Données personnelles : mais à quoi sert la CNIL ? – Cash Investigation ce mardi 6 octobre 2015 | Le Net Expert Informatique

Données personnelles : mais à quoi sert la CNIL ? – mardi 6 octobre 2015

Certaines associations caritatives vendent en toute illégalité leurs fichiers de donateurs à La Poste. Face à Elise Lucet, la présidente de la CNIL ne semble pas au courant et se déclare « surprise ». Un extrait de « Cash Investigation » diffusé sur France 2 le mardi 6 octobre à 20h55. Lire la suite….
Ci-dessous, le rapport d'activité 2014 de la CNIL dont il est fait mention dans le reportage (Merci à Eric EGÉA) :
http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-35e_rapport_annuel_2014.pdf.pdf

---

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.francetvinfo.fr/internet/cash-investigation-donnees-personnelles-mais-a-quoi-sert-la-cnil_1109973.html

Il est nécessaire d’éduquer et de former les élèves à la cybersécurité ! | Le Net Expert Informatique

Il est nécessaire d’éduquer et de former les élèves à la cybersécurité !

Il est désormais du devoir des institutions et de l'Éducation nationale d'encadrer les plus jeunes afin de les aider à devenir des citoyens numériquement responsables.

À l'occasion du mois européen de la cybersécurité, qui se tiendra en octobre, il est primordial de penser à faire évoluer les pratiques d'Internet des jeunes Français et de leur en inculquer les bases d'un usage sécurisé. C'est un fait, aujourd'hui les enfants de 9 à 16 ans utilisent quasiment tous Internet (93 %), et ce malgré les risques qu'il comporte (1).

Avec l'arrivée des objets connectés (smartphones, tablettes, accessoires, etc.) pouvant s'avérer être, pour certains individus parmi les plus jeunes, une réelle addiction, les cyber-risques ne cessent de croître. La formation de nos chères têtes blondes à devenir des utilisateurs responsables d'Internet et à être au fait de ses enjeux de sécurité ne doit pas seulement se limiter à celles des parents, les institutions et l'Éducation nationale doivent également y participer.

L'importance de différents niveaux d'apprentissage de la cybersécurité

Les écoles sont comme une seconde maison pour les enfants, où les enseignants viennent complémenter les parents en termes de connaissances, d'enseignement et de discipline. Voilà pourquoi l'École apparaît tout naturellement comme une bonne option pour dispenser une véritable éducation en matière de cybersécurité.

Aujourd'hui, une telle contribution est vitale dans la préparation des enfants au monde virtuel. Des sujets tels que la cyber-civilité, la cyber-image, la cyber-hygiène et la cybersécurité pourraient, par exemple, être mieux appréhendés et expliqués dans une salle de classe. Or, à ce jour, la plupart des écoles n'offrent seulement qu'un bref aperçu de ce qu'est la cybersécurité.

Bien entendu, l'enseignement de la sécurité du « cyber-life » se doit de différer en fonction de l'âge de l'élève, mais quelques règles de base sont communes à tous afin de mieux les prémunir dans le cadre de leurs interactions tant dans leur vie sociale que digitale !

Pour les plus jeunes, c'est au moment où l'intérêt des enfants pour l'univers digital est minime qu'il faut les sensibiliser à la cybersécurité. Des règles et enseignements simples pourraient être inculqués comme leur apprendre à demander l'autorisation à leurs parents avant d'utiliser un appareil, être sensibilisé à la dangerosité de communiquer avec des personnes inconnues sur le Net ou encore la nécessité de prévenir ses parents en cas d'échange bizarre sur le Net, etc.

Quant aux préadolescents, la cyberéducation doit intervenir au moment où ils commencent à jouer en ligne, à regarder des vidéos sur le Net, à créer leur propre compte sur les réseaux sociaux, etc. Afin qu'ils puissent surfer en toute sécurité, il est primordial de leur enseigner quelques bases de sécurité par exemple l'importance de créer un mot de passe efficace et sécurisé, la manière de reconnaître un site/une application sûr(e), les risques de vol existant en ligne, les dangers du téléchargement et du partage de contenu personnel sur le Web, etc.

