Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Pour savoir si les applications installées sur nos téléphones portables se montrent respectueuses de nos données personnelles, la Cnil a élaboré, avec l'aide de l'Inria, un logiciel de contrôle et l'a fait tourner sur 121 applications Android pour vérifier la collecte éventuelle d'informations de localisation, du carnet d'adresses, du calendrier ou même des numéros de téléphone.

Le résultat est édifiant, révèlent nos confrères d'Europe 1 : 66 % des applications communiquent sur le type de réseau Internet (Wi-Fi, 3G, 4G) auquel l'utilisateur est connecté, 24 % accèdent à la géolocalisation, le plus souvent à l'insu de l'utilisateur, cinq applis ont accédé au numéro de téléphone de l'utilisateur et deux ont été jusqu'à récupérer la liste des identifiants des points d'accès Wi-Fi présents autour de l'utilisateur.

Une application qui n'est pourtant pas dédiée à la recherche d'itinéraire, Google Play, boutique de téléchargement d'applications pour Android, a même accédé à plus d'un million de fois à la géolocalisation d'un smartphone unique en trois mois !

La Cnil assortit ses conclusions de quelques conseils. La meilleure façon de se protéger consiste à éviter les téléchargements inutiles, et à faire régulièrement le tri dans celles qui sont installées sur son appareil. On peut également régler les paramètres de son téléphone (menu Paramètres Google, option « désactiver annonces par centres d'intérêt ».)

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

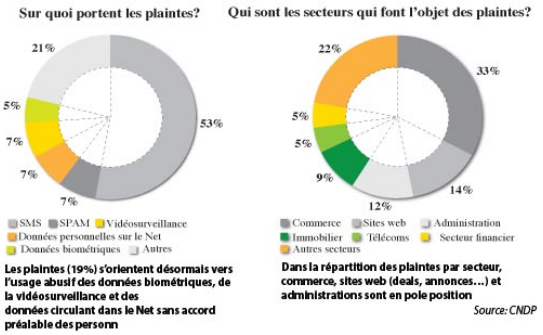
Source : http://www.industrie-techno.com/smartphones-deux-applis-sur-trois-nous-espionnent-revele-la-cnil.35111
Par Muriel de Véricourt

Nouveau tournant pour la protection de la vie privée au Maroc

Nouveau tournant pour la protection de la vie privée au Maroc

La Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) publie son premier rapport d'activité 2010-2013. Installée fin août 2010, cette autorité administrative se charge de préserver le respect de la vie privée. Elle s'appuie sur la loi 09-08 relative à la protection des personnes physiques du traitement des données personnelles (Bulletin officiel en français n°5714 du 15 mars 2009).

«Les plaintes qui nous parviennent sont en hausse d'année en année. Ce qui signifie que la culture de la protection des données personnelles commence à se répandre. Certes, cette culture n'est qu'à ses débuts, mais les résultats réalisés (…) sont franchement encourageants», relève avec optimisme le président de la CNDP, Saïd Ihraï. Une seule plainte en 2011, 7 en 2012 et 43 en 2013. Qu'est-ce qui explique cette progression? L'accessibilité de la procédure joue: dans 83% des cas, les plaintes sont enregistrées en ligne (www.cndp.ma). Elles sont aussi déposées sur place ou envoyées par fax. «Toutefois, le nombre de réclamations reste limité à cause notamment d'une grande réticence à les faire par écrit», selon le rapport.



Les SMS indésirables arrivent en tête des plaintes, suivis par les Spam… «Près de la moitié des cas ont été réglés. Pour les envois abusifs de SMS, les contacts pris avec le régulateur télécoms et les trois opérateurs ont permis de mettre en place une stratégie de lutte…». Sauf que le business illégal des bases de données se poursuit. C'est pourquoi nos boîtes électroniques sont bombardées par des publicités intempestives. Avec un pourcentage relativement modeste (voir illustration), l'usage abusif de données biométriques et de la vidéosurveillance interpellent (voir encadré). Toutes rubriques confondues, les 51 plaintes déposées jusqu'à fin 2013 émanent surtout de Casablanca et de Rabat (88%). Cette concentration géographique a une cause. Regroupant les grands centres économiques et administratifs, les deux métropoles centralisent par conséquent une masse significative de données personnelles et les responsables des traitements: patronyme, numéro de la carte d'identité et de téléphone, email, photo, empreinte digitale, ADN, relevé d'identité bancaire… Ces données permettent «d'identifier directement ou indirectement» salariés, actionnaires, clients, visiteurs, fournisseurs, administrés…

La CNDP veille à ce que le traitement des informations liées à nos vies privées ait «des finalités précises, claires et légitimes». Conformément à la loi du 18 février 2009, le responsable du traitement doit notifier son activité à la Commission (voir page 6), avoir l'autorisation préalable des personnes concernées, veiller au respect de la confidentialité des données… Le non-respect de la loi expose à des amendes et des sanctions pénales. Vous voilà avertis.

