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

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises | Le Net Expert Informatique

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises

Fin juillet, le Contrôleur Européen de la Protection des Données a publié ses recommandations sur le futur règlement européen portant à quatre le nombre de versions du document. L'occasion de faire le bilan sur les trois évolutions du règlement qui auront le plus d'impact pour les entreprises.

QUEL CHANGEMENT POUR LES ENTREPRISES ?

Mise en place du Privacy by Design (Articles 23, 30, 32a, 33a et 33)

Première nouveauté, les entreprises devront définir et mettre en œuvre des procédures permettant d'intégrer les problématiques liées à la manipulation des données personnelles dès la conception de nouveaux services.

Cette démarche s'accompagne de l'obligation de réaliser des analyses de risques relatives à la vie privée des personnes (discrimination, diffusion de données confidentielles, etc.) préalablement à la mise en place des traitements les plus sensibles et à chaque modification du traitement.

Face aux risques sur la vie privée des personnes induits par ces traitements, il sera imposé aux entreprises d'adopter des mesures de sécurité adéquates en vue de les maitriser.

Concrètement que retenir du Privacy by Design ?

Une mise à jour de la méthodologie projet afin d'identifier au plus tôt les traitements sensibles et une méthode d'analyse de risques à définir et outiller.

Il sera pour cela possible de s'inspirer des guides pratiques de la CNIL intitulés « Etude d'impact sur la vie privée », qui seront à simplifier et contextualiser aux besoins spécifiques de l'entreprise.

Responsabilisation ou « Accountability » (Articles 22 et 28)

Toute entreprise devra désormais être capable de prouver sa conformité vis-à-vis du règlement.

Cette exigence se traduit par :

• l'adoption d'une politique cadre de gestion des données à caractère personnel ;

• une organisation associée ;

• des procédures opérationnelles déclinant les thèmes du règlement (information, respect des droits des personnes, transfert à des sous-contractants, etc.).

L'entreprise devra également être en capacité de prouver l'application de ces politiques et donc, de mettre en place des processus de contrôle.

L'occasion de parler de la personne qui illustrera ce principe d' « Accountability » : le DPO (pour Data Protection Officer). Il devient quasiment obligatoire et remplace le CIL actuel.

Concernant ce DPO, le texte entérine l'obligation de lui fournir le personnel, les locaux, les équipements et toutes les autres ressources nécessaires pour mener à bien ses missions. Encore une fois le parlement souhaite aller au-delà de cette exigence : il propose de nommer au sein de la direction une personne responsable du respect du règlement.

Comment appliquer ce principe ? Il sera nécessaire de définir a minima une politique avec des règles de protection des données ainsi qu''un plan de contrôle et de formation. Cette politique pourra par exemple s'inspirer du modèle des BCR « Binding Corporate Rules », dont le principe a été entériné dans le futur texte, pour lesquelles des modèles types et des premiers retours d'expérience existent déjà.

Obligation de notification des fuites (articles 31 et 32)

L'ensemble des parties s'accordent sur l'obligation de notification des fuites aux autorités. Le Parlement propose même que les entreprises mettent en ligne un registre listant les types de brèches de sécurité rencontrées. Il sera intéressant de constater comment cette exigence cohabitera avec les législations nationales en matière de sécurité et la protection des intérêts de la nation qui tendent à limiter la diffusion de ce type d'information.

La notification de fuites aux personnes concernées, quant à elle, n'est obligatoire que si l'entreprise n'est pas en mesure de démontrer qu'elle a mis en œuvre des mesures afin de rendre cette fuite sans conséquence. D'où l'intérêt d'effectuer correctement l'analyse de risques, de définir et d'implémenter des mesures appropriées.

Au final, deux recommandations afin d'anticiper le futur règlement sur ce point :

• un processus de gestion des fuites de données à définir en l'orchestrant avec les dispositifs de gestion de crise existants et les processus de relation client,

• la réalisation d'exercices réguliers afin de tester son efficacité avec tous les acteurs concernés.

UNE MISE EN CONFORMITÉ À ANTICIPER

Au-delà de ces trois nouveautés majeures, d'autres modifications plus limitées en termes d'impacts organisationnels sont également à prendre en compte, comme la création du droit à la portabilité ou l'extension de la liste des données sensibles. On peut par ailleurs noter le renforcement d'obligations existantes comme le droit à l'information et le recueil du consentement. Le diable se nichera dans les détails.

