ses positions anti-Donald Trump, qu'il relayait également sur Twitter. Il ne cachait pas non plus sa condition épileptique.
Mi-décembre, à la suite d'une discussion animée sur Fox News, où il était interviewé par l'éditorialiste (très) conservateur Tucker Carlson, Eichenwald subit les assauts de plusieurs soutiens à Trump sur son compte Twitter. Une journée malheureusement normale sur les réseaux sociaux, mais qui s'est très mal terminée. L'un des trolls, répondant au nom clairement antisémite de @jew_goldstein, lui envoie un gif stroboscopique, agrémenté du message : *« Tu mérites une crise pour ton message. »*
La femme d'Eichenwald trouvera peu après son mari sur le sol de bureau, le message Twitter clignotant sur son écran, comme le rapporte son avocat au *New York Times*. Après avoir appelé les secours, elle a répondu à l'envoyeur : *« C'est sa femme qui parle. Vous avez causé une attaque. J'ai récupéré vos informations. J'ai appelé la police et leur ai fait part de votre agression. »*
Suivre


Kurt Eichenwald
✔@kurteichenwald
@jew_goldstein This is his wife, you caused a seizure. I have your information and have called the police to report the assault.
05:31 – 16 Dec 2016
•
•
2 6942 694 Retweets
•
4 0594 059 j'aime

La réaction épileptique de Kurt Eichenwald, qui a duré huit minutes selon le *Dallas News*, a été particulièrement violente : incapacité de travailler durant plusieurs jours, perte de la sensation de la main gauche et trouble de l'élocution durant plusieurs semaines. De quoi pousser la police de Dallas et le FBI à mener une enquête sérieuse.

Un iPhone, son Cloud et des preuves

Un mandat de recherche a été émis à l'encontre de @jew_goldstein et a permis de remonter la piste de plusieurs messages privés envoyés par le compte anonyme au sujet de Kurt Eichenwald. Dans ses échanges, l'utilisateur parlait de la condition médicale du journaliste et espérait *« qu'il fasse une crise »* voire *« qu'il meure »*. La police a été capable de relier le compte Twitter à un numéro de téléphone, puis à un modèle de smartphone – un iPhone 6 – qui les a ensuite menés, après avoir cité Apple à comparaître, au Cloud appartenant à un certain John Rayne Rivello.
Dans ses données, les enquêteurs ont trouvé une liste de preuves accablantes : l'image animée qui a provoqué la crise, une capture d'écran du tweet en question et de la réponse de la femme du journaliste, une capture d'écran de la page Wikipédia de Kurt Eichenwald, modifiée avec une fausse date de décès (le jour de l'envoi du tweet), une autre capture d'une liste d'éléments pouvant déclencher une crise d'épilepsie ou encore l'adresse du domicile du journaliste.
Pour l'avocat de Kurt Eichenwald, interrogé par *Newsweek*, l'action de Rivello sur Twitter *« n'est pas différente de celle de quelqu'un qui envoie par courrier une bombe ou des enveloppes remplies d'anthrax »*.
John Rayne Rivello s'apprête à passer devant le tribunal de Dallas avec une accusation tout à fait inédite. Le troll de 29 ans est accusé de cyber-harcèlement avec *« utilisation d'une arme mortelle »*, en l'occurrence l'image animée. Rivello encourt jusqu'à dix ans de prison. Ou quand le gif ne fait plus rire du tout.



Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cyber-harcèlement : quand le gif animé devient une arme mortelle – L'actu Médias / Net – Télérama.fr*

« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les

publicités mensongères

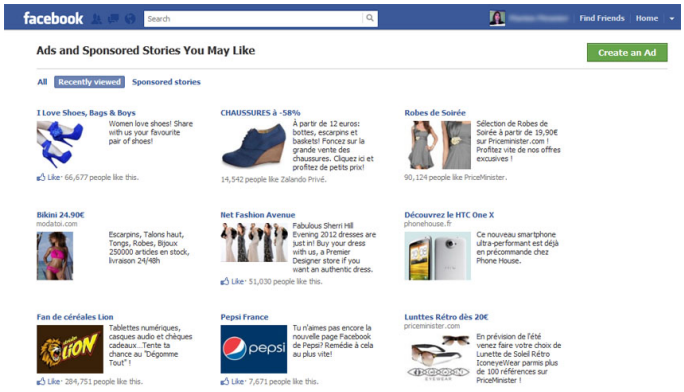
	« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères

Publicités, confidentialité ou encore respect des droits des consommateurs : Bruxelles a souhaité mettre au clair ses demandes auprès des grands réseaux sociaux. Épinglés par l'Union sur différent dossiers, Facebook, Google et Twitter ont désormais un mois pour appliquer les changements exigés.