Contrôles inopinés

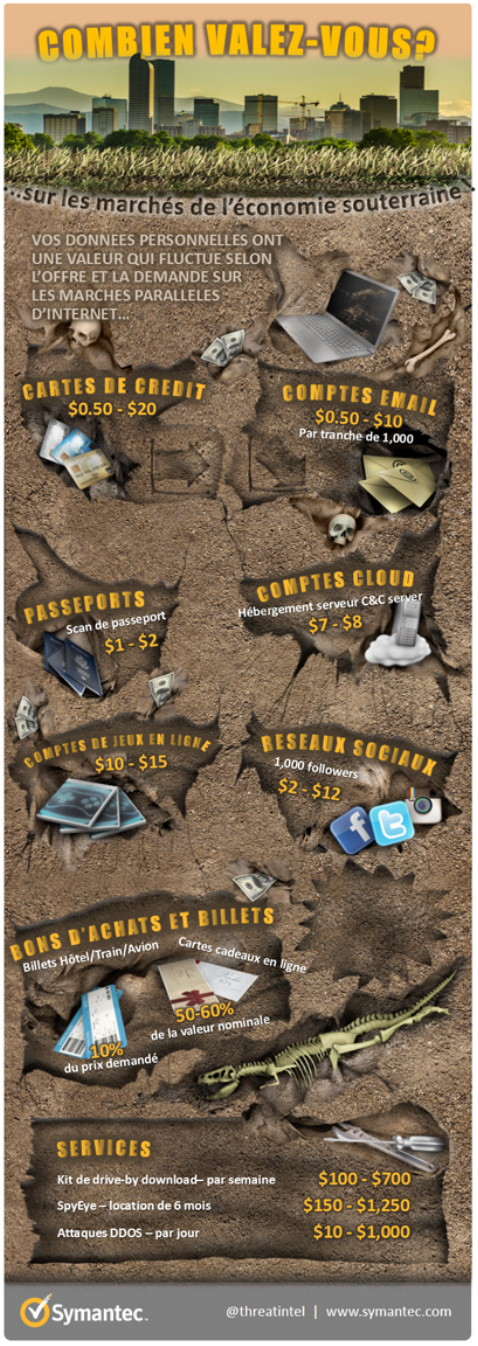
Rappelons à bon entendeur les termes de la Délibération adoptée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) fin mai 2013 à Rabat. Celle-ci porte sur «les conditions nécessaires à la mise en place d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs» (cf. L'Economiste du 15 novembre 2013). Malgré son importance, la Délibération n° 350-2013 demeure largement ignorée par les personnes physiques et morales (entreprises, établissements publics, ministères…).

Particuliers, entreprises et administrations doivent s'attendre à des contrôles inopinés d'agents assermentés. La collecte et le traitement d'images des lieux surveillés constituent une manipulation de données personnelles. L'utilisation de caméra de surveillance doit être notifiée préalablement à la CNDP.

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

Source : http://www.leconomiste.com/article/962774-donnees-personnelles-nouveau-tournant-pour-la-protection-de-la-vie-privee
par Faiçal FAQUIHI

Données volées ! Services d’attaques ! Quels sont prix sur le marché de la cybercriminalité ?

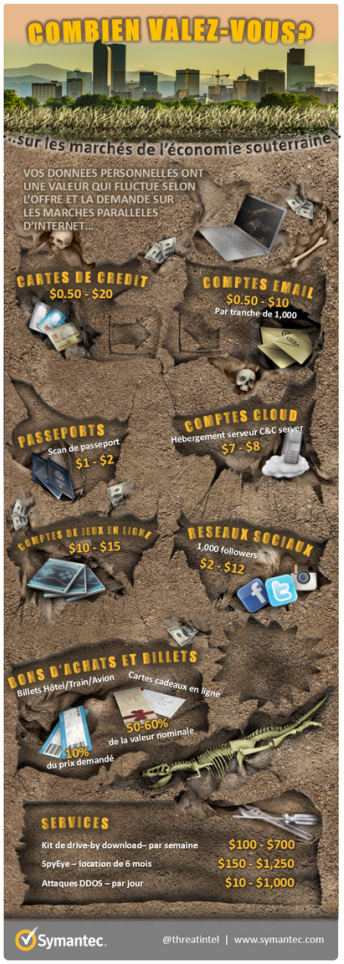


Données volées ! Services d’attaques ! Quels sont prix sur le marché de la cybercriminalité ?