Vient ensuite la période de l'adolescence, où les jeunes aiment se retrouver et échanger sur des sites Internet communautaires au sein desquels le risque de partage d'informations personnelles et d'interaction avec des inconnus est omniprésent. L'adolescence se présente également comme une période au cours de laquelle il faudrait renforcer l'apprentissage des adolescents en termes de pratiques éthiques, de reflet d'image, de sûreté et de sécurité des outils, etc., l'idée étant de faire des adolescents des citoyens numériques responsables et conscients de dangers que représente la Toile (addiction, hacking, phishing, cyberharcèlement, etc.).

Espérons que les actions menées par les associations et les professionnels concernés à l'occasion du mois européen de la cybersécurité s'imposent comme un détonateur dans la prise de conscience des politiques et de l'Éducation nationale quant à la nécessité de l'apprentissage numérique des plus jeunes afin de mieux protéger et sécuriser les individus et le monde de demain.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lesechos.fr/idees-debats/cercle/cercle-140152-il-est-necessaire-deduquer-et-de-former-les-eleves-a-la-cybersecurite-1160311.php?XMmKySpwheCXjjJG.99

Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique | Le Net Expert Informatique

Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique

Windows 10 est disponible gratuitement pour les PC sous Windows 7 ou Windows 8.1. Il propose des changements face à ses prédécesseurs dont certains touchent à la surveillance, l'analyse et la collecte de données personnelles concernant ses utilisateurs. La CNIL met en garde et propose un tutoriel pour se protéger des yeux indiscrets de la firme.

En France, la CNIL a rapidement réagi devant les nombreux systèmes de surveillance et de collecte de données accompagnant Windows 10. Dans un dossier mis en ligne quelques jours seulement après le lancement de l'OS, elle propose « quelques réglages de confidentialité qui permettent de limiter la communication de vos informations à l'éditeur et à ses partenaires ».

Windows 10, des fuites dans Cortana, Microsoft Edge ou encore la synchronisation

Ils se concentrent sur trois thèmes, Cortana avec un paramétrage de la » vie privée « , la synchronisation des comptes sur les autres appareils utilisés et le navigateur Microsoft Edge.

Elle recommande ainsi de désactiver la géo-localisation, d'empêcher la collectes de données liées à l'Appareil photo, le Microphone, les Informations de Compte, des Contacts, du Calendrier, de la Messagerie, des communications Radio ou encore d'agir sur la fonctionnalité » apprendre à me connaître » pour la dictée vocale. Au sujet du nouveau navigateur, Microsoft Edge, il est recommandé de désactiver l'option » Utiliser la prédiction de page pour accélérer la navigation, et améliorer le mode lecture ainsi que mon expérience globale » puisque celle-ci requiert d'envoyer votre historique de navigation tandis l'obtention de suggestions de recherche demande qu'une grande partie des informations que vous saisissez dans la barre de navigation soit envoyée au moteur de recherche Bing. Il est donc recommandé de désactiver « Afficher les suggestions de recherche à mesure que je tape « .

Vous trouverez ici, un pas à pas complet pour reprendre la main sur vos données personnelles : Régler les paramètres vie privée de Windows 10

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.ginjfo.com/actualites/logiciels/windows-10/windows-10-et-sa-vie-privee-la-cnil-met-en-garde-et-une-fiche-pratique-20150928

Panne de Facebook ? La carte des dysfonctionnements | Le Net Expert Informatique

Panne de Facebook ? La carte des dysfonctionnements

Facebook est un réseau social en ligne sur internet. Il permet de publier des informations (photos, liens, textes) en contrôlant la visibilité.
Il est aujourd'hui le réseau social le plus populaire. Fondé en 2004 par Mark Zuckerberg, le site est devenu incontournable au fil des années.