Ce vendredi, la Commission européenne a finalement mis en demeure les trois principaux réseaux sociaux (Facebook, Twitter et Google+) qui agacent Bruxelles sur de nombreux dossiers.
Avertie notamment par les régulateurs de concurrence des pays de l'UE, la Commission voulait mettre fin à de nombreuses pratiques publicitaires illégales au sein des frontières européennes. Mais Bruxelles ne s'en est pas tenu à une simple auscultation des publicités des réseaux, l'exécutif européen a également tenu à évaluer minutieusement la gestion des données personnelles et la réactivité des réseaux face aux contenus illégaux.

UN MOIS POUR EN FINIR AVEC LES IPHONE À 1€

Désormais, après avoir rencontré ce jeudi les autorités européennes, les entreprises, Facebook, Twitter et Google, disposent d'un mois pour changer leurs pratiques en adéquations avec les exigences légales. Les autorités auraient proposé aux dirigeants certains aménagements pour s'adapter au cadre juridique européen selon Reuters.
Dans le viseur de la Commission, les procédures juridiques entre consommateur européen et société américaine. Pour Věra Jourová, commissaire européenne chargée de la justice, « *il est inacceptable que les consommateurs de l'Union puissent seulement saisir une juridiction californienne en cas de litige.* »



Mais elle n'a pas épargné la publicité mensongère, les arnaques, et le contenu sponsorisé mal identifié : la Commission a notamment visé les fameuses arnaques qui proposent « ***des iPhone ou iPad à 1 euro mais étant associées à un abonnement de longue durée caché, pour plusieurs centaines d'euros par an*** » explique les autorités bruxelloises qui prennent très au sérieux cette affaire.
Du côté des grandes entreprises américaines, Google assure déjà procéder à un examen approfondi de ces conditions. Facebook et Twitter préfèrent encore garder le silence sur les requêtes de Bruxelles.
En dehors des dossiers publicitaires, qui sont nécessairement sensibles pour les deux sociétés, la question de la modération et de la gestion de contenus calomnieux reste un problème douloureux du côté de Facebook comme du côté de Twitter. Les deux réseaux sont par ailleurs également pressés par l'Allemagne qui exigera prochainement une réactivité forte dans la lutte contre la désinformation et la calomnie sur les plateformes, sous peine sinon de voir la République Fédérale pénaliser Facebook d'une amende pouvant aller jusqu'à 50 millions d'euros.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères – Politique – Numerama*

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

---

L'organisation fondée par Julian Assange publie un second corpus de documents présentés comme émanant de la CIA qui décrivent les méthodes de l'agence pour pirater des ordinateurs Apple et des iPhone.

Wikileaks remet le couvert. Près de deux semaines après avoir mis en ligne « Vault 7, Year Zero », un ensemble de plusieurs milliers de documents internes détaillant des dizaines de programmes d'espionnage électronique et informatique de la CIA, l'organisation fondée par Julian Assange a publié une deuxième vague d'archives décrivant les techniques utilisées par l'agence du renseignement extérieur américain pour pirater des produits Apple. Baptisé « Dark Matter », ce second volet explique comment la CIA peut pirater un ordinateur Apple, même si son propriétaire y installe un nouveau système d'exploitation, ou un iPhone neuf en pénétrant le réseau d'approvisionnement et de distribution de la marque à la pomme.
• Wikileaks : 5 questions pour comprendre les dernières révélations

