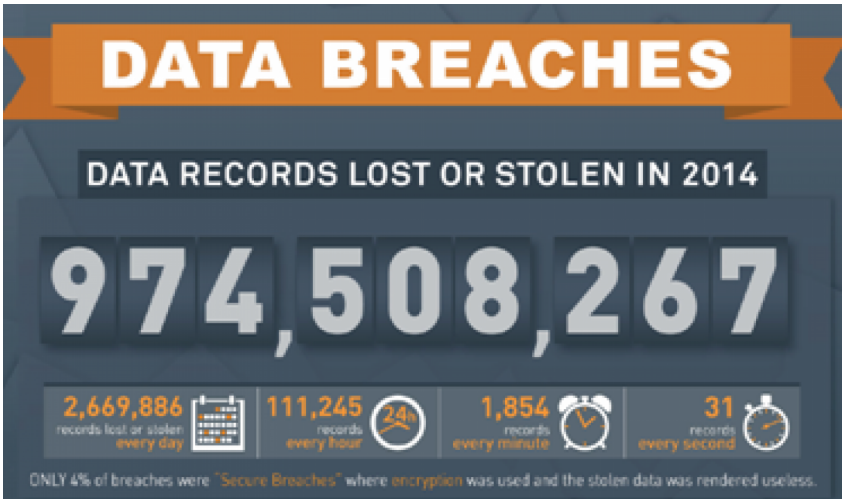
Cybercriminalité : un milliard de données volées en 2014 !



Cybercriminalité : un milliard de données volées en 2014 !

Selon l'étude Breach Level Index publié par le leader mondial de la sécurité numérique plus de 1 500 failles de données ont été enregistrées en 2014, entraînant le vol d'un milliard d'enregistrements de données. Par rapport à 2013, ces chiffres représentent une augmentation de 49 % du nombre de failles de données et de 78 % des enregistrements de données volées ou perdues.

Selon les données recensées dans l'indice BLI initialement réalisé par SafeNet pour l'année 2014, les cybercriminels sont principalement intéressés par le vol d'identité, 54 % des failles y étant rattachées, soit davantage que toute autre catégorie de failles y compris l'accès aux données financières. De plus, les infractions concernant les vols d'identité représentent également un tiers des failles de données les plus graves selon la notation du BLI (« catastrophique » pour une note comprise entre 9,0 et 10, ou « sévère » pour une note comprise entre 7,0 à 8,9). Les failles sécurisées, c'est-à-dire les failles de sécurité périmétrique où les données sont totalement ou partiellement cryptées, ont progressé de 1 % à 4 %.
« Nous assistons sans l'ombre d'un doute à un tournant dans la tactique abordée par les cybercriminels, le vol d'identité à long terme se substituant de plus en plus à l'immédiateté qui caractérise le vol des numéros de cartes de crédit », affirme Tsion Gonen, Vice-président en charge de la stratégie, Identity & Data Protection, Gemalto. « Le vol d'identité peut entraîner l'ouverture de nouveaux comptes de crédit frauduleux, la création de fausses identités à des fins criminelles, ainsi que d'autres activités d'une grande gravité. Les failles de données sont de plus en plus personnalisées, et il apparaît que pour l'utilisateur lambda, l'exposition aux risques est de plus en plus forte ».
Outre cette évolution vers le vol d'identité, les failles ont également augmenté en gravité en 2014, deux tiers des 50 failles les plus importantes selon leur score BLI ayant eu lieu l'année dernière. De plus, le nombre de failles de données impliquant plus de 100 millions d'enregistrements de données a doublé par rapport à 2013.
« Non seulement le volume des failles de données est en hausse, mais leur gravité est également de plus en plus importante. La question n'est plus de savoir « si » vous allez être victime d'un vol de données, mais « quand ». ajoute Tsion Gonen. La prévention des failles et la surveillance des menaces s'arrêtent là et ne sont pas toujours suffisantes pour repousser les cybercriminels. Les entreprises doivent adopter une vision des menaces numériques « centrée sur les données » en commençant par la mise en œuvre de meilleures techniques de gestion des identités et de contrôle d'accès, telles que l'authentification multi-facteurs, le chiffrement ou la gestion des clés pour sécuriser les données sensibles. Ces outils rendent les données subtilisées par les voleurs parfaitement inutilisables », précice-t-il.
En ce qui concerne les secteurs touchés, les services financiers et la grande distribution ont connu en 2014 les évolutions les plus significatives par rapport à d'autres segments industriels. La grande distribution est en légère augmentation par rapport à l'an dernier, avec 11 % de l'ensemble des failles de données enregistrées en 2014. Cependant, par le nombre d'enregistrements de données touchées, ce secteur est passé de 29 % en 2013 à 55 % en 2014 et ce, en raison de l'augmentation du nombre d'attaques visant les terminaux point de vente (TPV). Pour le secteur des services financiers, si le nombre de failles de données est resté relativement stable d'une année sur l'autre, le nombre moyen de dossiers perdus par faille a été multiplié par dix, passant de 112 000 en 2013 à 1,1 million en 2014.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://afriqueinside.com/cybercriminalite-milliard-donnees-volees-en-2014-12022015/

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Safe Harbor et CNIL : des régulateurs allemands dénoncent le laxisme de la Federal Trade Commission (FTC)

Des commissaires de la Cnil allemande ont lancé pour la première fois des procédure administratives contre deux transferts de données vers les Etats-Unis réalisés par des entreprises américaines sur la base de l'accord «Safe Harbor».

« La légitimité de l'accord est de plus en plus remise en question » a déclaré le commissaire Johannes Caspar (Hambourg) la semaine dernière lors d'un évènement consacré à la protection des données et organisé à Berlin. La frustration des commissaires les plus en pointe sur ce dossier vient du fait que cet accord n'a connu aucune réforme de fond suite aux révélations d'Edouard Snowden mentionnant que la NSA surveillait les données privées des citoyens allemands.
Dernier épisode en date, deux procédures administratives ont donc été initiées contre des entreprises américaines dans les landers de Berlin et de Brême.
Le programme Safe Harbor est un accord crucial pour les entreprises américaines. Google, Facebook ou encore Twitter peuvent en vertu de cet accord transférer légalement des données commerciales de l'Union européenne vers les États-Unis s'ils acceptent de respecter la loi applicable à la protection des données des citoyens des pays de l'UE. Cette loi porte essentiellement sur la collecte et le traitement des données.
C'est la FTC américaine qui doit vérifier que les exigences du Safe Harbor sont bien respectées par les entreprises américaines. Si l'accord venait à être dénoncé, cela aurait un impact important sur les activités des GAFA dans l'Union européenne.