Les statistiques d'usages sont ahurissantes :
Utilisateurs actifs mensuels (MAU, juillet 2015) : 1,49 milliard
En Europe : 3011 millions
En Amérique du Nord : 213 millions
En Asie : 496 millions
Dans le reste du monde : 471 millions
En France : 30 millions d'utilisateurs

Utilisateurs actifs mensuels sur mobile : 1,314 milliard.
En France : 24 millions d'utilisateurs
Utilisateurs actifs mensuels uniquement sur mobile : 655 millions.
Utilisateurs actifs quotidiens (DAU) : 968 millions

Ainsi, une panne de Facebook de quelques minutes, ou plus comme celles passées en Octobre 2015, impactera des utilisateurs de toute la planète.
Lien vers la carte des pannes de Facebook

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://touteslespannes.fr/statut/facebook/carte/

Quinze millions de clients T-Mobile victimes d'un piratage | Le Net Expert Informatique

Quinze millions de clients T-Mobile victimes d'un piratage

Des cyberpirates ont dérobés les données personnelles de 15 millions d'abonnés de l'opérateur de téléphonie T-Mobile. Le piratage a ciblé son prestataire Experian, spécialisé dans la relation client et l'analyse du risque de crédit. Le butin comprend notamment des noms, adresses, dates de naissance ainsi que des numéros de sécurité sociale.

L'opérateur T-Mobile et Experian, son prestataire chargé de vérifier la solvabilité ont annoncé qu'un piratage massif avait permis à des cybercriminels de dérober les données personnelles de quelques 15 millions de clients. Évoquant une "acquisition d'information non autorisée" depuis l'un de ses serveurs, Experian a révélé qu'il s'agit de données sensibles telles que des noms, adresses, dates de naissance, numéros de sécurité sociale, numéros de passeport ou de permis de conduire ainsi que des informations relatives aux évaluations des emprunteurs. L'intrusion s'est produite entre le 1er et le 16 septembre.

Dans un message adressé à ses clients, John Legere, le P-dg de T-Mobile, assure que les données bancaires n'ont pas été exposées. Il a également annoncé que tous les clients concernés avaient droit à un abonnement de deux ans à un service de surveillance et protection en cas d'usurpation d'identité et de fraude.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.zdnet.fr/actualites/quinze-millions-de-clients-t-mobile-victimes-d-un-piratage-39825840.htm

Les sites Web du gouvernement thaïlandais attaqués | Le Net Expert Informatique

Les sites Web du gouvernement thaïlandais attaqués

Plusieurs sites gouvernementaux thaïlandais ont été la cible, dans la nuit de mercredi 30 septembre à jeudi 1er octobre, d'attaques dites de « déni de service », qui les ont rendus inaccessibles pendant plusieurs heures. Ce type d'attaque, appelée DDoS, consiste à multiplier les requêtes inutiles sur un site afin de le saturer. Parmi les sites visés, celui du gouvernement, du ministère de l'information et du ministère de la défense. Certains étaient encore difficiles d'accès jeudi matin.

Ces attaques sont généralement automatisées, mais mercredi, des appels à surcharger ces sites ont été relayés sur les réseaux sociaux, incitant les internautes à s'y connecter et à rafraîchir les pages au maximum. Objectif : dénoncer les projets du gouvernement sur l'avenir d'Internet.

« Grande muraille »

Les Thaïlandais s'inquiètent en effet de la censure grandissante exercée par la junte militaire au pouvoir sur Internet, qui a amplifié sa politique de censure, et multiplié les poursuites contre les internautes ayant émis des critiques sur la famille royale.

L'inquiétude est montée d'un cran la semaine dernière, après l'annonce discrète, sur un site gouvernemental, d'un projet de mise en place d'une gateway (« passerelle ») unique. Une gateway est une sorte de porte d'entrée permettant à un pays de se connecter au réseau mondial. La Thaïlande en possède actuellement une dizaine, gérées par des opérateurs publics ou privés. Se limiter à une seule gateway, opérée par la junte, pourrait faciliter la surveillance et la censure, dénoncent les détracteurs du projet.

