Palmarès des mots de passe 2015

	**Palmarès des mots de passe 2015**

Comme chaque année, Splashdata dévoile les mots de passe les plus utilisés par les internautes, une liste qui est le fruit de données volées et rendues publiques. Sans surprise, « 123456 » et « password » se disputent toujours les deux premières places. Mais ce palmarès 2015 révèle aussi l'influence de Star Wars dans le choix des internautes.

Tous les ans à la mi-janvier, nous attendons avec impatience la réponse à cette question : l'humanité a-t-elle enfin compris que la plus grande des failles informatiques était un mot de passe trop simple à trouver ?
Mais cette fois encore, la déception est au rendez-vous : ces satanés « 123456 » et « password » trônent encore, là, tout en haut du classement.
Évidemment, on peut modérer ce sentiment en rappelant que la liste en question est obtenue en étudiant « seulement » deux millions de mots de passe échappés dans la nature. Comparé aux près de trois milliards d'internautes dans le monde, qui possèdent chacun plusieurs mots de passe (si, si, ça existe), cela reste faible.
Mais l'échantillon demeure représentatif, et on peut malheureusement imaginer que dans notre entourage proche, certains utilisent encore 12345678 (troisième du classement) ou même 12345 (qui rétrograde en cinquième position).

La tête de ce classement 2015 s'éloigne assez peu de celle du palmarès 2014, mais laisse tout de même de la place pour quelques nouveautés, dont le très original « welcome », directement propulsé en onzième position, immédiatement suivi par un autre promu, le très complexe « 1234567890 ».
Enfin, on note l'influence de la sortie de l'épisode 7 de *Star Wars* sur ce millésime 2015 : « princess » (en 21e position) et « solo » (23e) peuvent le laisser penser, alors que « starwars » (25e) ne laisse pas de place au doute.
Le classement en question :

- 1. 123456 (-)
- 2. password (-)
- 3. 12345678 (+1)
- 4. qwerty (+1)
- 5. 12345 (- 2)
- 6. 123456789 (-)
- 7. football (+3)
- 8. 1234 (-1)
- 9. 1234567 (+2)
- 10. baseball (-2)
- 11. welcome (nouveau)
- 12. 1234567890 (nouveau)
- 13. abc123 (+1)
- 14. 111111 (+1)
- 15. 1qaz2wsx (nouveau)
- 16. dragon (-7)
- 17. master (+2)
- 18. monkey (-6)
- 19. letmein (-6)
- 20. login (nouveau)
- 21. princess (nouveau)
- 22. qwertyuiop (nouveau)
- 23. solo (nouveau)
- 24. passw0rd (nouveau)
- 25. starwars (nouveau)

Réagissez à cet article

Source : *Palmarès des mots de passe 2015 : du classique, mais avec un peu de Star Wars*

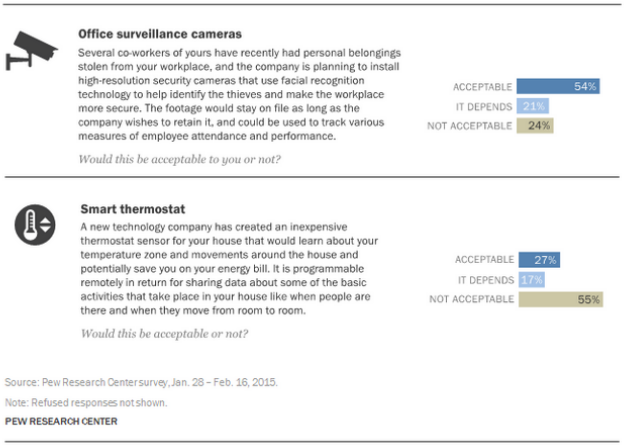
Données personnelles : les Américains sont prêts à faire des concessions

Données personnelles : les Américains sont prêts à faire des concessions

---

Selon une étude de Pew Research Center, une large proportion d'Américains est prête à dévoiler des informations personnelles en échange d'un bien ou d'un service. Du gagnant-gagnant ?