Quel impact en cas de suspension du Safe Harbor ?
Suite au scandale d'espionnage de la NSA, de nombreuses voix européennes se sont élevées pour demander la suspension du programme Safe Harbor. Au lieu de suspendre l'accord, cependant, en novembre 2013, la Commission européenne a envoyé aux États-Unis une liste de 13 réformes qu'elle souhaite voir apporter au Safe Harbor. Le gouvernement américain n'a toujours pas pleinement répondu à la demande, même s'il avait promis de le faire pour l'été 2014. Tout cela pourrait être réglé en mai prochain, aux dernières nouvelles.
Reste que nul ne sait quel serait l'impact réel de la suspension du programme Safe Harbor. N'étant plus autorisés à transférer des données hors de l'UE, des entreprises comme Twitter, dont tous les serveurs sont aux Etats-Unis, auraient des difficultés majeures pour faire fonctionner leur activité européenne. Pour les entreprises qui ont des serveurs en Europe, cela affecterait néanmoins leur activité back-office, les données locales pouvant être transférées outre Atlantique pour subir un traitement algorithmique à des fins de profilage ou de détection des fraudes.
Mais la fin du Safe Harbor pourrait également porter préjudice à des entreprises européennes qui opèrent des données ailleurs qu'en Europe. Siemens, SAP et même BMW pour ne citer que les allemands, ont tout intérêt à expédier leurs données aux Etats-Unis quand cela est nécessaire d'un point de vue business.

5 000 membres de Safe Harbor
Plus de 5 000 sociétés sont membre de Safe Harbor, dont en plus des sociétés citées précédemment Amazon, Hewlett-Packard, IBM ou encore Microsoft. Ces entreprises affirment se conformer à un niveau 'adéquat' au exigences de protection des données personnelles de l'Union européenne.
Mais les inspections, réalisées par la FTC (Federal Trade Commission) des Etats-Unis, sont sporadiques, et les sanctions peuvent difficilement être appliquées. « De mon point de vue, la charge de la preuve n'est pas du ressort des entreprises américaines » a dit cependant Holger Lutz, associé chez Baker & McKenzie à DataGuidance. « C'est plus du ressort de l'autorité compétente en matière de protection des données ».
Les principes du Safe Harbor sont basés sur ceux de la Directive 95/46 du 24 octobre 1995 affirme la Cnil.
Les domaines couverts concernent l'information des personnes sur la collecte de données, la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite des personnes pour le recueil de données sensibles, le droit d'accès, de rectification et enfin la sécurité.
« Le Safe Harbor permet donc d'assurer une protection adéquate pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis » assure la Cnil, qui précise que la liste des entreprises ayant adhéré aux principes du Safe Harbor se trouve sur le site du Département du Commerce américain.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/safe-harbor-des-regulateurs-allemands-denoncent-le-laxisme-de-la-ftc-39814338.htm
Par Guillaume Serries

Télés connectées : un espion dans le salon ?

	Télés connectées : un espion dans le salon ?

Les téléviseurs Samsung sont l'équivalent du télécran du roman 1984 : un objet de surveillance qui enregistre tout ce qui est dit dans une pièce et épie les faits et gestes des utilisateurs. C'est la comparaison que faisait, dimanche, Parker Higgins, militant de l'organisation de défense des libertés américaines EFF.

Depuis, un vent de panique s'est emparé de possesseurs de téléviseurs connectés de la marque sud-coréenne et d'une partie de la presse. La raison : une phrase figurant dans les conditions d'utilisation édictées par Samsung, qui précise que **les services de commande à la voix existant sur ses téléviseurs peuvent être amenés à transmettre des conversations privées à un « service tiers »** :

« Nous vous signalons que, si les mots que vous prononcez contiennent des informations privées ou confidentielles, ces informations feront partie des données transmises à un tiers lorsque vous utiliserez le service de reconnaissance vocale. »

Glaçante, la phrase n'est pourtant pas une nouveauté : elle figure depuis longtemps dans les conditions d'utilisation des téléviseurs Samsung. Et on la retrouve également, presque mot pour mot, dans les conditions d'utilisation d'un téléviseur de la marque concurrente LG. Que signifie réellement ce jargon juridique ?

Actif ou passif ?

Pour le comprendre, il faut savoir comment fonctionnent les technologies de reconnaissance vocale. Qu'il s'agisse d'un téléphone Android ou iOS, d'une télévision, d'un ordinateur de bord dans une voiture, les objets dotés de cette fonctionnalité fonctionnent selon deux modes, actif ou passif. Dans le mode actif, il faut appuyer sur une touche pour indiquer à l'objet qu'il doit « écouter » ; dans le mode passif, l'objet « écoute » par défaut ce qui se passe autour de lui et déclenche une action s'il reconnaît une commande préenregistrée.

La reconnaissance vocale est une technologie complexe, qui nécessite une importante puissance de calcul pour bien fonctionner et reconnaître correctement les mots prononcés. Dans la plupart des cas, les objets qui ont besoin de pouvoir reconnaître plus que quelques mots-clés utilisent la puissance de calcul de machines très rapides connectées à Internet, et non uniquement la puce du téléphone ou de la télévision.

Les mots captés par l'objet sont donc transmis à distance à un serveur qui les analyse et renvoie sa conclusion à l'appareil. Pour fonctionner, ces services ont donc besoin de « transmettre des données à un tiers » – en l'occurrence, pour les téléviseurs Samsung, le leader mondial de la reconnaissance vocale, Nuance. Les données sonores transmises peuvent effectivement contenir des informations très personnelles, puisque la reconnaissance vocale « traite » l'ensemble de ce qui lui est transmis. La présence de ces termes dans les conditions d'utilisations est donc « normale » et s'apparente à un avertissement.

Accusé d'écouter les conversations de ses clients, Samsung a affirmé au Guardian qu'il n'enregistrait pas les sons captés par ses téléviseurs, et que les données sonores étaient uniquement « fournies à un service tiers durant une recherche de commande vocale ». Sollicitée par Le Monde, Nuance confirme qu'elle est bien destinataire de ces données vocales. *« Nous n'utilisons ces données qu'à des fins d'amélioration de notre technologie. […] Lorsque nous travaillons avec des entreprises tierces, un contrat garantit la confidentialité des données. […] Nous ne vendons pas ces données à des fins de marketing ou de publicité »*, écrit Gretchen Herault, le responsable de la vie privée de la société.

