La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende

La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende

Pourtant hostile au départ, le gouvernement est désormais favorable à un renforcement du pouvoir de sanction de la Cnil : jusqu'à 20 millions d'euros en cas de récidive. Et la portabilité des données ? « Ce sont les gros qui sont énervés » répond Axelle Lemaire.

Le projet de loi République numérique présenté par Axelle Lemaire est actuellement débattu par les députés. De nombreux amendements sont à l'étude, dont certains rejetés par le gouvernement. Celui-ci s'est en revanche rallié à une proposition des parlementaires en faveur d'un renforcement du pouvoir de sanction de la Cnil, l'autorité en charge de la protection des données personnelles.
Selon Les Echos, le gouvernement soutient donc désormais un amendement prévoyant, en cas de récidive, de permettre à la Cnil d'infliger une sanction pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. A ce jour, en cas de récidive, la sanction ne peut pas dépasser les 300.000 euros.

Les « gros » sont « énervés »

Une autre mesure portant sur les données fait grincer des dents au sein de plusieurs organisations d'entreprises du numérique : la portabilité des données entre plateformes.
« Par son caractère large, il impose des contraintes extrêmement lourdes à des secteurs dans lesquels la portabilité n'apporte pas d'intérêt du point de vue des consommateurs et sur le plan de la concurrence. En l'état, il menace directement les investissements massifs réalisés par les entreprises du secteur afin d'améliorer leurs services » dénonçaient-elles notamment dans un communiqué du 14 janvier.
Message reçu au sein du gouvernement ? Difficile à dire puisque la ministre du numérique déclarait lundi 18 janvier sur RMC vouloir « protéger la concurrence ». « Ce sont les gros qui sont énervés, pas les petits » ajoutait-elle.

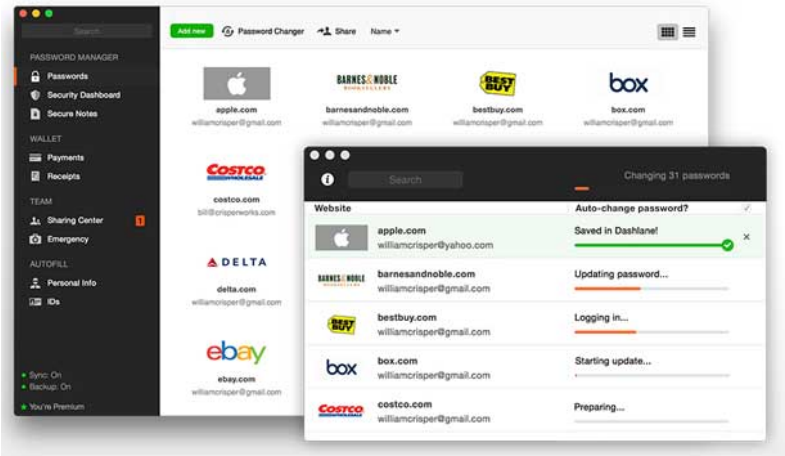
Réagissez à cet article

Source : *La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende*

Dashlane : 500 mots de passe modifiés en un clin d’oeil

Dashlane : 500 mots de passe modifiés en un clin d’oeil

La nouvelle version de l'outil français des gestion des mots de passe propose d'automatiser la gestion des mots de passe. De quoi soulager des utilisateurs toujours plus sollicités sur le terrain de la sécurité.



La multiplication des services en ligne fait exploser le nombre de mots de passe utilisés par les professionnels. Au point de poser des problèmes de mémoires insolubles. Google réfléchit à les remplacer grâce au smartphone.

Dashlane propose le changement automatique de mot de passe pour 500 sites Web. (Source : Dashlane)

La pépite Dashlane propose elle une alternative au stockage manuel de plusieurs mots de passe en automatisant le stockage et la modification des mots de passe. Et la dernière version de l'outil permet de le faire pour 500 sites (au lieu de 75 jusqu'alors) et services web en un seul clic, avec la fonctionnalité Password Changer.

Banque et mot de passe

8 formats de documents sont désormais pris en charge : les applications, les bases de données, les documents financiers, les documents juridiques, les abonnements, les licences logicielles et les mots de passe Wi-Fi. Autres nouveautés de cette quatrièmes version de Dashlane, 7 langues différentes sont supportées et l'interface graphique a été revue de mnière à être identique quelque soit la plateforme (Mac, PC, iOS et Android). Autre amélioration, un moteur de recherche plus performant et un affichage des résultats sous divers formats.

Côté moyen de paiement, 618 nouvelles banques internationales peuvent être utilisées dans les moyens de paiement. A noter que la version de base de Dashlane est proposées gratuitement, et que la version Premium 39,99 euros/an) permet de synchroniser les données sur mobile (nombre illimité d'appareils) et de les sauvegarder en mode sécurisé.