La protection de la vie privée serait un concept à géométrie variable pour les Américains, selon une étude menée par le **Pew Research Center**. Selon lui, une majorité d'Américains ne verraient pas d'inconvénient à partager avec des tiers leurs données personnels, en échange d'un produit, d'un service, ou pour d'autres bénéfices.
Ainsi, 54% d'entre eux estiment qu'il est acceptable pour un employeur d'installer des caméras de surveillance dans les locaux de l'entreprise, pour dissuader – officiellement- d'éventuels voleurs et 47% sont enclins à délivrer des infos personnels pour disposer d'une carte de fidélité.
Alors que, paradoxalement, 55% des personnes interrogées sont réticentes à l'idée d'utiliser au sein de leur foyer un thermostat connecté, susceptibles de relayer auprès de prestataires des informations sur les us et coutumes d'une maisonnée.



En outre, les Américains sondés sont aussi réfractaires aux sollicitations que ne leur « rapportent » rien en échange : ils n'apprécient ainsi que très peu les envois de spams et les demandes de contacts intempestives qui arrivent après avoir partagé avec une entreprises des données personnelles.
Les plus réfractaires au partage d'informations privées mettent surtout en exergue le fait qu'ils ne sont pas tenus au courant des types d'entreprises qui ont accès à ces données. L'anonymisation ne se fait qu'en un seul sens…
Ils s'interrogent aussi sur intentions qui motivent ce type d'entrepris, ravivant ainsi une certaine peur du « Big Brother ».

Crédit image : Gajus – Shutterstock.com

Réagissez à cet article

Source : *Données personnelles : les Américains sont prêts à faire des concessions | ITespresso.fr*

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

L’e-réputation ne concerne plus les entreprises et les organisations de marque. Tout le monde peut disposer d’une image sur internet. En effet, avec ou sans permission, des sujets peuvent parler d’une personne notamment via des discussions, des images ou des vidéos. Or, dans ces discours et mauvaises appréhensions ne restent pas dans le monde virtuel. En fait, cela peut impacter la vie quotidienne, détruire des relations et même des carrières professionnelles. Heureusement que ce n’est pas une fatalité. L’e-réputation peut être géré et même utilisé à bon escient. Comment faire ?

Ajouter de l’importance à son image
Quels que soient les documents ou fichiers qu’il faut mettre en ligne, il faut les prendre en conscience. CV, photos ou des commentaires faits sur les plateformes sociales, ils contribuent tous à l’e-réputation d’une personne. Bien que quelque peut inévitable, ces contenus sont les vitrines d’une personne, alors autant qu’elle lui ressemble. La meilleure façon est de ne jamais négliger son e-réputation. Tout ce qui est sur internet reste sur internet ! Telle est la règle.

Avoir un bon aspect de l’état des lieux
Le mieux est d’évaluer son e-réputation le plus tôt possible. C’est très simple, il n’y a pas besoin de faire appel à une agence e-réputation pour avoir une idée de son e-réputation. Pour ce faire, il suffit de taper une requête sur la barre de recherche des moteurs de recherche. De porter une analyse sur au moins les deux premières pages (au lieu de rester sur la première). La suite consiste à vérifier s’ils coïncident avec l’image voulue, s’ils peuvent être lus publiquement…

Penser à son avenir
Les réseaux sociaux constituent en fait une bonne alternative pour constituer un réseau professionnel. Il y a également les sites dédiés avec qui, il faut prendre à l’avance des précautions. En fait, pour une candidature donnée les recruteurs ne s’arrêtent pas sur leur site. Ils peuvent étendre (et c’est bien compréhensible) leur recherche sur les autres plateformes sociales et même sur la totalité des moteurs de recherche.
De même pour les amis Facebook par exemple, ce sont les personnes les plus susceptibles de devenir un danger pour un internaute. La situation n’est pas toujours délibérément provoquée, par contre une identification sur une photo relatant une soirée vertigineuse entre élève et prof employer et employeur ne fait pas bon ménage. Pour éviter cette situation, il est indispensable de bien maitriser les paramètres (ce que peu de gens font également).
Après les constatations, les actions ! Quelle que soit la plateforme, il faut toujours vérifier les paramètres. Entreprendre des petites actions peut permettre à aider des problèmes plus graves. Comme le classement des amis par rapport au lien et relation partagée. Par exemple pour Facebook, cliquer sur rubrique confidentialité et choisir option « examiner les publications dans lesquelles vos amis vous identifient avant qu’elles n’apparaissent sur votre journal ».