Sur les marchés de l'économie souterraine sur Internet, combien valent les données personnelles volées lors des récentes violations de données massives ? A combien sont proposés les services d'attaques ?

Les chercheurs de Symantec ont mené une étude empirique sur les marchés souterrains florissants de l'Internet et déterminé comment les données volées ou les services d'attaques varient selon la loi de l'offre et de la demande. Si la valeur des emails a diminué de façon significative, le spam ne faisant plus vraiment recette, la valeur d'autres biens et services illicites reste stable.
A titre d'exemples (illustrés via l'infographie ci-dessous) :

– Les scans de passeport coûtent entre 1$ et 2$ et sont utilisés pour les vols d'identités
– Les comptes de jeux en ligne volés se monnaient entre 10$ et 15$, puisqu'ils peuvent rapporter gros dans le monde virtuel
– Les malwares customisés se paient entre 12$ et 3,500$, comme par exemple des outils pour voler des bitcoins en détournant les flux de paiement vers les cybercriminels
– 1 000 followers sur les réseaux sociaux coûtent entre 2$ et 12$
– Les comptes cloud volés sont à 7$ ou 8$. Ils peuvent être utilisés pour héberger des serveurs de commandes et contrôles



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

Source : http://www.infohightech.com/donnees-volees-services-dattaques-quels-sont-prix-sur-le-marche-de-la-cybercriminalite/

Une charte pour protéger les données personnelles

Une charte pour protéger les données personnelles

«l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Atlanta se positionne en protecteur des données personnelles. En effet, à l'occasion de la Journée mondiale des droits de l'Homme, la compagnie d'assurances a publié une charte régissant la protection des données personnelles de ses partenaires et ses clients. Ayant l'ambition d'être reconnu par ses clients, ses collaborateurs et ses partenaires comme «l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Un document qui matérialise les engagements de la compagnie envers ses clients et décrit les modalités suivant lesquelles la compagnie collecte et utilise les données personnelles de ses clients.
Affichée en interne, chez tous les agents et dans son site web, cette charte est en parfaite conformité avec la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

La publication de cette charte intervient suite à une large mise à niveau de l'ensemble des standards et procédures de la compagnie qui, par ailleurs, a reçu de la part de la Commission nationale de contrôle de protection des données à caractère personnel (CNDP) l'autorisation de traitement des données concernant les process opérationnels.

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

Source : http://www.aujourdhui.ma/une/actualite/atlanta-une-charte-pour-proteger-les-donnees-personnelles-115014#.VIyAT9KG92o
Par ALM

Droit à l’oubli pour les entreprises, plus qu’une idée…

	Droit à l’oubli pour les entreprises, plus qu’une idée…

Au nom du principe de la protection de la vie privée, une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles.

Dis-moi comment te référence Google, je te dirai qui tu es… ou pas. Car parfois, la révélation est rude, humiliante, voire dégradante, de celle que l'on voudrait effacer. Mais Internet possède malheureusement une très bonne mémoire, vive et éternelle. Pourtant, le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) a joué les hypnotiseurs : « Oubliez ! Je le veux », a-t-elle dit en substance aux moteurs de recherche. Une décision historique – ont estimé les commentateurs –, instaurant un « droit à l'oubli ». Mais est-ce vraiment sûr ? A y regarder de près la décision n'a qu'une portée limitée. Entre le moteur de recherche et l'internaute, désormais, c'est un peu « je t'oublie, moi non plus ». Parce que ce « droit à l'oubli » existe depuis… 1995.
C'est au nom du principe de la protection de la vie privée qu'une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles. La Cour de justice a souligné ce point au début de son arrêt, plaçant sa décision sous le signe de la sauvegarde des droits fondamentaux. « La CJUE a décidé que l'exploitant du moteur de recherche est tenu de supprimer, sur demande, les liens vers des pages Web, à condition que la démarche de l'internaute soit justifiée. L'arrêt n'instaure pas cependant un "droit à l'effacement des données", mais un "droit à la désindexation" : les liens perdurent, notamment à partir du site américain Google.com, accessible à un internaute européen », explique Olivier Cousi, avocat et associé du cabinet Gide, expert en droit de la propriété intellectuelle.