« Tempête dans un verre d'eau »

Autant d'informations qu'il est parfois difficile d'appréhender dans les conditions d'utilisation de ces télévisions connectée. Clauses floues, langage juridique abscons, textes interminables et difficilement accessibles… Ces textes sont la plupart du temps incompréhensibles pour quelqu'un qui n'a pas des connaissances en droit ni la patience de les lire.

En réaction, le Consumentenbond, l'équivalent néerlandais de l'UFC-Que choisir, a lancé l'an dernier une étude exhaustive sur les problèmes de vie privée posés par les téléviseurs connectés. L'organisation de protection des consommateurs a dressé un tableau comparatif des conditions d'utilisation de ces appareils, et le résultat est sans appel : celles de Sony ne font « que » six pages, tandis que celles de Samsung atteignent… cinquante-sept pages.

« La polémique autour de Samsung est de l'ordre de la tempête dans un verre d'eau », explique-t-on au siège de l'organisation, interrogée par Le Monde sur le sujet :

« Ces téléviseurs n'écoutent pas en permanence tout ce qui se passe dans la pièce – le problème le plus important, c'est que leurs conditions d'utilisation ne sont absolument pas transparentes et sont beaucoup trop longues. »

Dans le détail, le Consumentenbond note que la quasi-totalité des constructeurs ont inclus des clauses extrêmement larges et peu claires, voire illégales en droit européen. LG et Samsung ne précisent par exemple pas clairement quelles données sont collectées et dans quel but ; Sony l'explique clairement, mais ne dit pas qui collecte et conserve les données ; Panasonic est non seulement trop flou, mais exige aussi un paiement pour l'accès à ses données personnelles. Philips est le constructeur qui s'en tire le moins mal, selon l'étude : ses conditions d'utilisation sont certes longues, mais plutôt complètes et claires. L'entreprise reste cependant peu claire sur les types de tiers pouvant avoir accès aux données.

Les analyses effectuées par le Consumentbond sur des modèles des cinq constructeurs montrent que ces derniers collectent de très nombreuses informations – chaînes regardées, nom du film en cours de diffusion, recherches effectuées… Prises isolément, ces informations peuvent sembler peu dangereuses pour la vie privée. Mais l'**agrégation de ces « métadonnées » sur l'activité d'un téléspectateur permet, en définitive, d'en savoir beaucoup sur lui, ses goûts, ses habitudes** – parfois plus que si la télévision « écoutait » réellement toutes les conversations autour d'elle.

De vastes quantités de données personnelles collectées

Pour le démontrer, un informaticien britannique, Jason Huntley, a décidé en 2013 de brancher un outil d'analyse de trafic sur la télévision LG qu'il vient d'acheter. Il découvre alors que l'appareil transmet au fabriquant une gigantesque quantité d'informations – comme les films qu'il regarde ou ses changements de chaîne. Plus ennuyeux encore, le téléviseur enregistre le nom de tous les fichiers présents sur les clés USB qui sont branchées dessus et envoie ces données aux serveurs de LG.

A l'époque, M. Huntley publie un post de blog où il détaille ses découvertes ainsi que la réponse du constructeur, lequel estime que ces captations ne posent pas de problème puisque M. Huntley a accepté les conditions d'utilisation de sa télévision. Après une série d'articles très critiques à l'encontre de LG, le constructeur bloque la collecte de données – prévue notamment pour l'affichage de publicités ciblées.

« Mais l'année dernière, LG a forcé ses utilisateurs à accepter de nouvelles conditions d'utilisation », explique au Monde Jason Huntley, avec des clauses très floues.

« Les nouvelles conditions semblent les autoriser à collecter toutes les informations qu'ils recueillaient auparavant, y compris des informations sur des fichiers personnels hébergés sur des objets connectés au téléviseur. Cependant, lors de tests que j'ai effectués depuis, je n'ai pas trouvé de preuve qu'ils enregistrent effectivement ces informations. Je les soupçonne d'avoir prévu tous les cas de figure si à l'avenir ils décidaient d'activer de nouvelles collectes. »

Dans ses analyses, Jason Huntley n'a pas détecté de transmission suspecte ou non chiffrée de données vocales, mais il note que les constructeurs sont libres de changer de technologie de reconnaissance vocale ou de décider de transmettre ces données à d'autres partenaires, **« ce qui augmenterait les chances que les données soient utilisées à mauvais escient ou volées »**.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2015/02/11/teles-connectees-un-espion-dans-le-salon_4573664_4408996.html
Damien Leloup Journaliste au Monde

Confidentialité de nos données : les opérateurs télécoms ne respectent pas toutes leurs obligations

Confidentialité de nos données : les opérateurs télécoms ne respectent pas toutes leurs obligations

Les opérateurs télécoms ne respectent pas tous leurs obligations d'information et de consultation de leurs clients concernant l'utilisation qu'ils font de leurs données de trafic et de localisation. Et lorsqu'ils le font, ils le font en interprétant différemment la réglementation, ressort-il d'un rapport récent de l'Institut belge des services postaux et des télécommunications (IBPT) que relaie samedi L'Echo.

« Tant la transparence de la part des opérateurs que la manière dont ils se servent du consentement de leurs abonnés laissent à désirer », écrit l'IBPT. Les principaux manquements observés sont un manque de clarté concernant les données à traiter, une absence de demande explicite du consentement du client et de la possibilité de le retirer, ou encore l'absence de garantie du respect de la confidentialité quand un opérateur communique ces données à un tiers. Le régulateur du secteur entend à présent étudier la manière d'améliorer la situation et prévoit d'effectuer un contrôle plus régulier de ces obligations.

Cet article concerne les opérateurs Belges.
Que pensez-vous des pratiques des opérateurs de télécommunication Français ?
Le débat est ouvert…

Source : http://www.rtl.be/info/magazine/hi-tech/confidentialite-les-operateurs-telecoms-ne-respectent-pas-toutes-leurs-obligations-698389.aspx
Par Belga

Données personnelles : Facebook va être scruté de très près

Données personnelles : Facebook va être scruté de très près comme l'a été Google en 2012

Comme Google en 2012, Facebook va voir sa nouvelle politique de confidentialité être passée au crible par les autorités européennes de protection (Article 29) qui ont mis en place un groupe de travail spécial à cet effet. Car le réseau social pourrait bien violer la législation.