Apparaitre ou ne pas apparaitre ?
Telle est la question ! En premier lieu, demander le droit de ne faire aucune publication sur internet ! C’est toujours possible à faire, mais il faut prendre en compte les autres internautes qui peuvent toujours influer l’e-réputation. L’inconvénient réside alors dans le fait qu’il n’y aura que du mauvais contenu à l’encontre de la personne en question. Un autre inconvénient est que les recruteurs n’aiment pas trop les candidats qui sont trop discrets sur le web.
Du coup, autant prendre le mal par les cornes ! Avoir le pouvoir de supprimer les contenus indésirables en contactant Google ou en faisant appel à une agence e-réputation.

Réagissez à cet article

Source : *Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1*

La Cour de cassation confirme la sanction de 10.000 €

contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés !

	**La Cour de cassation confirme la sanction de 10.000 € contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés !**

La commission restreinte de la Commission nationale de l'informatique et des libertés avait relevé que la société avait manqué à l'obligation de proportionnalité en plaçant et maintenant sous surveillance l'un au moins de ses salariés bien au-delà du délai de mise en conformité fixé par la mise en demeure.

L'arrêt N°371196 du Conseil d'État du 18 novembre 2015 a confirmé la sanction pécuniaire prise par la CNIL – Commission Nationale Informatique et Liberté – d'un montant de 10.000 € avec la publication de la décision sur le site internet de la CNIL et sur le site Légifrance, à l'encontre d'une entreprise qui avait installé un système de vidéosurveillance intrusif sur le lieu de travail des salariés.

Dans ce litige, la Cour de cassation a considéré que les données à caractère personnel collectées par un responsable de traitement doivent être " *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées ainsi et de leurs traitements ultérieurs* ". De plus, aux termes de l'article L1121-1 du Code du travail : " *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ".

La surveillance des salariés par l'employeur

L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail.

Toutefois, l'article L1222-4 du Code du Travail indique qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

De plus, l'article L2323-32 du même Code précise que le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

L'arrêt N°10-23482 de la Cour de Cassation du 10 janvier 2012 a indiqué qu'un employeur qui utilise la vidéosurveillance pour contrôler ses salariés doit les prévenir préalablement.

Ainsi, un employeur n'est pas autorisé à utiliser, comme mode de preuve licite, les enregistrements d'un système de vidéo-surveillance installé pour permettre le contrôle de leur activité et de leurs horaires d'arrivée et de départ, si les salariés et le comité d'entreprise n'ont pas été préalablement informés.

Le respect à la vie privée des salariés au travail

La délibération 2012-475 du 3 janvier 2013 de la CNIL avait déjà indiqué sa position sur la vidéosurveillance des salariés d'une entreprise en interdisant de surveiller en permanence des salariés sur leurs lieux de travail sauf circonstances particulières.

La CNIL, conformément à l'article L1121-1 du Code du Travail, précise que : " *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ".

Ainsi, il est interdit de filmer les salariés en continu sur les lieux de travail sauf circonstances particulières, par exemple en cas de personnes exposées à un risque d'une particulière gravité.

Toutefois, la sanction pécuniaire prise par la CNIL – Commission Nationale Informatique et Liberté – d'un montant de 10.000 € avec la publication de la décision sur le site internet de la CNIL et sur le site Légifrance, est justifiée à l'encontre d'une entreprise qui avait installé un système de vidéosurveillance intrusif sur le lieu de travail des salariés.

Réagissez à cet article

Source : *CNIL : La Cour de cassation confirme la sanction de*

10.000 € contre un employeur qui utilisait abusivement la vidéosurveillance sur le lieu de travail des salariés ! | Infos Droits

---

Le « friend finder » de Facebook devient illégal en Allemagne

Le « friend finder » de Facebook devient illégal en Allemagne

---

La plus haute cour de justice allemande a déclaré illégal l'outil de recherche d'amis « friend finder » du réseau social américain Facebook.

Le comité de la Cour fédérale d'Allemagne a jugé que la fonction de recherche d'amis de Facebook viole la loi sur la publicité, a rapporté le journal britannique The Guardian.

© FLICKR/ MOMPL

Facebook: cachez-moi cette sirène que je ne saurais voir!