Ceux-ci ont réussi à réunir plus de 130 000 signatures sur une pétition en ligne contre ce projet surnommé « Great firewall of Thaïlande », en référence au Great firewall of China, cette « Grande Muraille » de l'Internet érigée en Chine.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.lemonde.fr/pixels/article/2015/10/01/les-sites-web-du-gouvernement-thailandais-attaques-pour-protester-contre-la-censure_4779521_4408996.html

---

La surveillance

internationale de masse refait surface | Le Net Expert Informatique

La surveillance internationale de masse refait surface

Après la censure partielle de la très contestée loi sur le renseignement, qui a été validée dans sa quasi-totalité par le Conseil Constitutionnel le 23 juillet dernier, la surveillance des communications internationales refait surface sous la forme d'une proposition de loi. En laissant au parlement le soin de présenter un texte rustine, le gouvernement agit à distance (ni projet de loi, ni étude d'impact) pour autoriser et encadrer la surveillance massive. Ce jeudi 1er octobre 2015 à l'Assemblée nationale, l'examen en séance publique du texte a débuté.

Compléter la loi sur le renseignement

La procédure est accélérée… Le texte relatif aux mesures de surveillance des communications électroniques internationales est présenté par les députés SRC Patricia Adam et Philippe Nauche de la Commission de la défense nationale et des forces armées de l'Assemblée. Ce texte prévoit la création d'un « cadre spécifique » à la surveillance des communications internationales (soit l'émission ou la réception d'une communication depuis l'étranger). Pour ses promoteurs, les services de renseignement français doivent pouvoir assurer, dans un cadre légal, cette surveillance « aux fins de défense et de promotion des intérêts fondamentaux de la Nation ».

Les « correspondances » (contenus) et les « données de connexion » (métadonnées) sont incluses dans la proposition. Par ailleurs, à la différence des interceptions de sécurité, les autorisations de surveillance délivrées par le Premier ministre « ou l'un de ses délégués », ne seront pas soumises à l'avis préalable de la Commission nationale de contrôle des techniques de renseignement (CNCTR). De plus, l'article 1er du texte, qui modifie le chapitre IV du titre V du livre VIII du code de la sécurité intérieure, « autorise l'exploitation non-individualisée des données de connexion interceptées ». La Commission de la défense a repoussé, mercredi 30 septembre, tous les amendements proposés par les députés Les Républicains Laure de La Raudière et Lionel Tardy et par l'écologiste Sergio Coronado (avec d'autres parlementaires). Seuls les amendements de forme ont été conservés.

Prévoir des exceptions… limitées

Amnesty International condamne un texte aux « motifs vastes et peu précis » qui « légalise la surveillance de masse », sans voie de recours. La surveillance à grande échelle, déjà présente dans la loi renseignement du 24 juillet 2015, ne viserait plus seulement l'antiterrorisme mais pourrait « être justifiée pour l'ensemble des finalités mentionnées à l'article 811-3 de la Code de la sécurité intérieure, y compris la défense et la promotion des intérêts majeurs de politique étrangère, économique et scientifique».

Une organisation, une entreprise ou un particulier qui communiquerait en France avec l'étranger ou recevrait une communication émise depuis l'international, pourrait donc tomber sous le coup de cette loi. Seuls les parlementaires, les magistrats, les avocats ou les journalistes qui exercent en France, pourraient théoriquement bénéficier d'une forme de protection…

Dans une tribune, des organisations citoyennes font le même constat. Elles jugent, par ailleurs, que « la période prévue pour la conservation des données est clairement injustifiée, excessive (un an pour le contenu, six ans pour les métadonnées et huit ans pour les communications chiffrées) et en contradiction avec les principes posés par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014. » Un point de vue partagé par l'association de défense des droits et libertés La Quadrature du Net. L'Observatoire des Libertés et du Numérique (OLN), dont elle fait partie, appelle les élus à rejeter la proposition de loi et le gouvernement à ouvrir un débat public sur la surveillance internationale.