Pour conclure, les deux années de mise en application du règlement ne seront pas de trop (soit une mise en conformité d'ici début 2018) et nous ne pouvons que conseiller d'initier la mise en conformité dès 2016, avec le cadrage et le lancement des premiers chantiers majeurs. D'autant plus que le sujet devient de plus en plus visible médiatiquement (condamnation récente de Boulanger, Google et l'application du droit à l'oubli, etc.) et que les sanctions financières deviennent réellement significatives (entre 2 et 5% du chiffre d'affaire mondial). L'occasion pour toutes les entreprises de communiquer largement sur les principes de respect de la vie privée effectivement appliqués.

Source : http://www.solucominsight.fr/2015/09/nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-anticiper-les-3-impacts-majeurs/

AVG envisage de vendre certaines données des utilisateurs aux annonceurs en ligne, pour financer ses produits gratuits | Le Net Expert Informatique

	AVG envisage de vendre certaines données des utilisateurs aux annonceurs en ligne, pour financer ses produits gratuits

La firme de sécurité tchèque AVG Technologies a annoncé dans un billet de blog des changements dans la collecte et l'utilisation des données de ses utilisateurs à des fins commerciales. Ces changements s'inscrivent dans une récente révision de la politique de confidentialité d'AVG, qui est censée prendre effet à partir du 15 Octobre prochain.

Dans sa nouvelle politique, le fabricant d'antivirus explique le besoin de collecter certaines données des utilisateurs. En général, les firmes de sécurité à l'instar de la société tchèque collectent certaines données des utilisateurs dans le but d'améliorer les produits et services offerts. Il s'agit entre autres des données relatives aux menaces de logiciels malveillants potentiels, des informations sur la façon dont les produits et leurs caractéristiques sont utilisés, ou encore les informations géographiques des utilisateurs des différentes produits et services.

A cette liste, AVG envisage d'ajouter des informations supplémentaires dans le but de financer certains de ses produits gratuits afin qu'ils le restent toujours. La société s'intéresse particulièrement à l'ID de publicité associé aux terminaux des utilisateurs, les historiques de recherche et de navigation, y compris les métadonnées, ainsi que les informations sur les fournisseurs de services Internet ou les réseaux mobiles utilisés pour se connecter à ses produits. AVG Technologies va également collecter les informations concernant d'autres applications que vous pourriez avoir sur votre appareil et comment vous les utiliser.

Visiblement, la société pourrait les vendre aux annonceurs en ligne qui se présentent comme des demandeurs potentiels de ces informations, qui pourraient leur permettre de diffuser des annonces ciblées. A ce sujet, la société explique dans un billet de blog que c'est une pratique générale pour les produits logiciels et sites web de collecter les données des utilisateurs. « Les données d'utilisation leur permettent de personnaliser l'expérience de leurs clients et partager également des données avec des tiers qui leur permettent d'améliorer ou de développer de nouveaux produits », explique AVG. Le fabricant d'antivirus rappelle d'ailleurs que c'est cette pratique qui permet aux annonceurs de savoir où placer les bannières publicitaires, et que même chez AVG, les données non personnellement identifiables sont recueillies dans le cadre des performances des applications.

AVG précise toutefois que « les données personnellement identifiables ne seront vendues à quiconque, y compris les annonceurs ». Certaines de ces données pourraient toutefois être partagées avec des collaborateurs et filiales de la société à des fins de statistiques et de recherche, mais avec des restrictions.

Face à la possibilité qu'il puisse y avoir une fuite des données personnellement identifiables via les historiques de navigation par exemple, le fabricant d'antivirus dit qu'il va prendre des mesures de précaution pour filtrer ces informations avant de vendre l'historique de navigation des utilisateurs.

Toutefois, cette nouvelle politique ne devrait pas être imposée aux utilisateurs des produits gratuits ciblés par la société. En effet, AVG explique que le délai accordé avant l'entrée en vigueur de sa nouvelle politique de confidentialité a été défini pour permettre aux utilisateurs d'en prendre connaissance afin de décider s'ils veulent participer à ce programme de collecte de données « anonymisées ». Si la société se réserve le droit de modifier sa politique à n'importe quel moment, elle confirme par contre qu'à l'heure actuelle, aucun partage des données ne se fera jusqu'à ce que ses clients soient en mesure de faire ce choix.