Réagissez à cet article

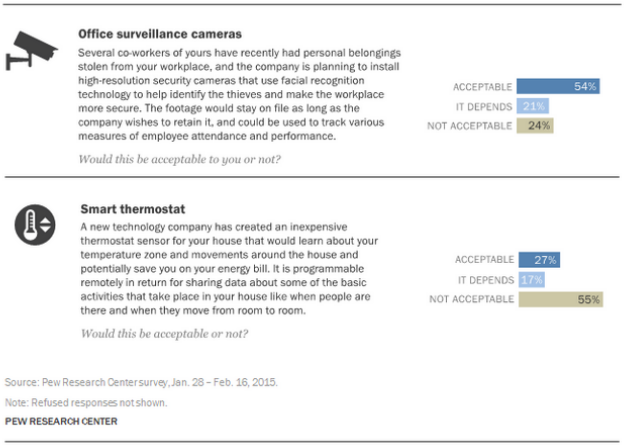
Source : *Dashlane : 500 mots de passe modifiés en un clin d'oeil*

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*

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…

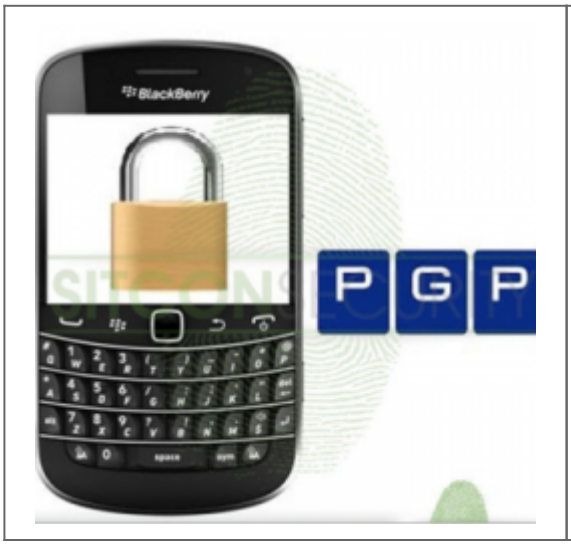
D'autres amendements concernant la CNIL ont en revanche été adoptés. L'autorité administrative pourra par exemple être consultée par le président de l'Assemblée nationale ou du Sénat sur une proposition de loi, sauf si le parlementaire à l'origine du texte s'y oppose. La gardienne des données personnelle 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*

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.

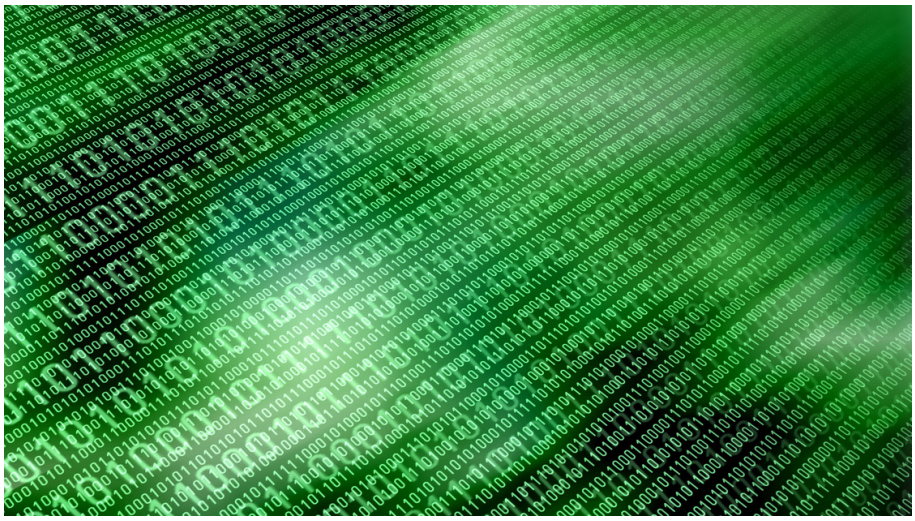
Réagissez à cet article

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

Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

	Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

Le Département des Alpes-Maritimes ,1er organisme français à obtenir le Label Gouvernance Informatique et Libertés de la CNIL.