Source : http://www.silicon.fr/loi-surveillance-communications-electroniques-internationales-127920.html

Comment protéger au mieux les données clients des cyberattaques ? | Le Net Expert Informatique

Comment protéger au mieux les données clients des cyberattaques ?

Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison… Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité. C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.

Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :

· Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître couteux à mettre en œuvre mais c'est une méthode de protection efficace.

· Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.

· Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail , d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.

· Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !

Par Bernard Girbal, Vice-Président EMEA chez Hexis Cyber Solutions

---

Source : http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html

---

Safe Harbor remis en question – Et si le transfert de

données personnelles aux US cessait ? | Le Net Expert Informatique

Safe Harbor remis en question – Et si le trans

Pour l'avocat général de la CUJE, la disposition autorisant les transferts de données vers les Etats-Unis (Safe Harbor) est invalide car le pays ne garantit pas la protection de ces données du fait de la surveillance par la NSA. Une Cnil européenne a de plus tout pouvoir pour suspendre ces transferts.

Entre Maximilian Schrems et Facebook, c'est une longue histoire d'amour (vache). C'est notamment à ce dernier qu'on doit d'avoir découvert l'ampleur de la collecte de données personnelles effectuée par le réseau social.
Remonté contre les pratiques de Facebook, le jeune autrichien l'est tout autant à l'encontre de la surveillance massive par les Etats-Unis. Pour accéder aux données des Européens, la NSA pourrait compter sur un dispositif : le Safe Harbor.

Une « des voies » des agences US pour accéder « à la collecte des données »

Le Safe Harbor prévoit le transfert automatique de données par les entreprises entre l'Europe et les Etats-Unis. C'est cet accord qui est visé par Maximilian Schrems au travers de sa plainte contre Facebook devant la justice irlandaise.
Le justiciable européen conteste le transfert de données à caractère personnel de Facebook Ireland à Facebook USA au motif que la protection de ses données n'est pas garantie du fait du programme PRISM de la NSA.
Saisie par la Haute Cour de Justice d'Irlande, la Cour de Justice européenne est appelée à se prononcer sur plusieurs points de droit. Pour l'heure, c'est l'avocat général de la CUJE, Yves Bot, qui a livré son analyse juridique.

Et en substance, ce dernier souligne le manque de garanties entourant le Safe Harbor et estime qu'une autorité nationale de protection peut enquêter sur les transferts de données réalisées dans ce cadre.

Plus encore, écrit l'avocat général, une autorité, au terme de ses investigations, « a le pouvoir de suspendre le transfert de données en cause » dès lors qu'elle estime qu'il « porte atteinte à la protection dont doivent bénéficier » les citoyens de l'UE.
Le Safe Harbor part du postulat que les Etats-Unis apportent un niveau de protection adéquat. Une obligation cependant qui se doit d'être continue, souligne Yves Bot. Cela « suppose qu'aucune circonstance intervenue depuis ne soit de nature à remettre en cause l'évaluation initiale effectuée par la Commission. »
Or, les révélations d'Edward Snowden au sujet de la surveillance par la NSA pourraient justement constituer une remise en cause. La Commission de l'UE elle-même estimait que le Safe Harbor était « l'une des voies par lesquelles les autorités américaines de renseignement ont accès à la collecte des données à caractère personnel initialement traitées au sein de l'Union. »

La « décision 2000/520 doit être déclarée invalide »