Source :
http://www.developpez.com/actu/90118/AVG-envisage-de-vendre-certaines-donnees-des-utilisateurs-aux-annonceurs-en-ligne-pour-financer-ses-produits-gratuits/

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne

respecte pas les règles ? | Le Net Expert Informatique

Géolocalisation des véhicules professionnels des employés : que faire si mon employeur ne respecte pas les règles ?

Vous avez plusieurs recours :
• Adresser une plainte à la CNIL : la CNIL peut contrôler tous les systèmes de géolocalisation installés en France. Si le contrôle confirme que l'employeur ne respecte pas les règles, il sera mis en demeure de respecter la loi, sous peine de sanctions ;
• Saisir les services de l'inspection du Travail de votre département ;
• Déposer une plainte pénale auprès du procureur de la République, des services de police ou de gendarmerie.
• Vous avez demandé à avoir accès aux informations de géolocalisation qui vous concernent et votre employeur a refusé ?

Vous pouvez, après un délai de 2 mois, adresser une plainte à la CNIL.

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 !

S o u r c e : https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=06EF1A234FB5C655BF980F0F5D5C31E9?name=G%C3%A9olocalisation+des+v%C3%A9hicules+professionnels+des+employ%C3%A9s+%3A+que+faire+si+mon+employeur+ne+respecte+pas+les+r%C3%A8gles+%3F&id=339

5,6M d'empreintes digitales de fonctionnaires américains dérobées | Le Net Expert Informatique

5,6M d'empreintes digitales de fonctionnaires américains dérobées

Alors qu'il était estimé à 1,1 million, le nombre d'empreintes digitales volées à l'occasion du gigantesque piratage du service du personnel des fonctionnaires américains révélé cet été se monte désormais à 5,6 millions. Un coup dur pour cette administration qui poursuit ses investigations.

Le bilan s'alourdit concernant le piratage massif dont a été victime l'Office of Personnel Management (OPM) aux Etats-Unis. Révélé en plein coeur de l'été, ce piratage a débouché sur le vol de données personnelles en tous genres dont essentiellement des numéros de sécurité sociale, mais pas seulement (historiques de consommation de drogue, problèmes juridiques et financiers, dossiers scolaires, historiques de carrières…), appartenant à plus de 20 millions de fonctionnaires américains. Parmi les données volées se trouvaient également des empreintes digitales. Mais alors que le nombre d'empreintes dérobées était auparavant estimé à 1,1 million, l'OPM a revu ce nombre à la hausse.

« Sur les 21,5 millions de personnes dont les numéros de sécurité sociale et d'autres informations sensibles ont été impactées par la faille, le nombre d'empreintes digitales qui ont été volées a été revu à la hausse pour passer de 1,1 à 5,6 millions », a indiqué l'administration. « Cela ne fait pas grimper le nombre de 21,5 millions de personnes touchées par cet incident ».

Les victimes notifiées seulement maintenant

Par ailleurs, le service du personnel des fonctionnaires américains indique qu'une équipe inter-agence est toujours mobilisée pour analyser et affiner les données précisément volées et se prépare à envoyer des lettres de notification à toutes les personnes touchées. A l'heure du big data et des solutions de traitement en masse de données, on ne peut que s'interroger sur le temps de latence – plus de deux mois – dont a eu besoin cette administration pour faire un point complet sur l'ensemble des personnes et données touchées. Un temps dont ont certainement pu profiter les pirates pour exploiter et mettre à l'abri ces données en vue de les réutiliser à des fins frauduleuses ou bien de les revendre.

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.lemondeinformatique.fr/actualites/lire-5-6m-d-empreintes-digitales-de-fonctionnaires-americains-derobees-62451.html

Un électeur peut-il utiliser la liste électorale ? | Le Net Expert Informatique

Un électeur peut-il utiliser la liste électorale ?

Tout électeur peut obtenir de sa mairie une copie de la liste électorale à condition de s'engager à ne pas en faire un usage commercial.
A noter : la Commission d'accès aux documents administratifs (CADA) considère que l'accès aux listes électorales peut s'exercer par consultation gratuite sur place ou par envoi de copies, sur support papier ou informatique.