En 2012, Google avait modifié sa politique de confidentialité des données. Depuis le géant est en conflit avec les autorités européennes de protection qui l'accusent de violer la législation européenne. La firme a d'ailleurs déjà été condamnée.
Facebook doit-il dès à présent se préparer à une telle bataille juridique ? Trop tôt pour le dire. Toujours est-il que sa nouvelle politique de confidentialité, entrée en vigueur en janvier, n'échappera pas elle non plus à un examen des autorités européennes réunies au sein de l'Article 29.

Tout n'est pas si simple Facebook
Le groupe des Cnil a en effet mis spécialement en place un groupe de travail composé de plusieurs autorités de protection afin de passer au crible la nouvelle politique de Facebook, dont le réseau social a pourtant vanté les qualités de transparence et de contrôle pour l'utilisateur.
Ce groupe de travail sera piloté par l'autorité Belge. Y participent également les gendarmes allemand et néerlandais de la protection des données personnelles. L'Italie pourrait également rejoindre cette « task force ».
Car si Facebook assure, comme Google en son temps, respecter le droit européen, ce n'est visiblement pas aussi limpide d'après l'Article 29. Des infractions flagrantes aux lois européennes sur la protection des données sont pointées du doigt par plusieurs de ces autorités.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/donnees-personnelles-facebook-va-etre-scrute-de-tres-pres-39814284.htm

---

Avez-vous un plan pour sécuriser vos données?

05

Avez-vous un plan pour sécuriser vos données?

La 9e journée internationale de la protection des données a lieu le 28 janvier dernier. Une occasion de faire le point sur les précautions à prendre pour se protéger contre le vol de données en ligne.

David Décary-Hétu est chercheur au Centre international de criminologie comparée et professeur adjoint à l'École de criminologie de l'Université de Montréal. « Une menace courante est le cheval de Troie grâce auquel les cybercriminels peuvent prendre le contrôle d'un ordinateur à distance pour scanner vos fichiers nommés visa.txt ou passeport.jpeg, par exemple, ou passer par votre connexion pour trouver de nouvelles victime. Et tout ça se fera de façon automatisée », explique-t-il.

Le mot de passe, ce verrou numérique à ne pas négliger

« Les mots de passe sont la principale faille de protection ! », estime Carl Charest, spécialiste en nouveaux médias et co-fondateur de Letube.tv. Il ne faudrait en effet que 2 secondes à un cybercriminel pour décrypter un mot de passe reprenant un numéro de téléphone montréalais, selon howsecureismypassword.net, un site qui permet de tester l'entropie de vos mots de passe.

Entropie ? C'est la « puissance » avec laquelle votre mot de passe pourra résister aux attaques des pirates qui tenteront le plus souvent de le percer en testant, une à une, toutes les combinaisons possibles. « On peut jouer avec des minuscules, des majuscules ou des caractères spéciaux, mais la vraie force d'un mot de passe est dans sa longueur », explique M. Décary-Hétu, qui recommande d'utiliser au moins 10 caractères.

Des logiciels se chargeant de recrypter vos mots de passe, comme PasswordBox, un gestionnaire d'identité numérique développé par une start-up montréalaise et récemment rachetée par Intel, permettent aussi d'augmenter votre sécurité en ligne.

Attention à la navigation en eaux troubles

À l'image des chevaux de Troie, les hackers parsèment certains sites de programmes malveillants qui risquent de compromettre la confidentialité de vos données personnelles. Internet Explorer, Windows, Acrobat Reader, les cybercriminels s'attaquent aux logiciels les plus utilisés. Ils ont bien compris qu'à la pêche aux informations, il valait mieux planter sa ligne dans les zones où gravitent des bancs de poissons !

« Les gens ont pris l'habitude de se promener dans des coins un peu sombres d'Internet, ajoute David Décary-Hétu, ils regardent aussi beaucoup des vidéos sur des sites de streaming souvent infestés de virus qui permettront aux pirates d'infiltrer directement leur ordinateur. » Et vous pourriez bien n'y voir que du feu si votre anti-virus ne détecte pas ces virus. Mais « un signe qui ne trompe pas, c'est une machine qui commence à devenir lente et qui met du temps à démarrer », prévient M. Décary-Hétu.

Que faire une fois que l'on est infecté ? Au mieux, plusieurs logiciels de nettoyage existent, mais au pire, il faudra mettre la hache dans le système d'exploitation, tout effacer et tout réinstaller. D'où l'importance de faire régulièrement des copies de sauvegarde de ses fichiers sur des disques amovibles.

Les autres pièges de la toile

« Dès qu'on va dans un endroit public et qu'on utilise une connexion wifi qui n'est pas sécurisée, on peut se faire prendre très facilement », témoigne Carl Charest, dont une connaissance s'est fait dérober toutes ses données en se connectant à distance à son ordinateur de maison alors qu'elle assistait à une conférence. Même les dossiers médicaux seraient devenus une des cibles privilégiées par les délinquants, car ils contiennent la majorité de vos informations personnelles, mais aussi des données bancaires présentes dans les dossiers d'assurance.

Enfin, on ne clique pas sur tout ce qui surgit à l'écran ou atterrit dans sa boîte de courriels ! Les techniques d'hameçonnage grâce auxquelles les cybercriminels se font passer pour de vrais sites sont aussi courantes pour dérober des informations personnelles et financières.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesaffaires.com/mes-finances/consommation/avez-vous-un-plan-pour-securiser-vos-donnees/575727
Par Nafi ALIBERT

Denis JACOPINI est intervenu au Salon du numérique 2015 le 3 février et a coanimé une conférence avec Orange

Denis JACOPINI est intervenu au Salon du numérique 2015 le 3 février et a coanimé une conférence avec Orange

Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.

Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter ! Comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Cette conférence était présentée par Denis JACOPINI (Le Net Expert Informatique) et Eric Wiatrowsi (Orange Business Services)

Présentation pdf de Denis JACOPINI Le Net Expert Informatique
Présentation pptx de Hervé JUHEL Crédit Agricole
Les infos pratiques du salon
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

	Remise des trophées du 1er concours EDUCNUM Opération Vie privée à la CNIL

Le 28 janvier 2015, lors de la journée européenne de protection des données, le collectif Educnum a remis à la CNIL les prix aux lauréats du premier concours Educnum en présence de Mme Najat Vallaud-Belkacem, Ministre de l'Education nationale, de l'Enseignement supérieur et de la Recherche.