Le Département a depuis longtemps intégré le numérique comme nouvelle dimension de la vie de l'usager. Il s'est ainsi engagé formellement dans le respect du droit des personnes au travers de la mise en oeuvre d'un cadre de confiance autour de l'économie numérique en établissant une politique de gestion des données à caractère personnel. Un engagement récompensé au niveau national pour la première fois en France.
Le 22 octobre 2015, la CNIL a délivré au Département des Alpes-Maritimes le premier Label Gouvernance Informatique et Libertés tous secteurs confondus. L'obtention de ce label vient récompenser le travail des services départementaux, ainsi que l'attachement éthique du Département à la protection des données relatives aux usagers ou à celles de ses agents.
Cette distinction et les bonnes pratiques qui en découlent, illustrent ainsi, à juste titre, le comportement responsable et loyal que la collectivité a engagé en matière de réalisation et d'exploitation des données à caractère personnel.
Le Lab 06 a ouvert ses portes le 25 septembre 2015 au cœur du Centre administratif départemental. Il incarne la volonté du Département des Alpes-Maritimes de s'engager davantage dans la voie de la transformation numérique avec la création de #E-zy06 dont l'ambition est d'offrir un service public encore plus accessible quelle qu'en soit la modalité : physique, téléphonique ou numérique.
L'objectif est de faire des Alpes-Maritimes un département pionnier dans le numérique, capable d'apporter le plus grand service aux usagers.

Réagissez à cet article

Source : *La politique départementale de sécurité des données personnelles saluée par la CNIL – Département des Alpes-Maritimes*

Comment protéger les données de vos enfants des pirates informatiques

Comment protéger les données de vos enfants des pirates informatiques

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Après l'annonce du piratage début novembre de VTech, le leader mondial des tablettes ludo-éducatives, c'est maintenant au tour d'Hello Kitty d'être accusée de mal sécuriser les données de ses utilisateurs. Pendant près d'un mois, les données personnelles de 3,3 millions de membres de la communauté en ligne du fabriquant japonais Hello Kitty (dont, évidement, beaucoup d'enfants) auraient été exposées en raison d'une faille de sécurité.

A quelques jour de Noël, ces deux affaires montrent clairement à quel point il est facile aujourd'hui pour les hackeurs de dérober des informations sensibles.Et aussi le danger qui peut en découler, comme le rappelle à metronews la Commission nationale de l'informatique et des libertés (CNIL) : « Nous constatons que certains secteurs industriels ajoutent une connectivité à leurs produits sans disposer historiquement d'une culture en sécurité informatique ».

► Vérifiez si votre mail est piraté
Il existe un moyen simple de savoir si votre adresse mail a été touchée. Pour cela, il faut se rendre sur le site haveibeenpwned.com. Entrez votre adresse mail, puis cliquez sur « pwned ? » pour lancer la recherche.
► Changez votre mot de passe
Par précaution, il est recommandé aux utilisateurs des services qui ont connu des intrusions de ce genre de changer leurs mots de passe. « Il doit être composé d'au moins 3 types de caractères différents parmi les quatre types de caractères existants : majuscules, minuscules, chiffres et caractères spéciaux ». Pour en savoir plus, rendez-vous sur le site de la CNIL.
► Ne communiquez que le minimum d'infos
Pour les enfants (et leurs parents), la CNIL recommande ainsi d'utiliser des pseudonymes sur les services en lignes, et de ne communiquer que le minimum d'informations. Par exemple, saisissez une date de naissance au 1er janvier si le système a besoin d'une indication de tranche d'âge.
► Veillez à bien lire les conditions d'utilisation
Outre les risques de sécurité révélés par la faille VTech, les parents doivent être vigilants concernant les possibilités de réutilisation des données collectées (profilage publicitaire) et s'assurer de la possibilité d'y accéder et de les supprimer.

Réagissez à cet article

Source : *Piratages VTech et Hello Kitty : comment protéger les données de vos enfants – metronews*

FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

	**#FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données**

Pendant longtemps, la sécurité des données se confondait avec celle de la sécurité des systèmes d'information. Or la décorrélation croissante entre le contenant (support physique ou applicatif) et le contenu en raison de l'émergence des technologies de virtualisation, du « cloud computing » et de nouveaux modèles économiques change aujourd'hui la donne. La donnée est devenue un « objet » à part entière qui s'appréhende indépendamment de son support.

Axe 1 : les données, carburant de la transformation numérique.

Les données sont omniprésentes et multiformes : on peut citer les données personnelles, sociales, médicales, bancaires, d'entreprises, de géolocalisation, de sécurité, de dossiers passagers (PNR) etc. Cette compartimentation en fonction des usages ou des secteurs d'activité a-t-elle cependant encore un sens ? Comment gérer l'information indépendamment des supports utilisés ? Au-delà de la métaphore, les données constituent-elles véritablement un « nouvel or noir » ?

Axe 2 : la maitrise des données, enjeu de souveraineté

Posséder une « industrie de la donnée » puissante est un atout essentiel dans la compétition mondiale et une composante importante de toute stratégie de puissance. Or l'Europe apparait de ce point de vue en net retrait par rapport aux Etats-Unis. Forte consommatrice de numérique, la faiblesse de son offre locale la conduit à exporter massivement ses données, principalement aux Etats-Unis. Comment passer d'une « Europe offerte » à une Europe « ouverte » ? Quelle est la situation des autres continents ? Peut-on parler de « géopolitique des données » ?