En accédant au carnet d'adresses de l'utilisateur, le « friend finder » récolte tous les contacts et leur envoie des invitations leur proposant de s'inscrire sur le réseau social. C'est ce mécanisme de collecte d'adresses électroniques et son utilisation dans un but marketing qui a été condamné.

La cour a conclu que cette pratique de marketing était trompeuse, confirmant les décisions de deux tribunaux de Berlin de 2012 et 2014, qui avaient constaté que Facebook violait les lois allemandes sur la protection des données et sur les pratiques commerciales déloyales.

La Cour fédérale a également déclaré que Facebook n'avait pas informé d'une façon adéquate les membres du réseau sur le mécanisme qui utilise les données de leurs contacts.

© AP PHOTO/ DAPD, JOERG KOCH

Facebook dévoile les sujets de discussion les plus populaires en 2015

Le représentant officiel de Facebook en Allemagne a, à son tour, déclaré que la société attendait le rapport explicatif de la décision finale et qu'elle l'étudierait les solutions « pour évaluer tout impact sur les services ».

C'est une vraie victoire pour l'association de protection des consommateurs allemands VZBV (Verbraucherzentrale Bundesverband) qui menait ce combat depuis 2010. En outre, elle ne compte pas arrêter sa lutte contre les géant d'Internet et souhaite maintenant vérifier les mécanismes de LinkedIn et Twitter.

« En plus de Facebook, d'autres services utilisent cette forme de publicité pour attirer de nouveaux utilisateurs. Ils doivent maintenant probablement repenser leurs systèmes », a déclaré Klaus Mueller, président de VZBV.

Réagissez à cet article

Source : *Le « friend finder » de Facebook devient illégal en Allemagne*

Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

	Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

Les députés de la commission des lois ont renforcé cette semaine les attributions de la Commission nationale de l'informatique et des libertés (CNIL), mais n'ont pas augmenté le montant des amendes pouvant être infligées par l'institution.

Le pouvoir de réprimande de la CNIL, qui peut actuellement prononcer des sanctions pécuniaires de 150 000 euros maximum en cas de premier manquement, c'est « cacahuète », dixit Axelle Lemaire ! Pour autant, l'intéressée s'est opposée dans le cadre de l'examen du projet de loi numérique à revoir ce niveau de sanctions… La secrétaire d'État au Numérique a en effet émis un avis défavorable sur les amendements visant à relever ce plafond (de 20 millions à 100 millions d'euros, selon les propositions des parlementaires).

En cause ? L'adoption imminente du règlement européen sur les données personnelles, sur lequel les institutions européennes sont parvenues à un accord fin 2015. « *La logique qui est poursuivie par le gouvernement jusqu'à présent, c'est de n'anticiper cette entrée en vigueur du texte européen que lorsqu'une marge de manœuvre est laissée à l'État membre. Ce n'est pas le cas en l'occurrence, même si je comprends tout à fait l'objectif posé par ces amendements* », s'est justifiée Axelle Lemaire. Le problème est surtout que le règlement n'a pas encore été officiellement traduit en français, ce qui ne permet pas de graver dès aujourd'hui dans le marbre des dispositions dont le législateur ne peut être certain qu'elles seront conformes au règlement européen…

« Marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois »

Pour certains députés, à l'instar de Philippe Gosselin (Les Républicains) et Isabelle Attard (Écologiste), la France aurait pourtant intérêt à anticiper l'entrée en vigueur du règlement – qui sera d'application directe mais sous deux ans à compter de l'adoption définitive du texte. « *Je pense que c'est important de marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois* » a ainsi plaidé l'élue du Calvados, reprenant une demande de la CNIL elle-même.

Crédits : Assemblée nationale

Invités par la secrétaire d'État au Numérique à retirer leurs amendements, les députés Gosselin, Attard et Martin-Lalande n'ont pas plié, Axelle Lemaire ne leur ayant donné que trop peu de gages. « *Je peux prendre l'engagement de tenter d'avancer sur ce sujet, sans vous assurer d'avoir une rédaction propre et définitive qui arrive dans quelques jours* [pour les débats en séance publique, ndlr]. *Je crois que les amendements que vous avez déposés ont le mérite de poser cette question. Si elle n'est pas suffisamment mûre à l'Assemblée nationale, elle aura peut-être mûri au Sénat, notamment parce que la traduction officielle sera disponible à ce moment-là* » a-t-elle déclaré, expliquant qu'un amendement gouvernemental sur ce sujet devrait être préparé en interministériel, notamment avec l'appui de la Chancellerie.