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.aide.cnil.fr/selfcnil/site/template.do;jsessionid=16F67A95B36120F226D2F8E337B98601?name=Liste+%C3%A9lectorale+%3A+un+%C3%A9lecteur+peut-il+l%27utiliser+%3F&id=175

L'Europe prend un mauvais virage en matière numérique |

Le Net Expert Informatique

	L’Europe prend un mauvais virage en matière numérique

Dans l'exercice consistant à élaborer de bonnes politiques en matière numérique, l'Europe a raté son premier test majeur. Au mois de mai, la Commission européenne annonçait la création d'un marché unique du numérique réunissant 500 millions de consommateurs, censé apporter 415 milliards € au PIB de l'Union européenne et créer quelque 3,8 millions d'emplois. Seulement voilà, une récente décision autour d'une problématique numérique majeure – la confidentialité des données – menace de faire dérailler la locomotive.

Au mois de juin, les ministres de l'Intérieur et de la Justice de l'UE ont voté en faveur de la conservation de pouvoirs nationaux significatifs en matière de protection de la confidentialité numérique, plutôt que d'élaborer un ensemble de règles s'appliquant aux 28 Etats de l'UE. Si le Parlement européen venait à approuver cette proposition, la divergence des règles nationales serait alors de retour. Plus inquiétant encore, ceci ouvrirait la voie à la mise en place de dispositions rendant illégales les activités bénignes et peu risquées d'exploration des données, qui sous-tendent la publicité en ligne.

La publicité sur Internet permet aux citoyens de l'UE d'accéder à de l'information, à des contenus éducatifs, à des canaux de commerce et autres sites de divertissement, sans avoir à en payer directement l'accès. En Europe, les montants dépensés dans ce domaine sont en pleine augmentation. Les revenus du secteur ont plus que quadruplé depuis 2006, malgré la stagnation de l'économie européenne dans son ensemble. Le nouveau combat de la confidentialité en UE vient menacer toute cette évolution. Non seulement faut-il s'attendre à une importante charge administrative liée aux coûts supplémentaires et aux difficultés bureaucratiques, mais un risque réel existe également de voir ces nouvelles règles mettre à mal le modèle d'entreprise d'un grand nombre des principales sociétés européennes en ligne.

Il s'agirait d'un véritable gâchis – qui plus est facilement préventible. En 2012, la Commission européenne a formulé une proposition de remplacement de la législation de l'UE existante en matière de protection des données, dont la plus récente version avait été élaborée en 1995, époque à laquelle Internet ne jouait qu'un rôle minime dans l'économie. Le texte initial était prometteur. Il entendait harmoniser les cadres juridiques fragmentés de l'Europe, fournir aux entreprises un guichet unique fort utile, et rassurer les consommateurs en leur garantissant une utilisation appropriée de leurs données.

Malheureusement, beaucoup des propositions les plus judicieuses ont été depuis abandonnées. Lors du rassemblement ministériel du mois de juin, le principe majeur de guichet unique a été véritablement éviscéré. Plutôt que de permettre aux entreprises d'avoir affaire à l'autorité de protection des données compétente au sein du pays dans lequel ces entreprises possèdent leur siège ou leur principale implantation européenne, les Etats membres insistent aujourd'hui pour que les régulateurs nationaux conservent le contrôle. Conformément aux nouvelles règles proposées, toute autorité « concernée » pourrait s'opposer à une décision prise par un autre régulateur national, donnant lieu à une procédure d'arbitrage complexe faisant intervenir l'ensemble des 28 agences.

Les ministres ont également adopté une large définition de ce que l'on entend par données personnelles. Y figureraient ainsi à la fois les cookies (petits ensembles de données stockés sur l'ordinateur d'un internaute) et les adresses IP (code utilisé pour identifier un ordinateur lorsqu'il se connecte à Internet) – bien que ces éléments ne fournissent aucun lien en direction d'un individu donné. Au mieux, cette définition étendue et peu pointue des données personnelles menace de créer des obstacles inutiles pour les annonceurs numériques basés dans l'UE. Au pire, elle risque de plonger leur modèle d'entreprise dans l'illégalité.

Ces règles inutilement strictes en matière de données sont vouées à affecter les entreprises européennes dans une mesure disproportionnée. On peut comprendre qu'il soit demandé à Google, Facebook et autres géants américains d'Internet de solliciter le consentement explicite de leurs utilisateurs. Pour autant, le secteur européen de l'Internet est dominé par des entreprises de B to B, dont les marques peu connues traitent effectivement les données des consommateurs, mais manquent d'un contact direct avec les utilisateurs. Ainsi, la seule véritable alternative consistera pour ces sociétés Internet européennes à travailler auprès des grandes plateformes américaines, et à devenir encore plus dépendantes de celles-ci.