Un logiciel indétectable et impossible à effacer

Selon les documents dévoilés par Wikileaks, la CIA a développé un outil en 2012 nommé « Sonic Screwdriver » permettant de passer outre le processus de démarrage d'un MacBook à partir des accessoires périphériques comme une clé USB ou un adaptateur Ethernet branché dans le port Thunderbolt. L'agence pouvait alors **introduire un micro indétectable dans le logiciel profond** (firmware) de l'ordinateur et **bénéficier d'un accès permanent à son contenu** car même une réinstallation du système d'exploitation ou un reformatage de l'appareil ne pouvait suffire à l'effacer. La CIA devait avoir accès physiquement aux appareils visés pour les infecter.
Un autre document montre que la CIA avait conçu cet outil dès 2008 pour l'installer physiquement sur des iPhone neufs. Selon Wikileaks, il est par conséquent « probable que beaucoup d'attaques physiques par la CIA aient infecté la chaîne d'approvisionnement » d'Apple « en bloquant des commandes ou des livraisons ». L'agence américaine « peut faire cadeau à une cible d'un MacBook Air sur lequel a été installé ce micro », indique un document daté de 2009. « L'outil prendra la forme d'un implant/relais opérant dans le (logiciel) profond du MacBook Air et nous permettant d'avoir les moyens de (le) commander et de (le) contrôler », peut-on lire dans ces documents.

Les produits actuels vraisemblablement pas concernés

Apple n'a pas encore réagi à ces révélations. La plupart des documents datant de plus de sept ans et concernent les premières générations d'iPhone. Il apparaît peu probable que les produits actuels du groupe soient vulnérables à ces techniques. La méthode « Sonic Screwdriver » utilisée pour infecter des MacBook rappelle la faille « Thunderstrike » découverte fin 2014, qui permettait de contaminer un Mac lors de l'allumage à l'aide d'un appareil Thunderbolt vérolé, et corrigée par Apple depuis.
Le 9 mars, Wikileaks avait déjà diffusé près de 9.000 fichiers mettant à nu les capacités d'espionnage de la CIA et le recours à des pratiques particulièrement intrusives pour transformer des télévisions et des voitures connectées en mouchards, espionner des iPhone et des smartphones Android ou contourner des antivirus commerciaux. La CIA n'a jamais authentifié les documents mais de nombreux experts les jugent crédibles. Apple avait fait savoir qu'elle avait corrigé les failles évoquées dans ces documents. Wikileaks affirme détenir des informations sur plus de 500 programmes au total et promet de les publier dans les prochaines semaines.
Benjamin Hue, Journaliste RTL

Source : *Wikileaks montre comment la CIA a piraté des MacBook et iPhone neufs*

Data Protection Officer : Qui seras-tu ?

Data Protection Officer : Qui seras-tu ?

Dès la mi-2018, la nouvelle directive européenne baptisée GDPR est appelée à remplacer les dispositions de la Loi Informatique et Libertés. Celle-ci va rendre obligatoire la nomination d'un DPO (Data Protection Officer) dans de nombreuses organisations pour lesquelles la protection des données représente un enjeu majeur. Selon l'étude « CIO Concern Management » de Janco Associates, la sécurité arrive en tête des préoccupations des DSI à hauteur de 68%. De la même manière, les fuites de données observées chez des majors du Web et largement relayées dans les médias ont participé à construire ce climat anxiogène.

Pour être efficace, un DPO doit considérer les deux fonctions principales de sa mission que sont la protection des données personnelles et la protection de la confidentialité des données.
La protection des données personnelles fait appel à des exigences en termes de moyens et processus à mettre en œuvre qui peuvent être très variables d'un pays à l'autre. Dans un contexte de développement à l'international, le DPO sera un soutien précieux afin d'appréhender les différents aspects réglementaires.
La protection de la confidentialité des données est quant à elle un peu plus poussée puisqu'il s'agit de garantir que chaque donnée soit protégée à hauteur de ses enjeux pour l'entreprise. Autrement dit, ce n'est plus la loi mais le client qui fixe les règles !
Toutes les données informatiques n'ont pas la même valeur. Une plaquette commerciale où le plan détaillé d'un prototype en cours de conception n'auront pas le même effet s'ils se retrouvent révélés. Le DPO doit donc, avec son client, mesurer le risque de divulgation de chaque donnée et son impact pour l'entreprise. De données « publiques » à « très secrètes », il doit être capable de garantir au client que ses exigences soient remplies en termes de sécurité… et même si l'on met en place assez facilement des méthodes de chiffrements sur les disques, cela ne résout pas tout !
La plus grande faille sécuritaire qu'il puisse exister réside finalement dans l'humain lui-même. Pour être totalement rassuré quant à la confidentialité de ses données, le client doit être certain que même les équipes système de son prestataire ne puisse pas les lire…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Data Protection Officer : Qui seras-tu ? – Global Security Mag Online*

Google, ou la révolution transhumaniste via le Big Data

Google, ou la révolution transhumaniste via le Big Data

A l'occasion de la sortie du livre de Christine Kerdellant Dans la Google du loup, Éric Delbecque décrypte le projet de « fusion » entre le vivant et le digital porté par le géant de l'informatique américain.