Tous leurs amendements ont cependant été rejetés (87, 265 et 454).

Vote de la saisine parlementaire de la CNIL, publicité de ses avis…

D'autres amendements concernant la CNIL ont en revanche été adoptés. L'autorité administrative pourra par exemple être consultée par le président de l'Assemblée nationale ou du Sénat sur une proposition de loi, sauf si le parlementaire à l'origine du texte s'y oppose. La gardienne des données personnelle est également autorisée à saisir l'ARCEP sur toute question relevant de sa compétence, et inversement.

Les amendements rendant obligatoire la publication des avis de la CNIL sur les projets de loi, alors que l'institution ne le fait aujourd'hui que sur demande du président de la commission des lois du Sénat ou de l'Assemblée nationale, ont d'autre part été votés. Il en ira de même pour les délibérations portant sur des décrets ou arrêtés pour lesquels la loi prévoit un avis de la gardienne des données personnelles.

Réagissez à cet article

Source : *Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros | Tech24*

La France aurait-elle peur de Intelligence artificielle ?

La France aurait-elle peur de Intelligence artificielle ?

L'intelligence artificielle caractérisée par l'autonomie croissante des machines, ça vous fait peur ? 65% d'un panel de Français répondent oui. Mais pour quelles raisons sont-ils inquiets ? Et aujourd'hui, l'IA, c'est quoi au juste ? Pas sûr qu'une majorité de Français puissent cette fois répondre.

	Plutôt d'accord	Plutôt pas d'accord
· L'intelligence artificielle est amenée à prendre un essor considérable avec le Big Data	69%	31%
· Le Big Data fera l'objet d'une utilisation très importante à long terme par les pouvoirs publics et les entreprises (profilage des individus, surveillance)	68%	32%
· Le Big Data présente des avantages à court terme pour la santé et le bien-être des individus (meilleure prévention des maladies et des risques, traitements plus adaptés, découvertes scientifiques, etc.)	67%	33%
· L'intelligence artificielle caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) vous inquiète	65%	35%

Non, ne paniquez pas, vous n'êtes pas pris dans une boucle spatiotemporelle et de retour en février 76, avec sur l'écran, face à vous, Roger Gicquel. Relativisons dès à présent. La France n'a pas peur de l'intelligence artificielle.
Mais une majorité de Français d'un panel de 10004 personnes se déclare plutôt d'accord lorsqu'on lui demande si l'intelligence artificielle « caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) » l'inquiète.

Des effets de génération dans les craintes

Et effectivement selon le sondage IFOP commandé par « L'Observatoire B2V des Mémoires », 65% se déclarent inquiets. Ce sentiment ne se diffuse cependant pas de façon uniforme d'un français à un autre.
Ainsi les 25-34 ans sont, en proportion, aussi inquiets (69%) que les 65 ans et plus (70%), bien plus en tout cas que les 18-245 ans (50%). De même, les résultats de l'étude font état de disparité géographique et en fonction du niveau de diplôme sur cette question.
« Il existe donc des effets de génération dans les craintes qui ne tiennent pas simplement à la jeunesse, à l'âge et au niveau d'éducation » commente dans un communiqué Jean-Gabriel Ganascia, professeur à l'Université Pierre et Marie Curie (Paris VI).
Les Français sondés sont donc en majorité inquiets, soit. Mais, et la question n'est pas pédante, combien de ces Français sont au fait des travaux autour de l'IA et de ses usages concrets ? Très certainement une très faible portion, car les notions et savoirs scientifiques associés à ce domaine de recherche s'avèrent d'une très grande complexité.
« Aujourd'hui beaucoup d'entreprises, dont Facebook, partagent cette même vision, à savoir que les problèmes que nous cherchons à résoudre sont infiniment complexes. Et même si nous employons les meilleurs talents, ce n'est pas suffisant pour résoudre ces problèmes comme celui de l'apprentissage non supervisé » expliquait ainsi Florent Perronnin, directeur du laboratoire de recherche parisien de Facebook dédié à l'intelligence artificielle.