L'ambition des trophées
Pour que le web reste un espace d'échange et d'inspiration, mais aussi de respect de la vie privée, le collectif pour l'éducation au numérique a lancé le 13 octobre 2014 un concours pour les étudiants.

Son objectif :
• sensibiliser les plus jeunes, de l'école primaire au lycée, aux bons usages du web, par un dialogue intergénérationnel ;
• susciter et valoriser la créativité des étudiants ;
• mettre en lumière et donner vie à des projets innovants.

Les étudiants avaient carte blanche pour participer : application mobile, dataviz, goodies ou kit de survie sur les réseaux sociaux, tous les projets étaient les bienvenus.

Les lauréats
25 projets ont été présentés à l'issue de 3 mois de concours.
Le Grand Prix du Jury avec une dotation de 7000 euros est remis à l'équipe du Master 2 « Droit, économie et gestion de l'audiovisuel » à la Sorbonne, pour le projet Les aventures croustillantes de Prince Chip.
Le Prix Spécial du Jury avec une dotation de 3000 euros est attribué à l'équipe de l'Ecole Boulle pour le projet Data Fiction, le site dont vous êtes le héros. Vivre l'aventure, faire réfléchir, accompagner sont au cœur de ces projets qui placent le jeune public au cœur de l'action.

Les projets récompensés
« Prince Chip » Appelle à la vigilance des « âges » pour les 6/10 ans
La pédagogie sur les bonnes pratiques à adopter sur le web passe ici par un divertissement dans l'univers familier des fruits et légumes. Elle repose sur l'identification à un personnage attachant et l'utilisation d'une technique moderne, le stop motion. Le webdocumentaire Les Aventures croustillantes de Prince Chip offre aux adultes un outil d'accompagnement pour parler aux plus jeunes, dès leurs premiers pas sur le net. Unanimité du jury pour remettre le Grand Prix à une fiction qui donne la frite !
Visionner le projet
Pour Serge Tisseron, psychiatre et co-auteur de l'avis de l'Académie des Sciences « L'enfant et l'écran » et membre du jury : « C'est un bonheur de découvrir comment, sur Internet, un méchant poivron peut se faire passer pour une jolie tomate ! Je fais le pari que les autres épisodes sauront toucher avec une égale efficacité la part d'enfance qui existe chez chacun, et à tout âge. »

Devenir héros de son propres site avec « Data fiction » pour les 12/18 ans
Le serious game Data Fiction fait de l'internaute un héros. En partant des outils et services numériques utilisés par les jeunes au quotidien, le projet révèle à l'utilisateur l'exposition de ses données. Ce jeu en trois étapes (découverte, appropriation, tutoriel) fait le pari de l'expérience pour sensibiliser : incité à dépasser ses limites, le jeune devient acteur. Les compétences-métier des étudiants en design de l'Ecole Boulle ont été particulièrement saluées par le jury, « une véritable œuvre d'art ! ».
Visionner le projet

Pour Stéphane Distinguin, Président de Cap Digital et membre du jury, : « Le projet de l'école Boulle m'a particulièrement impressionné, par sa créativité, ses angles, très bien choisis, et la qualité remarquable de sa réalisation. Très cohérent et utile, je l'ai trouvé particulièrement juste ».

Et après ?
Lors de la soirée de remise des prix organisée à la CNIL, les lauréats ont pu rencontrer des membres du collectif Educnum et de la CNIL, la Présidente d'Universcience, la Direction du numérique pour l'éducation. Autant de bons conseils à échanger pour faire grandir ces projets et transmettre les bonnes pratiques au plus grand nombre.
« L'éducation au numérique est une responsabilité partagée qui nécessite une mobilisation générale. Les membres du collectif s'engagent à valoriser les projets retenus sur leurs supports de communication : sites Internet, réseaux sociaux.C'est le moyen pour ces étudiants d'avoir une très bonne visibilité et de pouvoir bénéficier d'une aide dans la réalisation future de leurs projets. », indique Isabelle Falque-Pierrotin, Présidente de la CNIL.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.cnil.fr/linstitution/actualite/article/article/remise-des-trophees-du-1er-concours-educnum-operation-vie-privee/

L’obligation de notification des violations de données à caractère personnel à la CNIL

L’obligation de notification des violations de données à caractère personnel à la CNIL

A l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées.

Cette obligation de notification a été transposée en droit français à l'article 34 bis de la loi informatique et libertés. Les conditions de sa mise en œuvre ont été précisées par le décret n° 2012-436 du 30 mars 2012, ainsi que par le règlement européen n° 611/2013 du 24 juin 2013.

Dans quels cas l'article 34 bis s'applique-t-il ?
L'article 34 bis de la loi informatique et libertés s'applique lorsque plusieurs conditions sont réunies :
• condition 1 : il faut qu'un traitement de données à caractère personnel ait été mis en œuvre
• condition 2 : le traitement doit être mis en oeuvre par un fournisseur de services de communications électroniques
• condition 3 : dans le cadre de son activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de son service de téléphonie ou d'accès à d'internet)
• condition 4 : ce traitement a fait l'objet d'une violation. Selon l'article 34 bis, une violation est constituée par une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel. Elle peut se produire de manière accidentelle ou illicite, l'intention malveillante étant l'un des possibles cas de figure, mais pas le seul.

Sont, par exemple, constitutifs d'une violation :
• Une intrusion dans la base de données de gestion clientèle d'un fournisseur d'accès internet (FAI) ;
• Une faille dans la boutique en ligne d'un opérateur mobile permettant de récupérer les numéros de cartes de crédits des clients ayant commandé un nouveau téléphone associé à un forfait (car ce sont les données clients collectées en tant qu'opérateur) ;
• Un email confidentiel destiné à un client d'un FAI, diffusé par erreur à d'autres personnes ;
• La perte d'un contrat papier d'un nouveau client par un agent commercial d'un opérateur mobile dans une boutique.

Ne sont pas des violations de données personnelles au sens de l'article 34 bis :
• Toute violation ne concernant pas un traitement du FAI comme un virus informatique qui s'attaque aux PC des abonnés du FAI pour collecter des données personnelles ;
• Toute activité ne concernant pas la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public tel que le piratage du fichier des ressources humaines du FAI.