Pour l'avocat général de la CUJE, le « droit et la pratique des États-Unis permettent de collecter, à large échelle, les données à caractère personnel de citoyens de l'Union qui sont transférées dans le cadre du régime de la sphère de sécurité, sans que ces derniers bénéficient d'une protection juridictionnelle effective. »
C'est donc le principe même du Safe Harbor et des transferts automatisés de données qui est contesté. « Nous sommes, dès lors, d'avis que la décision 2000/520 doit être déclarée invalide dans la mesure où l'existence d'une dérogation qui permet d'une manière aussi générale et imprécise d'écarter les principes du régime de la sphère de sécurité empêche par elle-même de considérer que ce régime assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées aux États-Unis depuis l'Union » va jusqu'à considérer le représentant de la CUJE.
« C'est formidable de voir que l'avocat général a utilisé cette affaire pour rendre un avis général sur les transferts de données vers des pays tiers et la surveillance de masse » réagit Maximilian Schrems.
« Si le système du Safe Harbor disparaît, il est très probable que les autorités de protection dans les 28 Etats membres de l'UE n'autoriseront pas les transferts de données des entreprises US soumises à des lois de surveillance de masse » ajoute-t-il.
Les géants américains du Web comme Facebook pourraient ainsi se voir interdire le droit de transférer les données des utilisateurs européens de leurs services vers les Etats-Unis. Les juges de la Cour de Justice de l'UE doivent toutefois rendre leur décision, en tenant compte ou non de l'avis de l'avocat général.

Source : http://www.zdnet.fr/actualites/safe-harbor-et-si-le-transfert-de-donnees-personnelles-aux-us-cessait-39825358.htm
Par Christophe Auffray

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis | Le Net Expert Informatique

L’Europe pourrait revoir le transfert de données personnelles vers les Etats-Unis

La justice européenne met un coup de canif dans le processus permettant aux services américains de puiser dans les informations personnelles d’internautes européens. Suite à une plainte concernant Facebook, l’avocat général de la CJUE demande qu’un pays puisse en demander l’arrêt.

Le Safe Harbor est un texte datant de 2000 autorisant, sous certaines conditions, des entreprises américaines à transférer des données personnelles présentes en Europe vers leur territoire. Un principe qui soulève des polémiques depuis les révélations autour de systèmes américains (NSA via le dispositif PRISM) permettant de consulter ces informations.
La justice européenne souhaite à présent revoir ce dispositif. L’avocat général de la Cour de Justice de l’Union européenne (CJUE) vient à ce titre de rendre un avis dans lequel il demande à ce que n’importe quel Etat membre puisse mettre en pause ce transfert de données. En conséquence, les services américains du renseignement ne pourraient plus puiser dans ce vaste vivier d’informations.
S’il ne s’agit ici que d’un avis (http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106fr.pdf) émis par l’avocat général Yve Bot sur l’épineuse question de la protection des données personnelles, le document demeure clair à l’encontre de la pratique. Il motive son avis en évoquant les cas de « défaillances systémiques constatées dans le pays tiers vers lequel des données à caractère personnel sont transférées, les États membres doivent pouvoir prendre les mesures nécessaires à la sauvegarde des droits fondamentaux protégés par la Charte des droits fondamentaux de l’Union européenne, parmi lesquels figurent le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel ».
Autrement dit, la justice considère que ce principe de transfert automatique de données constitue une « ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données ». Elle demande donc à ce que les autorités nationales de protection des informations personnelles puissent conserver la main sur ce type d’activité.

Max Schrems, un étudiant autrichien au début de la polémique

Depuis à présent 4 ans, Max Schrems, un jeune autrichien s’attaque aux pratiques de Facebook en matière de conservation et de protection des données de ses utilisateurs. Après avoir en premier lieu reproché au réseau social de créer des profils fantômes de personnes inexistantes, il avait attaqué le service pour avoir communiqué à la NSA des informations sur ses inscrits, notamment dans le cadre du programme PRISM.
L’affaire avait été portée devant la Data Protection Commissioner (DPC), l’équivalent de la Cnil en Irlande puis auprès de la Haute Cour du pays (Etat dans lequel le siège de Facebook Europe se trouve). Le cas est ensuite remonté jusqu’à la CJUE.
Suite à la remise de cet avis, la question de la suspension du Safe Harbor se pose à nouveau. La Cour de justice peut désormais suivre ou non l’avis de l’avocat général avant de remettre sa décision définitive. Celle-ci devrait survenir dans les prochains mois.

Source :
http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-780512-facebook-europe-cour-justice.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1165961926#pid=22889469