« **La peur est dans la population parce qu'elle ne sait pas de quoi on parle** »

Mais celui qui résume le mieux le résultat de cette étude, c'est peut-être Michel Nachez dans une interview à Rue 89 :
« La séduction [à l'égard de l'IA] est du côté de ceux qui sont dans le milieu de l'informatique robotique, et chez les fans de science-fiction. La peur est dans la population parce qu'elle ne sait pas de quoi on parle. Elle est influencée par la littérature, le cinéma, les séries, où la machine finit par tourner mal, se retourne contre l'homme et le détruit. »
Cela ne signifie pas néanmoins que l'intelligence artificielle ne puisse pas être une source légitime d'inquiétude ou de questionnement, mais alors pour des risques bien différents de ceux qui pourraient être imaginés par certains, comme des machines douées de conscience se retournant contre leur créateur.
« Ceux d'entre nous en première ligne dans la fourniture de code sont très excités par l'intelligence artificielle, mais nous ne voyons pas de chemin réaliste permettant à notre logiciel d'acquérir une conscience » déclarait d'ailleurs à ce sujet Andrew Ng, un spécialiste renommé du machine learning (apprentissage automatique).

Et si le risque c'était l'homme et non l'IA ?

Plusieurs personnalités de l'univers des technologies, comme Bill Gates et Elon Musk, ont pourtant argué des dangers représentés par l'IA. Mais pour Jean-Gabriel Ganascia, interrogé par Le Monde, ces « allégations ne reposent sur rien […] Ce n'est même pas que je suis en désaccord sur le plan scientifique, c'est qu'il n'y a rien sur le plan scientifique. »
« Une machine peut être autonome au sens technique du terme : elle peut effectuer une chaîne d'actions (capter des informations, prendre une décision puis agir) sans que l'homme intervienne, à part en amont. Cela n'est pas dangereux en soi, car la machine est soumise au but que l'homme lui a donné » ajoutait-il.
Des dérives découlant de l'utilisation de ces technologies sont possibles. La FTC, le régulateur américain du commerce, souligne ainsi dans un rapport récent les risques potentiels d'exclusion engendrés par l'exploitation d'algorithmes (qui peuvent faire appel à de l'IA) appliqués au Big Data.
Mais la source de ces risques n'est pas alors l'IA elle-même, mais l'auteur ou l'exploitant des algorithmes, par exemple au travers d'un usage tourné essentiellement vers la maximisation du profit, et négligeant l'intérêt des consommateurs, la législation ou portant « atteinte à des valeurs fondamentales d'inclusion et d'équité. »
Et ces risques sont sans doute bien plus plausibles que l'émergence d'une intelligence artificielle malfaisante asservissant la race humaine. « Il pourrait y avoir, dans un futur lointain, une race de robots tueurs, mais je ne travaille pas aujourd'hui à éviter de rendre l'IA malveillante pour la même raison que je ne m'inquiète pas du problème de surpopulation sur la planète Mars » commentait Andrew Ng lors de la conférence GTC 2015.

Réagissez à cet article

Source : *Intelligence artificielle – La France a peur. Mais de quoi au juste ?*

Nissan victime d'une cyberattaque

Nissan victime d'une cyberattaque

Victime d'une cyber-attaque, le constructeur auto nippon a annoncé mercredi qu'il suspendait l'accès à tous ses sites internet. Les hackers d'Anonymous ont revendiqué l'action. Elle serait liée à la nouvelle campagne de chasse à la baleine par des navires japonais.

Anonymous contre Nissan, le tout sur fond de chasse à la baleine. Info ou intox ?

Les vérifications sont en cours mais la piste semble très sérieuse. Le constructeur auto nippon a annoncé mercredi qu'il suspendait l'accès à ses sites internet (www.nissan-global.com) « en raison d'une potentielle attaque par déni de service » (saturés par un nombre insurmontable de requêtes simultanées, les serveurs de la cible deviennent indisponibles, Ndlr) lancée la veille.

Un activiste se réclamant de la mouvance des Anonymous a posté sur son compte Twitter un message revendiquant l'action en faisant référence à la chasse aux baleines. « Nous sommes en train d'examiner la situation, nous ne savons pas pour l'heure si c'est vraiment lié à Anonymous », a précisé à l'AFP un porte-parole de Nissan.

Mercredi matin, Anonymous a levé le doute en confirmant l'attaque sur son compte Twitter. Mais pas encore le motif qui devrait faire l'objet d'un prochain post sur Tweeter.