Bien que le Royaume-Uni, la Suède, la Norvège et les Pays-Bas comptent parmi les pays leaders de l'Internet à travers le monde, de nombreux autres Etats européens évoluent considérablement à la traîne. Ainsi, l'économie numérique contribue au PIB de l'UE à hauteur d'environ 4 %, contre 5 % aux États-Unis et 7,3 % en Corée du Sud. Les nouvelles réglementations proposées ne feront qu'accentuer cet important retard des entreprises européennes par rapport à leurs concurrentes internationales.

L'Europe est confrontée à un choix important. Bien entendu, l'UE doit pouvoir rassurer ses citoyens quant à l'utilisation appropriée de leurs données ; les mesures en ce sens peuvent contribuer à la croissance de l'économie numérique. En revanche, les dirigeants du continent ne doivent pas oublier qu'un marché unique du numérique ne pourra exister aussi longtemps que les règles accentueront la divergence des approches nationales autour de la confidentialité, et qu'elles feront obstacle à l'utilisation par Internet des données anonymes à des fins de publicité numérique. Le sort d'une génération toute entière d'entrepreneurs numériques européens est aujourd'hui en jeu.

Source : http://www.libe.ma/L-Europe-prend-un-mauvais-virage-en-matiere-numerique_a66663.html

Par Christopher Engman PDG de la société suédoise de commercialisation en ligne, «Vendemore» (Traduit de l'anglais par Martin Morel)

100% des montres connectées présentent des failles de sécurité | Le Net Expert Informatique

Les montres équipées de connexion réseau et de fonctions de communication représentent une nouvelle cible pour les cyberattaques. Tel est le principal résultat de l'étude, menée par HP Fortify, qui révèle que 100% des montres testées recèlent d'importantes vulnérabilités, comme par exemple des fonctions d'authentification insuffisantes, un manque de capacités de chiffrement, et des soucis dans la protection des données personnelles1. Dans ce rapport, HP recommande un certain nombre d'actions pour améliorer la sécurité dans la conception et l'utilisation des montres, à la maison ou dans son environnement de travail.

Avec le déploiement de l'Internet des Objets, les smartwatches gagnent en popularité en raison de leur côté pratique et des nouvelles fonctionnalités qu'elles proposent. En devenant des objets usuels, ces montres vont collecter de plus en plus d'informations personnelles sensibles, comme des données de santé. La possibilité de les connecter avec des applications disponibles sur smartphone risquent prochainement de leur donner accès à encore plus d'informations, comme par exemple les codes permettant d'ouvrir votre maison ou votre véhicule.
« Les montres connectées commencent à peine à entrer dans nos vies. Elles offrent déjà de nouvelles fonctionnalités innovantes qui pourraient ouvrir la voie à de nouvelles menaces sur des informations et des activités sensibles », a déclaré Jason Schmitt, Directeur Général Fortify de l'entité HP Security. « Avec l'accélération de l'adoption des smartwatches, cette plate-forme va devenir bien plus attrayante pour tous ceux qui voudraient en faire une utilisation frauduleuse. Il devient nécessaire de prendre des précautions lors de la transmission des données personnelles ou du raccordement de ces équipements aux réseaux d'entreprise. »
L'étude HP s'interroge ainsi sur la capacité des smartwatches à stocker et à sécuriser les données sensibles pour lesquelles elles ont été conçues. HP s'est appuyé sur HP Fortify on Demand pour évaluer 10 montres connectées à des applications mobiles et un cloud Android ou iOS.

Cette étude révèle de nombreuses failles de sécurité parmi lesquelles les plus fréquentes et les plus faciles à corriger sont :

L'insuffisance des fonctions d'autorisation et d'authentification des utilisateurs :
Chaque montre connectée testée était couplée à une interface sur téléphone mobile qui ne gérait pas l'authentification à deux facteurs, et qui ne verrouillait pas les comptes après 3 ou 5 saisies de mots de passe infructueux. Trois montres sur dix, c'est à dire 30%, étaient vulnérables aux tentatives de moisson de comptes utilisateurs, ce qui veut dire qu'un pirate informatique pourrait obtenir le contrôle de la montre et de ses données en profitant d'une politique de mots de passe faible, du non blocage des comptes, ou en énumérant des listes de comptes utilisateur potentiels.