Qui doit notifier la CNIL et informer les personnes concernées par la violation ?
L'article 34 bis vise les « fournisseurs de services de communications électroniques accessibles au public ». Il s'agit des opérateurs devant être déclarés auprès de l'ARCEP (article L. 33-1 alinéa 1 du code des postes et des communications électroniques) (par exemple, les fournisseurs d'accès à internet ou de téléphonie fixe et mobile).
Les services de la société d'information, tels que les banques en ligne, les sites d'e-commerce ou les téléservices des administrations, ne sont pas concernés.

Quand et comment notifier la CNIL ?
Toute violation doit être notifiée à la CNIL, quelle que soit son niveau de gravité.
La notification doit être adressée à la CNIL dans les 24h de la constatation de la violation.
Si le fournisseur de services de communications électroniques ne peut fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, il est possible de procéder à une notification en deux temps :
Une notification initiale dans les 24 heures de la constatation de la violation ; puis
Une notification complémentaire dans le délai de 72 heures après la notification initiale.
Cette notification doit se faire par lettre remise contre signature ou via le formulaire de dépôt en ligne accessible sur le site de la CNIL, à l'aide du formulaire de notification prévu à cet effet [faire un lien vers le formulaire de notification].

Quand informer les personnes ?
L'information des personnes doit être effectuée sans retard injustifié après constat de la violation de données à caractère personnel (article 91-2 du décret).
Cependant, le fournisseur n'a pas l'obligation d'informer les personnes dans les cas suivants :
la violation n'est pas susceptible de porter atteinte aux données ou à la vie privée des personnes (un outil permettant d'évaluer le niveau de gravité d'une violation est disponible sur le site de la CNIL) ;
la violation est susceptible de porter atteinte aux données ou à la vie privée des personnes, mais le fournisseur a mis en place des mesures techniques de protection appropriées (article 91-3 du décret). Mises en place préalablement à la violation, ces mesures doivent avoir rendues les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (voir ci-dessous).

Que sont des mesures de protection appropriées ?
Il s'agit de toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Par exemple, le fait de chiffrer les données permet de rendre les données incompréhensibles à des tiers dans la mesure où la clé de chiffrement n'a pas été compromise.
Si le fournisseur a mis en œuvre de telles mesures de protection, il doit en informer la CNIL au moment de la notification. En effet, pour que le fournisseur puisse être dispensé d'informer les personnes, la CNIL doit d'abord constater que les mesures sont appropriées et qu'elles ont été efficacement mises en œuvre.
La CNIL a deux mois pour se prononcer sur ces mesures. En cas de silence de la CNIL, elles sont considérées comme ne répondant pas aux exigences de l'article 34 de la loi informatique et libertés et le fournisseur doit avertir les personnes.

La CNIL peut-elle imposer au fournisseur d'informer les personnes ?
Oui, la CNIL peut imposer au fournisseur d'informer les personnes si elle constate que la violation porte atteinte aux données ou à la vie privée des personnes, que les mesures de protection mises ne place n'étaient pas appropriées ou que les personnes n'ont pas été ou ont été mal informé.

Comment informer les personnes ?
L'information des personnes doit être faite par tout moyen permettant d'apporter la preuve de l'accomplissement de cette formalité (par courrier électronique, par exemple). Cette information doit contenir les éléments suivants :
• le nom du fournisseur ;
• l'identité et les coordonnées du correspondant informatique et libertés ou d'un point de contact auprès duquel les personnes peuvent obtenir des informations supplémentaires ;
• le résumé de l'incident à l'origine de la violation ;
• la date estimée de l'incident ;
• la nature et la teneur des données concernées ;
• les conséquences vraisemblables de la violation pour la personne ;
• les circonstances de la violation ;
• les mesures prises pour remédier à la violation ;
• les mesures recommandées par le fournisseur pour atténuer les préjudices potentiels.
En outre, cette information doit être rédigée dans une langue claire et aisément compréhensible. Elle ne doit pas être utilisée comme un moyen de promouvoir ou d'annoncer de nouveaux services ou être associée à d'autres informations (être mentionnée sur la facture adressée aux personnes concernées, par exemple).

Quels sont les risques pris par le fournisseur qui ne notifierait pas ?
Le fournisseur encourt des sanctions pénales car le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-17-1 du code pénal).
En outre, tout manquement à la loi informatique et libertés est passible de sanctions administratives, notamment financières pouvant aller jusqu'à 300 000 €.

En cas de violations, le fournisseur a-t-il d'autres obligations que la notification ?
Oui, il doit tenir à jour un inventaire des violations qui doit notamment contenir les modalités de la violation (ce qui s'est passé), l'effet de la violation (les conséquences) et les mesures prises pour remédier à la violation (les actions correctives mises en œuvre).
Ce recensement des violations peut être réalisé sous format papier ou numérique, et doit être conservé à la disposition de la CNIL.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.cnil.fr/linstitution/actualite/article/article/la-notification-des-violations-de-donnees-a-caractere-personnel

---

Le délit d'usurpation d'identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

Le délit d'usurpation d'identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

L'usurpation d'identité numérique n'est pas un phénomène nouveau. Ce type d'escroquerie sur internet, visant à se faire passer pour un autre (entreprise, administration) pour accéder à des données ou des comptes bancaires et détourner des fonds, ou porter atteinte à la réputation d'une entreprise ou d'une personne physique s'est développé parallèlement à l'essor de l'internet. En ces périodes troublées, le détournement de comptes bancaires pour en soutirer les fonds, ou de comptes personnels sur les réseaux sociaux à des fins de propagande par exemple, est plus que jamais un phénomène d'actualité.

Avant l'entrée en vigueur de la loi LOPPSI II, adoptée le 14 mars 2011, la victime d'une usurpation d'identité sur internet ne pouvait poursuivre l'auteur de l'infraction que sur des fondements généraux du droit pénal, tels l'escroquerie, la prise du nom d'un tiers aux fins de commission d'une infraction pénale (ex. diffamation, escroquerie), l'atteinte à un traitement automatisé de données, l'atteinte à la vie privée et l'atteinte au droit à l'image.
La LOPPSI II de 2011, qui comprend un chapitre dédié à la lutte contre la cybercriminalité, a créé une nouvelle infraction spécifique : l'usurpation d'identité numérique. [1]

La première condamnation sur le fondement de l'usurpation d'identité numérique a été prononcée par le Tribunal de grande instance de Paris le 18 décembre 2014, dans une affaire concernant la création d'un faux site web. [2]
Toutefois, la collecte des preuves, et surtout, l'identification de l'auteur du délit reste un obstacle difficile à surmonter pour la victime souhaitant engager des poursuites.
Nous analysons ci-dessous les aspects spécifiques de la notion d'usurpation d'identité numérique puis les moyens de défense dont disposent les victimes.