Et ce n'est pas une première. Selon la chaîne japonaise NHK qui cite la police, Anonymous a déjà pris pour cible une centaine d'organisations dans l'archipel au cours du dernier trimestre 2015, l'accès au site officiel du bureau du Premier ministre Shinzo Abe a même été perturbé en décembre.

Une faille dans le moratoire

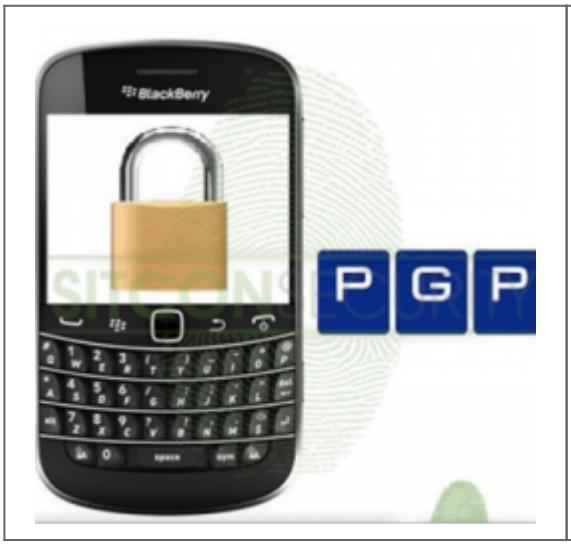
En dépit des admonestations répétées de l'ONU et de la Cour internationale de justice , les autorités nippones ont en effet repris la chasse à la baleine dans l'océan Antarctique en novembre dernier . Tokyo avait été contraint de renoncer à la saison 2014-2015 de prises de cétacés dans la zone australe après une décision en mars 2014 de la CIJ qui, saisie par l'Australie, avait jugé que le Japon détournait à des fins commerciales une activité présentée comme étant destinée à la recherche animale. A savoir : le programme de recherche scientifique baptisé «Jarpa», aux contours pour le moins flous.

Depuis, le pays a soumis un nouveau programme à la Commission baleinière internationale (CBI), lequel prévoit de capturer 3.996 petits rorquals (ou baleines de Minke) en Antarctique dans les douze prochaines années, soit 333 par saison contre environ 900 dans le cadre du précédent programme condamné.

Réagissez à cet article

Source : *Nissan victime collatérale de la cause des baleines – Industrie – Services*

Les Blackberry PGP déchiffrés par la Police hollandaise



Les Blackberry PGP déchiffrés par la Police hollandaise

Commercialisés par de nombreux vendeurs en ligne, les smartphones Blackberry embarquant en surcouche le standard de chiffrement de messagerie PGP seraient loin d'assurer un échange confidentiel des données. Tout du moins pour la Police hollandaise qui a confirmé être en mesure de les déchiffrer.

Les oreilles des défenseurs de la vie privée vont encore siffler. Des enquêteurs de la Police hollandaise ont en effet confirmé à Motherboard être en mesure d'accéder aux messages chiffrés envoyés depuis un terminal Blackberry sur lesquel le standard de chiffrement PGP est intégré en surcouche. « Nous sommes capables d'obtenir des données chiffrées depuis les terminaux Blackberry PGP », a fait savoir Tuscha Essed, responsable presse du Netherlands Forensic Institute (NFI), qui assiste la Police dans la recherche de preuves pour ses enquêtes en Hollande. L'information était parue initialement en décembre sur le blog misdaadnieuws.com où plusieurs documents sourcés NFI ont été publiés.

Le fait que les emails chiffrés puissent être lus et les messages effacés retrouvés, ne semble en tout cas pas perturber outre mesure les fournisseurs de Blackberry PGP. « Nous n'avons pas été affecté. Nos services sont complètement sécurisés et nous n'avons jamais été compromis », a indiqué un porte-parole de GhostPGP dans un mail à Motherboard. « Nous utilisons le dernier chiffrement PGP du moment qui est aussi impossible à déchiffrer. Nos clients sont très satisfaits du niveau de sécurité fourni », a quant à lui indiqué un représentant de TopPGP.com.

Réagissez à cet article

Source : *Les Blackberry PGP déchiffrés par la Police hollandaise – Le Monde Informatique*