Axe 3 : les données, un capital menacé

Si les attaques en déni de service visent les infrastructures elles-mêmes, les données sont souvent l'objectif ultime des attaquants, qu'il s'agisse de cybercriminalité (vol d'information, crypto-locking…) ou d'espionnage. Quelles sont les dernières tendances observées ? Quels sont les modes opératoires des cybercriminels ? Comment calculer la valeur de ses données pour engager des poursuites ?

Axe 4 : droit et données

La donnée est une notion immatérielle qui soulève de nombreuses questions au plan juridique. Peut-on appliquer la notion de propriété à la donnée, notamment à la donnée personnelle ? Quel lien entre données et territoire ? Comment mettre en œuvre efficacement le droit à l'oubli aujourd'hui consacré dans certains pays ? Comment définir le vol de données au plan pénal ?

Axe 5 : quelles stratégies de sécurité des données pour l'entreprise ?

Pour les entreprises, la sécurité des données repose sur une approche globale impliquant : classification des données, évaluation des données, analyse de risques, définition et mise en œuvre d'une stratégie de sécurité. Le développement du cloud computing et l'externalisation croissante de l'IT soulèvent à cependant de nombreuses questions. Peut-on utiliser « en toute sécurité » un CRM ou un ERP dans le Cloud ? Quelles conséquences en termes de maîtrise des données ? Comment assurer les risques liés aux données ?

Axe 6 : quelles technologies pour sécuriser les données ?

Le responsable sécurité des systèmes d'information dispose aujourd'hui d'une vaste bibliothèque d'outils et de technologies lui permettant de sécuriser ses données, qu'il s'agisse d'outil de protection, de destruction sécurisée, de détection de fuites d'information ou d'investigation. La vitesse du progrès technologique et le « time to market » imposé par le marché aux éditeurs sont-elles compatibles avec les cycles d'adoption relativement lents des organisations ? Compte tenu de ce même « time to market », comment intégrer la sécurité de façon native (security by design) dans les applications à disposition des utilisateurs ?

Axe 7 : données et enjeux sectoriels

La transformation numérique et les données qui la nourrissent irriguent l'ensemble des secteurs économiques et des activités humaines. Les données sont ainsi au cœur de la « smart revolution » qui touche aussi bien l'individu dans sa vie quotidienne, la collectivité ou l'entreprise au travers des objets connectés et de « l'informatique omniprésente ». Quels sont les enjeux liés aux données dans la « ville intelligente », « l'usine du futur », le monde médical etc. ?

Axe 8 : enjeux sociétaux et éthiques liés aux données.

La transformation numérique, et la croissance exponentielle des données qu'elle génère, constituent à n'en pas douter des opportunités. Mais la rapidité de cette évolution et ses conséquences majeures sur l'Homme militent également pour une certaine prise de recul et un questionnement éthique et philosophique. Au plan individuel, que signifie désormais la notion de « vie privée » ? Est-il également possible de replacer l'utilisateur au cœur de cette transformation en lui permettant de se réapproprier « ses » données ? Faut-il enfin imaginer, sur le modèle de la loi bioéthique, une loi sur l'éthique numérique fixant un cadre pour l'exploitation des données à des fins prédictives ou à des fins de surveillance ?

Réagissez à cet article

Source : *Le FIC 2016 aura lieu les 25 et 26 janvier 2016 sur le thème de la sécurité des données | Observatoire FIC*

Les entreprises françaises bientôt condamnées à changer leur système de traitement des donnée personnelles ?

Les entreprises Françaises bientôt condamnées à modifier leur système de traitement des données personnelles ?

L’échéance se rapproche dangereusement. A partir de la fin du mois de janvier, entreprises américaines et européennes ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Le 6 octobre 2015, la Cour de justice européenne a en effet rendu une décision invalidant le « Safe Harbor », ce traité transatlantique sur le transfert des données personnelles. Premiers touchés, les géants américains du numérique, comme Facebook, Google ou Microsoft, qui exploitent massivement les donnes personnelles.

Qu’en est-il des entreprises françaises qui, sans toujours le savoir, communiquent les données personnelles de leurs clients. De leurs salariés, de leurs contacts… sur des serveurs aux États Unis ? (Gmail, DropBox, Google Drive…)

A partir de la fin du mois de janvier, les entreprises américaines et européennes, et donc françaises, ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Vous avez des doutes, vous souhaitez être accompagné ?
contactez-nous

Réagissez à cet article

Source : *Fin du « Safe Harbor » : Gattaz tire la sonnette d’alarme*