Le manque de chiffrement lors du transfert de données :
Le chiffrement lors du transport d'information est essentiel, dans la mesure où des informations personnelles sont envoyées vers de multiples destinations dans le cloud. Même si 100 pourcents des montres testées intégraient le chiffrement lors transport avec le protocole SSL/TLS, environ 40% des connexions vers le cloud restaient vulnérables à l'attaque POODLE, permettant l'utilisation d'outils de déchiffrement peu puissants, ou encore le protocole SSL v2.

Interfaces peu sécurisées :
30% des montres testées utilisaient des interfaces web accessibles en mode cloud, et toutes présentaient des risques d'énumération de comptes utilisateur. Dans un test spécifique, 30% ont également révélé des risques d'énumération de comptes utilisateur depuis leurs applications sur mobile. Cette défaillance permet aux hackers d'identifier des comptes utilisateurs valides en s'appuyant sur les informations reçues via les mécanismes de réinitialisation de mots de passe.

Logiciels et microcode peu sécurisés :
70% des montres ont révélé des failles dans la protection des mises à jour de microcode, comme par exemple la transmission en clair des mises à jour, sans chiffrer les fichiers. Cependant, plusieurs mises à jour étaient protégées par une signature, évitant ainsi l'installation d'un microcode contaminé. Même si des updates malicieuses ne peuvent être installées, le manque de chiffrement permet aux fichiers d'être téléchargés puis analysés.

Soucis sur la protection des données personnelles :
Toutes les montres collectent des données personnelles – comme le nom, l'adresse, la date de naissance, le poids, le sexe, la fréquence cardiaque, et bien d'autres informations relatives à la santé de l'utilisateur. Si l'on rapproche ceci des problèmes relevés sur l'énumération des comptes utilisateur ou l'utilisation de mots de passe faiblement sécurisés sur certaines montres, le risque de diffusion des données personnelles depuis une montre connectée devient un problème réel.

En attendant que les fabricants incorporent les dispositifs nécessaires permettant de mieux sécuriser leurs smartwatches, les utilisateurs sont priés d'examiner scrupuleusement les fonctions de sécurisation existantes avant de choisir un modèle de montre connectée. HP recommande aux utilisateurs de ne pas activer les fonctions de contrôle des accès sensibles, comme par exemple l'accès à leur domicile ou leur véhicule, sauf si un mécanisme d'autorisation performant est proposé par la montre. De plus, en activant la fonctionnalité passcode, en imposant des mots de passe sophistiqués et en introduisant une authentification à deux facteurs, il est possible d'éviter des accès frauduleux aux données. Au delà de la protection des données personnelles, ces mesures sont essentielles dès lors que la smartwatch va être utilisée dans un environnement de travail et connectée au réseau de l'entreprise.

Méthodologie
Réalisée par HP Fortify, l'étude HP Smartwatch Security Study a utilisé la méthodologie HP Fortify on Demand IoT testing methodology, combinée avec des tests manuels et d'autres outils de test automatisés. Les équipements et les composants testés ont été évalués sur la base de l'outil OWASP Internet of Things Top 10 et des vulnérabilités spécifiques associées à chacune des 10 premières catégories.
Toutes les données et les tous les pourcentages inclus dans l'étude ont été extraits des tests menés sur les 10 montres évaluées. Malgré l'existence d'un nombre croissant de fabricants et de modèles de smartwatches, HP pense que les résultats obtenus sur cet échantillon de 10 modèles donne un bon indicateur du niveau de sécurité des smartwatches actuelles du marché.

Des conseils complémentaires sur la sécurisation des smartwatches sont disponibles dans le rapport complet (http://go.saas.hp.com/fod/internet-of-things)

Pour toute information complémentaire, il est possible de consulter le premier rapport de la série sur l'Internet des Objets, 2014 HP Internet of Things Research Study, qui passe en revue le niveau de sécurité des 10 objets connectés les plus courants du marché. De plus, l'étude 2015 HP Home Security Systems Report (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-7342ENW&cc=us&lc=en) examine les 10 systèmes les plus répandus en matière de protection connectée du domicile.
(1) "HP Internet of Things Security Report: Smartwatches," HP, Juillet 2015.