Christine Kerdellant a relevé un beau défi *Dans la Google du loup* (Plon)! Elle met le doigt là où Google pose véritablement problème, à savoir sur la révolution anthropologique du transhumanisme… Pour ce qui concerne sa participation à la société de surveillance globale que fabriquent un certain nombre d'acteurs publics et privés, l'affaire est entendue depuis des années… Sous l'administration Obama, les dirigeants de Google se rendirent à la Maison-Blanche 230 fois! Ils confirmèrent en 2013 que les agences gouvernementales de l'Oncle Sam les sollicitaient annuellement – dans le cadre du Patriot Act – pour surveiller 1000 à 2000 comptes. En janvier 2015, la firme vedette du Web a reconnu avoir fourni au Ministère de la Justice américain l'intégralité des comptes Google de trois membres de WikiLeaks.

Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons.

Il paraît dès lors compliqué de penser qu'une idéologie sécuritaire explique à elle seule l'extension de l'ombre de Big Brother sur le monde. Les géants du numérique du secteur privé (les GAFA: Google, Amazon, Facebook, Apple) participent largement à la manœuvre, plus ou moins volontairement (pas pour des raisons politiques, mais économiques). Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons. Sa stratégie en matière de renseignement doit se lire comme un fragment d'un système cybernétique (au sens de science du contrôle) beaucoup plus vaste, où le capitalisme financier californien et numérique occupe une place décisive. Séparer ce dernier du complexe militaro-sécuritaro-industriel de l'Oncle Sam devient de plus en plus difficile, voire hasardeux.

L'intérêt plus décisif du livre de Christine Kerdellant est ailleurs. Il explore de manière très accessible et percutante le cœur du projet Google, ou plutôt sa signification philosophique profonde. Derrière les joyeux Geeks de la Silicon Valley s'exprime la volonté de réifier l'humanité, de l'enchaîner à une raison calculante. Cette dernière va nous émanciper nous répète-t-on, nous libérer – via le Big Data – des limites de notre condition, nous délivrer de la mort et transformer notre existence en un jardin de fleurs. Mais lorsqu'on choisit d'examiner de plus près les conséquences des propositions de Google, on découvre une perspective d'avenir moins réjouissante…[lire la suite]

Réagissez à cet article

Source : *Google, ou la révolution transhumaniste via le Big*

Data

RGPD : Ce qui va changer pour les professionnels de santé

	**RGPD : Ce qui va changer pour les professionnels de santé**

Fin des déclarations Cnil, demandes de consentement et sanctions renforcées, une nouvelle réglementation européenne* va venir chambouler la gestion des données personnelles en magasin. En tant que commerçants et professionnels de santé, vous collectez et transmettez des données relatives à vos clients. Le GDPR (General Data Protection Régulation) devra donc s'appliquer à votre point de vente. Zoom sur ce qui change dès le 25 mai 2018.

Registre des traitements et désignation d'un délégué à la protection des données

Quotidiennement vous gérez, stockez et envoyez les données de santé de vos clients que ce soit pour la pratique du tiers payant ou effectuer une commande auprès de vos fournisseurs. Identité, numéro de Sécurité sociale, facturation, prescription… vous êtes amenés à traiter des données personnelles, qui doivent actuellement faire l'objet d'une déclaration auprès de la Cnil (Commission nationale de l'informatique et des libertés). Mais bientôt, vous n'aurez plus besoin de cette formalité préalable.

En effet, le règlement européen sur la protection des données personnelles repose sur une logique de conformité, dont les acteurs seront désormais responsables. En d'autres termes, le poids de la procédure administrative va être transféré de la Cnil. **Dès le 25 mai 2018, vous devrez être en possession et tenir un « registre des traitements mis en œuvre ».** Ce dernier devra notamment spécifier :

- les catégories de données traitées ;
- la finalité ;
- les différents destinataires ;
- la durée de conservation.

« Ce registre informatisé permettra au professionnel de se ménager des preuves vis-à-vis de la Cnil. Il prouve son adhésion à un code de conduite, explique Maître Cécile Vernudachi, avocate au Barreau de Paris. Les grandes enseignes pourront également désigner un délégué à la protection des données, qui deviendra le point de contact avec la Cnil et un véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Dans les plus petites structures, ce ne sera pas une obligation », précise-t-elle.