1. La notion d'usurpation d'identité numérique.
1.1 La définition légale.
L'usurpation d'identité est constituée quand elle porte sur l'identité même de la victime (nom, prénom, surnom, pseudonyme, identifiants électroniques) ou sur toute autre donnée de nature à l'identifier. Cette dernière expression permet de s'affranchir de la notion de données à caractère personnel, au sens de la loi Informatique et Libertés, et de rechercher tous autres éléments permettant une identification. Il est donc possible d'y inclure les adresses IP, les URL, les mots de passe, ainsi que des logos, images, voire même un avatar, tous ces éléments permettant de pointer vers une personne physique. Les juges seront amenés à interpréter et affiner cette notion et son périmètre.

L'usurpation d'identité "numérique", telle que prévue à l'article 226-4-1 al. 2 du code pénal, est commise sur un réseau de communication au public en ligne, ce qui comprend notamment les courriers électroniques, les sites web, les messages publiés en ligne et les profils en ligne sur les réseaux sociaux (Facebook, Twitter). [3]
Le préjudice effectif ou éventuel s'analyse en un trouble de la tranquillité de la personne dont l'identité est usurpée ou celle d'un tiers, ou en une atteinte à son honneur ou à sa réputation.
L'auteur de l'infraction, personne physique, encourt un an d'emprisonnement et 15.000€ d'amende. La condamnation peut atteindre 75.000€ lorsque l'auteur de l'infraction est une personne morale.

1.2 Usurpation d'identité numérique : phishing, faux sites web et faux profils.
L'usurpation d'identité numérique peut porter préjudice à deux catégories de victimes :
- la personne dont l'identité a été usurpée : l'auteur de l'infraction nuit à son image, à sa réputation, à sa marque ou trouble sa tranquillité ;
- le tiers trompé : l'auteur de l'infraction induit l'internaute en erreur et lui soutire des informations et/ou de l'argent.
L'usurpation d'identité numérique est généralement commise de deux manières : par la technique du phishing (ou hameçonnage), ou par la création d'un faux site web ou d'un faux profil sur un service de réseau social.

Le phishing ou hameçonnage
Le cyber-escroc usurpe l'identité d'un tiers, généralement une entreprise (banque, opérateur téléphonique) ou une administration, en communiquant via un faux courrier électronique et/ou via un site web contrefait. L'escroc reproduit alors les identifiants visuels et graphiques de la marque, en vue d'obtenir de la part d'internautes trompés, des informations personnelles (identifiants, mots de passe ou coordonnées bancaires). Ces informations sont ensuite utilisées pour accéder à leurs comptes et effectuer des opérations sous l'identité de l'internaute (virement, souscription d'un crédit, abonnement). [4]
Par exemple, dans un jugement rendu le 21 septembre 2005, le Tribunal de grande instance de Paris a condamné un internaute pour contrefaçon de marque et contrefaçon d'un site web. Ce dernier avait imité la page d'enregistrement du service Microsoft MSN Messenger, et sa marque figurative (le papillon MSN), pour obtenir des données personnelles des personnes au moment de leur enregistrement sur le service. [5]

La création d'un faux site web ou d'un faux profil sous l'identité d'une tierce personne
L'usurpation d'identité numérique est également réalisée via la création d'un faux site web, reprenant à l'identique les composants d'un site "légitime" (charte graphique, reproduction de tout ou partie du contenu, etc.). Cette technique est souvent liée à une "campagne" de phishing.
La création d'un faux site web ou d'un faux profil a pour objet ou pour effet de porter atteinte à l'honneur ou à la réputation du titulaire du site ou du profil, personne physique ou morale.

1.3 Le jugement du 18 décembre 2014.
Le Tribunal de grande instance de Paris a rendu un premier jugement le 18 décembre 2014 condamnant l'auteur d'une usurpation d'identité numérique sur le fondement de l'article 226-4-1 du Code pénal.
Dans cette affaire, un informaticien avait créé un faux « site officiel » de la députée-maire Rachida Dati. Le faux site reprenait la photo de Rachida Dati ainsi que la charte graphique du site officiel et permettait aux internautes de publier des commentaires sous la forme de communiqués de presse, soi-disant rédigés par Rachida Dati, mais au contenu trompeur. L'internaute se trouvait en réalité sur le site officiel, très similaire au faux site. L'auteur de cette usurpation avait utilisé une faille de sécurité du site de la députée-maire, permettant d'y injecter du code indirect (opération dite « XSS » ou cross-site scripting).

Le directeur du Cabinet de Madame Dati a déposé plainte contre X pour usurpation d'identité sur support numérique et atteinte aux systèmes de traitement automatisé de données. L'enquête, menée par la BEFTI (Brigade d'enquête sur les fraudes aux technologies de l'information), a permis d'identifier l'auteur des agissements.

Dans un jugement du 18 décembre 2014, le TGI de Paris a retenu les deux chefs d'accusation à l'encontre du prévenu. Le Tribunal considère en effet, que l'identité de Madame Rachida Dati avait été numériquement usurpée, dans la mesure où "ces mentions ["je vous offre un communiqué… » ou "merci pour ce geste citoyen "], aux côtés du nom de Madame Rachida Dati et sur un site reprenant la photographie officielle de la députée-maire, sa mise en page et sa charte graphique, ne peut que conduire l'internaute à opérer une confusion avec le site officiel de celle-ci".

Par ailleurs, le Tribunal a retenu que l'auteur du faux site avait mis en place un dispositif permettant la mise en ligne par les internautes de faux communiqués au contenu sexiste et dégradant. Or, en sa qualité de modérateur du site, il avait la possibilité de fermer son site ou de désapprouver les termes des commentaires mis en ligne par les internautes.

Le prévenu a également été considéré coupable d'introduction frauduleuse de données dans un système de traitement de données, du fait d'avoir exploité la faille de sécurité du site officiel pour y introduire des instructions dans le but d'en modifier son comportement. L'ensemble de ces éléments entraînant la confusion avec le site officiel de la femme politique, l'internaute a été reconnu coupable d'usurpation d'identité numérique. Condamné à une amende de 3.000€, l'auteur du faux site a fait appel de la décision.
Le fournisseur d'hébergement a quant à lui été reconnu complice de cette infraction.