Source : http://www.itrnews.com/articles/157450/100-montres-connectees-presentent-failles-securite.html et ITRmobiles.com

Le certificat électronique est une arme efficace contre la Cybercriminalité | Le Net Expert Informatique

	Le certificat électronique est une arme efficace contre la Cybercriminalité

Lutter contre la cybercriminalité est un axe stratégique pour les entreprises et les institutions. En effet, nous assistons quotidiennement à des attaques toujours plus sophistiquées qui viennent durablement compromettre l'intégrité et la confidentialité des échanges réalisés sur le net. Bien entendu, nombre d'entreprises et d'institutions mettent en place des dispositifs pour se protéger, mais en laissant «certains trous dans la raquette» qui sont immédiatement utilisés par les pirates pour mener à bien leurs actions.

Très répandues, ces pratiques créent des désastres financiers et montrent bien que les flux sortants sont tout aussi exposés que les flux entrants. Il est donc nécessaire de les prendre en compte dans la mise en œuvre de dispositifs de protection efficace.

L'usage du certificat électronique ID (pour personne physique) est la piste à privilégier. Il est d'ailleurs largement plébiscité par l'Etat et les collectivités avec la norme RGS. Véritable rempart contre l'usurpation d'identité, il permet au destinataire d'un mail d'en vérifier l'émetteur, il permet également de garantir la confidentialité des données échangées. L'autre avantage tient à sa simplicité d'utilisation sur les mobiles et tablettes. Avec un certificat, les envois de mails à partir d'un smartphone ne représentent plus une faille de sécurité mais sont protégés efficacement.

Au regard de ces éléments, institutions et entreprises doivent accélérer le déploiement de certificats pour sécuriser leurs échanges de données. Une prise de conscience dans ce domaine permet de colmater des brèches importantes et complète des dispositifs traditionnels de type Firewall qui jouent pour leur part un rôle de filtrage pour les données entrantes. Avec les certificats électroniques, les flux sortants sont parfaitement sécurisés, leur apport dans la lutte contre la cybercriminalité est donc stratégique, d'autant que leur coût d'acquisition n'est pas onéreux.

Source : http://www.edubourse.com/finance/actualites.php?actu=89518

L'état des lieux de la protection des données personnelles en Tunisie | Le

Net Expert Informatique

L’état des lieux de la protection des données personnelles en Tunisie

Chawki Gaddes, président de l'INPDP explique les missions et ambitions de cette instance chargée de la protection des données personnelles.

Fruit d'un travail juridique entamé en 2002, l'Instance nationale de la protection des données personnelles (INPDP), régie par la loi organique no 2004-63 du 27 juillet 2004, n'a pu être mise en route qu'au début 2009. Et c'est avec la nomination de son 3e président, en la personne du juriste Chawki Gaddes, qui a succédé, le 5 mai 20015, au magistrat Mokhtar Yahiaoui (les présidents et les membres de l'instance sont désignés par décret pour 3 ans), que le travail effectif a réellement démarré.

«Il faut commencer par sensibiliser, vulgariser et expliquer aux Tunisiens ces notions de données personnelles et leur importance aux échelles individuelle et collective dans tout le pays», insiste Chawki Gaddes.

Les données sensibles

Le président de l'INPDP précise, dans ce contexte, que la donnée personnelle est toute information qui permet d'identifier ou de rendre identifiable une personne (articles 4 et 5 de la loi de 2004). En d'autres termes, toute information qui permet à remonter à la personne concernée : nom et prénom, date de naissance, adresse aussi bien physique qu'électronique, numéro de téléphone, plaque minéralogique de la voiture, numéro d'identification, empreintes digitale ou rétinienne, photo, code génétique, état de santé, opérations bancaires, traces informatiques… «Et la liste n'est pas close, car la science et les techniques évoluent et élargissent davantage le champ de définition de cette notion», ajoute M. Gaddes.

Il y a, en effet, aussi, des données que l'on a pris l'habitude de qualifier de «sensibles»: origine raciale ou génétique, convictions religieuses, opinions politiques, antécédents judiciaires… «Ces données sont, par principe, interdites de traitement», souligne le président de l'INPDP. Et on entend par traitement toutes les opérations réalisées de manière automatique ou manuelle sur les données personnelles. Elles touchent à tout le cycle de la vie d'une information, de sa naissance jusqu'à sa mort : la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation l'expédition…

Des règles à respecter

Toutes ces opérations doivent respecter les règles définies par la loi qui stipule dans son article premier que toute action sur les données personnelles doit se faire «dans le cadre de la transparence, la loyauté et le respect de la dignité humaine».