Consentement renforcé et transparence

Le règlement européen impose également la mise à disposition d'une information claire, intelligible et aisément accessible à vos clients. Il définit en ce sens l'expression du consentement : « **les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.** La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe », précise le document.

En d'autres termes, avant chaque devis ou chaque vente, vous êtes tenus d'obtenir le consentement de votre porteur pour pouvoir traiter et transmettre ses données personnelles. « Concernant la correction, seul le patient peut donner son accord pour la transmission de cette donnée, souligne Maître Vernudachi. **Son consentement doit obligatoirement être écrit.** Dans le cadre de l'exécution d'un contrat, il n'y a alors plus de restriction. Toutefois, il est interdit d'utiliser cette information pour la vendre à un tiers ou à des fins marketings et commerciales ».

Spécificité pour les moins de 16 ans :

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Des sanctions encadrées et graduées

Les responsables de traitement, autrement dit les dirigeants ou chef d'entreprise, les plateformes de services et les complémentaires santé, peuvent enfin faire l'objet de **sanctions administratives importantes en cas de non-conformité au nouveau règlement**. Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes dans le cas d'une entreprise, elles peuvent s'élever de 2% à 4% du chiffre d'affaires annuel mondial, en fonction de la catégorie de l'infraction.

Notons que selon l'étude « Crossing the Line » du cabinet KPMG**, les Français sont 2ème sur le podium des consommateurs les plus vigilants quant au traitement de leurs données personnelles. Aussi, le règlement européen sera en vigueur dès le 25 mai 2018. Il vous faut donc être vigilant et vous y préparer dès maintenant !

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

****étude publiée en novembre 2016***

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Ce qui va changer dans les magasins pour le traitement des données personnelles | Acuité*

Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

---

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

De plus en plus d'élèves confrontés au cyberharcèlement

	**De plus en plus d'élèves confrontés au cyberharcèlement**

Brimades, insultes, sexting (envoi de messages et photos explicites)… un adolescent sur six, en moyenne, est confronté au harcèlement. Un sujet qui reste pourtant tabou. L'école IESPP a décidé de prendre le problème à bras-le-corps et de lancer des ateliers de sensibilisation auprès de ses plus jeunes élèves.

Les élèves ont visionné le film « Marion, 13 ans pour toujours ».

On sait à quel point les enfants peuvent être cruels entre eux… mais désormais, avec les réseaux sociaux et les smartphones, les conflits qui éclatent à l'école se poursuivent jusqu'à la maison : « *Ils sont tellement connectés H24 qu'il n'existe plus cette frontière, ce temps de répit le soir* », précise Olivier Bogaert, spécialiste de la cybercriminalité et invité à participer activement au projet mené par l'IESPP de Tournai.

Et surtout, dans le chef des enfants, puisque c'est virtuel… ce n'est pas si grave : « *Ils ne se rendent pas compte que multiplier des messages d'insultes peut devenir du harcèlement* », ajoute le policier fédéral. « *Beaucoup affirment que ce n'était pas sérieux* »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Tournai: des élèves de plus en plus confrontés au cyberharcèlement – nordeclair.be*

Les CNIL européennes s'inquiètent du décret Trump pour le Privacy Shield

Les CNIL européennes s'inquiètent du décret Trump pour le Privacy Shield

---

Les CNIL européennes s'inquiètent du récent décret sur l'immigration du Président Trump. Elles veulent s'assurer que le Privacy Shield n'en souffrira pas.

Alors que Donald Trump a annoncé la présentation d'un nouveau décret sur l'immigration la semaine prochaine, les CNIL européennes se sont penchées sur le premier décret, suspendu par la justice. Celui-ci a été pris le 25 janvier dernier et comportait une clause pouvant avoir un impact sur le récent accord de transfert transatlantique des données : le Privacy Shield.

En effet, la clause numéro 14 du décret indique que « *les agences devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables* ». Les agences citées dans le texte sont bien évidemment celles du renseignement comme la NSA ou le FBI. Pour autant cette notion de « *pas de protection de la confidentialité pour les citoyens non-américains* » heurte l'essence même du Privacy Shield. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que le droit européen…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Privacy Shield : Les CNIL européennes s'inquiètent du décret Trump | Silicon*