2. Les moyens de défense à la disposition des victimes.
2.1 Pour la personne usurpée.
Face à ce type d'agissement, il est possible de prendre des mesures proactives, ou en cas de constatation d'une infraction, de prendre des mesures en réaction.
Les institutions fournissent des recommandations, proactives – concernant la sécurité des comptes personnels, et réactives – concernant les mesures de retrait de contenu ou de dépôt de plainte.
L'Hadopi (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet) fournit une série de recommandations aux fins d'éviter l'usurpation d'identité numérique. Ces recommandations, qui relèvent souvent du bon sens, consistent notamment, à utiliser des mots de passe complexes et de ne pas les communiquer à des tiers, activer les protections anti-phishing existant dans certains navigateurs web, éviter de se connecter sur des sites sensibles (sites de banques ou de vente en ligne) dans les lieux publics ou chez des tiers, ne pas répondre à des emails provenant de prétendus organismes de confiance et demandant de communiquer mots de passe ou autres coordonnées personnelles confidentielles, ne jamais cliquer sur les liens ni ouvrir les documents contenus dans ces messages, etc. [6]
Si des informations d'identification ont été publiées sans autorisation et/ou détournées, le responsable du site sur lequel ces informations ou données sont publiées doit être contacté pour en demander leur suppression. A cet effet, la CNIL (Commission nationale de l'informatique et des libertés) propose sur son site des modèles de courriers pour formuler cette demande. [7] A défaut de réponse, il conviendra alors de porter plainte en ligne via le site de la CNIL.
La Commission aide ainsi à la suppression des informations détournées et à la récupération de l'accès à sa messagerie électronique. [8]

2.2 Les moyens de preuve à l'appui d'une action en usurpation d'identité numérique
La difficulté à identifier l'auteur de l'infraction.
Il existe encore peu de décisions judiciaires condamnant ces pratiques. La victime se heurte en effet à deux difficultés majeures : l'identification des auteurs de l'escroquerie, rendue difficile notamment à cause des procédés d'anonymisation ; et la localisation de l'auteur. Lorsqu'il est possible de remonter jusqu'à l'auteur, celui-ci est souvent situé à l'étranger, rendant les poursuites difficiles et la procédure coûteuse.
Comme mentionné ci-dessus, la victime d'une usurpation d'identité numérique peut adresser une plainte à la CNIL. Elle peut également porter plainte soit auprès des forces de l'ordre (police ou gendarmerie), soit directement auprès du procureur de la République.

Afin que l'affaire ne soit pas classée sans suite, il est fortement recommandé de fournir des éléments de preuve remontant jusqu'à l'auteur de l'infraction. A cette fin, la victime peut contacter le fournisseur d'accès à internet ou le fournisseur d'hébergement afin d'obtenir la communication des données permettant d'identifier l'auteur de l'infraction.

Les moyens de preuve. Afin de faciliter l'identification des auteurs d'une infraction, la loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN), impose aux prestataires techniques, fournisseurs d'accès à internet et hébergeurs, la conservation des données "de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles (ces personnes) sont prestataires" (article 6 II). [9]
Ainsi, à la demande de l'autorité judiciaire, FAI et hébergeurs doivent transmettre toute information en leur possession, nécessaire à la constitution du dossier, dans le respect des délais de prescription. Il est à noter cependant que, suivant les catégories de données concernées, différents délais de prescription s'appliquent. Ainsi, les données de connexion ne seront conservées que pendant un an.
Par ailleurs, il peut être utile de faire établir un constat d'huissier afin de conserver la preuve des écrans, pages web et autres éléments à l'appui des poursuites.

Une infraction "autonome"
Depuis la LOPPSI II, le délit d'usurpation d'identité numérique est une infraction autonome. Ainsi, le seul fait de commettre un acte de phishing, même sans accès effectif aux comptes dont les données ont été récupérées, est suffisant pour être qualifié d'acte d'usurpation d'identité numérique. Il n'est donc pas obligatoire de rapporter la preuve selon laquelle l'usurpation a été commise en vue de la réalisation d'une infraction (telle que le détournement de fonds ou l'apologie du terrorisme par exemple).
Le législateur exige cependant un dol spécial : l'accusation doit rapporter la preuve que l'usurpateur a agi en vue de troubler la tranquillité de la personne dont l'identité est usurpée ou de celle d'un tiers, ou afin de porter atteinte à son honneur ou à sa considération.
Toutefois, le législateur n'impose pas de prouver une répétition des agissements fautifs, alors que la rédaction initiale de l'article 226-4-1 al. 2 dans le projet de loi LOPPSI II avait prévu une condition de réitération.
Une infraction "instantanée". L'usurpation d'identité numérique étant un délit, la victime dispose d'un délai de prescription de trois ans pour agir. Le délit d'usurpation d'identité numérique est une infraction instantanée : le point de départ du délai de prescription se situe au jour où l'identité a été usurpée.
Cependant, comme mentionné plus haut, il convient d'agir sans attendre. En effet, selon les catégories de données concernées, différents délais de prescription peuvent avoir pour conséquence que certaines d'entre elles ne seront plus disponibles au moment de la constitution du dossier.

Betty SFEZ
Avocat au Barreau de Paris
Deleporte Wentz Avocat
http://www.deleporte-wentz-avocat.com/

En savoir plus sur http://www.village-justice.com/articles/Delit-usurpation-identite,18790.html
Par Betty Sfez, Avocat

[Notes]
[1] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
[2] TGI Paris, 13e ch. corr., 18 décembre 2014, MP c/ X.
[3] Art. 226-4-1 du code pénal : "Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne."
[4] Les auteurs de l'escroquerie utilisent régulièrement la technique du "social engineering", ou ingénierie sociale, méthode de manipulation abusant de la crédulité de personnes, afin qu'elles divulguent des données confidentielles.
[5] TGI Paris, 31e ch. corr., 21 septembre 2005, Microsoft Corporation c/ Robin B.
[6] Fiche Hadopi relative aux moyens de sécurisation : Identité numérique/Usurpation d'identité publiée en décembre 2011, accessible à : http://www.hadopi.fr/sites/default/files/page/pdf/UsurpationIdentite.pdf.
[7] Accessibles sur le site de la CNIL à : http://www.cnil.fr/vos-droits/les-courriers-pour-agir/
[8] Voir http://www.cnil.fr/vos-droits/plainte-en-ligne/ et http://www.cnil.fr/vos-droits/la-cnil-a-vos-cotes/
[9] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).