L'opération de traitement doit être connue de la personne concernée et de l'instance de contrôle. Aucun fichier n'est créé ni géré dans le secret, et l'INPDP mettra en ligne sur son site la base de données relatives à tout traitement sur le territoire national. Cela permet au citoyen (et à tout résident) de savoir où les données sont collectées et auprès de qui il peut y accéder et éventuellement s'y opposer. Il s'agit d'éthique, de confiance et d'honnêteté de sorte que la finalité du traitement soit définie à l'avance sans être détournée vers d'autres buts

En définitive, traiter les données personnelles c'est se mettre à l'esprit que l'on gère des êtres humains et non des choses. Il y va donc de la dignité humaine. Le citoyen, de par l'article 24 de la Constitution, a le droit à la préservation de sa vie privée contre toute intrusion qui, de nos jours, est mise à rude épreuve eu égard au recours intensif aux technologies de l'information et de la communication.

La Convention 108

Dans un monde sans frontières, la question n'a pas été laissée au hasard. En effet, les premiers pas dans le domaine de la protection des données personnelles remontent à 1974, en France, avec l'institution d'un identifiant unique, un projet en cours de réalisation en Tunisie.

L'idée a, depuis, fait beaucoup de chemin, malgré l'opposition d'une commission parlementaire française qui considère qu'il s'agit, bel et bien, d'une atteinte aux libertés des individus. C'est ainsi que la loi «Informatique et Liberté» a vu le jour en 1978 pour instituer les règles essentielles en la matière qui ont servi de support à la Convention 108 du Conseil de l'Europe.

La Tunisie, soucieuse de se conformer aux pratiques internationalement reconnues en matière de respect des droits humains, a demandé, en juillet dernier, à adhérer à cette convention en vue d'instaurer un climat de confiance aussi bien vis-à-vis de ses citoyens que des intervenants étrangers. Elle sera le 5e Etat non-européen à adhérer à cette convention, après l'Uruguay, l'Ile Maurice, le Maroc et le Sénégal.

La Tunisie sera, ainsi, labellisée «espace de confiance» dans le monde et pourra faire partie des marchés de traitement des données personnelles (ou offshoring) «qui contribuera à la création de 50.000 postes d'emploi et à une rentrée de devises de pas moins de 2000 millions de dinars. Encore faut-il qu'elle réussisse sa bataille contre la violation des données personnelles», tient à affirmer le président de l'INPDP

L'Europe a fortement besoin d'externaliser le traitement des données personnelles, compte tenu des coûts assez élevés de cette opération dans l'espace européen, et la Tunisie est appelée à saisir cette opportunité, à l'instar de l'Inde ou de la Roumanie, qui profitent déjà de ce filon.

Les abus et des sanctions

La loi qui garantit tous les droits en matière d'usage des données personnelles a prévu aussi des sanctions qui vont de l'amende, légère ou lourde (pouvant atteindre 50.000 dinars), jusqu'à la peine de 2 à 5 ans de prison lorsqu'il s'agit de communication ou de transfert de données vers l'étranger

Pour se rendre compte de l'acuité de cette problématique et de ses retombées sur la vie de tous les jours, il faut parcourir la liste des infractions possibles et qui pourraient passer inaperçues, telle l'installation des vidéo-surveillance dans les lieux autres que ceux ouverts au public, ainsi que la liste des peines et des pénalités encourues.

Bref, c'est tout un chantier qui est ouvert devant l'INPDP, qui se donne pour mission d'inculquer et divulguer la culture de la préservation des données personnelles et sensibiliser le citoyen sur ses droits dans ce domaine.

Quand on sait que jusqu'au mois de mai 2015, aucun dossier se rapportant à un abus commis dans ce domaine n'a encore été traité et qu'aucun rapport d'activité n'a été ni élaboré ni présenté, on mesure le chemin qui reste à faire dans ce domaine. «Nous comptons sur la société civile et sur les médias pour nous aider dans cet effort de communication en faveur de la préservation des données personnelles», conclue Chawki Gaddes.

Source : http://kapitalis.com/tunisie/2015/09/06/chawki-gaddes-letat-des-lieux-de-la-protection-des-donnees-personnelles-en-tunisie/
Propos recueillis par Wajdi Msaed