Zones grises
En outre, si la protection des données est encore imparfaite pour les particuliers, elle est inexistante pour l'entreprise. En effet, la protection comme l'entend l'arrêt de la CJUE ne concerne que les personnes physiques. Alors comment l'entreprise peut-elle gérer son e-réputation ? Quelle démarche pour contrer l'information fausse ou malveillante la concernant ? Autre sujet : cette absence d'intimité, renforcée en France par l'absence de secret des affaires, donne peu d'armes à l'entreprise pour contrer la diffusion de données confidentielles – procès-verbaux de conseil d'administration, chiffre d'affaires… C'est une des zones grises du droit à l'information qui protège également, c'est le bon côté de la médaille, d'une entreprise qui voudrait réécrire son histoire. Pour le reste, il faudra utiliser le bon vieux droit de la presse (diffamation) ou dénoncer la concurrence déloyale pour essayer de se défendre.
Un espoir quand même, un projet de règlement européen, qui doit être adopté « au plus tard en 2015 » par la France et l'Allemagne devrait venir réformer la directive de 1995. Il recommanderait un réel effacement des données et pourrait étendre la protection des données personnelles à certaines informations concernant les entreprises.

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

Source : http://www.lesechos.fr/enjeux/les-plus-denjeux/idees/0203967538313-pas-encore-de-droit-a-loubli-pour-lentreprise-1074046.php
par Valérie de Senneville

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

L'arrêt rendu ce matin par la Cour de Justice de l'Union européenne en matière de vidéosurveillance risque d'avoir de douloureux effets en France. Il remet en effet en cause les efforts du ministère de l'Intérieur pour se passer de la CNIL dans l'installation des caméras de « vidéoprotection. »

Les faits examinés par la CJUE visait le cas d'un Tchèque ayant installé une caméra de surveillance chez lui, mais dont le champ de vision débordait sur la voie publique. Les flux étaient stockés sur disque dur, chez lui. Par ce biais, ce particulier avait finalement permis à la police d'identifier une personne suspectée d'avoir caillassé les fenêtres de sa maison. Cependant, la CNIL locale lui a infligé une amende, faute pour ce particulier d'avoir zappé le consentement préalable des personnes filmées. On pourra revoir notre actualité sur les solutions proposées par la Cour, mais l'important n'est peut-être pas là car l'arrêt est supposé provoquer un vent de panique en France, au ministère de l'Intérieur. Explication.

Vidéosurveillance, donnée personnelle, traitement automatisé

La Cour a en effet posé qu'en principe la vidéosurveillance relevait du champ d'application de la directive de 1995 sur les données personnelles, du moins « dans la mesure où elle constitue un traitement automatisé ». Cette analyse fait suite à un développement très logique :
La donnée personnelle embrasse « toute information concernant une personne physique identifiée ou identifiable. »
Est réputée identifiable « une personne qui peut être identifiée, directement ou indirectement, notamment par référence […] à un ou plusieurs éléments spécifiques, propres à son identité physique.»
Du coup, « l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel (…) dans la mesure où elle permet d'identifier la personne concernée ». En clair, une caméra de vidéoprotection capte donc des données à caractère personnelles quand les personnes filmées sont identifiées ou identifiables.
Mais y a t-il pour autant traitement automatisé de ces données ? La directive de 95 définit ce traitement par « toute opération ou [tout] ensemble d'opérations […] appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement […] la conservation ». La CJUE considère donc qu' « une surveillance effectuée par un enregistrement vidéo des personnes (…) stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue (…) un traitement de données à caractère personnel automatisé. »

Fort de ces enseignements, auscultons le régime français.

Les contrariété du régime français de la « vidéoprotection »
Une circulaire du 14 septembre 2011 décrit le cadre juridique applicable à l'installation de caméras de vidéoprotection, terme officiel pour repeindre de manière plus sympathique les outils de vidéosurveillance. Cette circulaire est importante puisqu'elle définit les (rares) cas où les autorités doivent effectuer une déclaration préalable auprès de la CNIL, et quand elles peuvent (très souvent) s'en passer.
Deux hypothèses sont envisagées par cette circulaire qui vient faciliter l'application du Code de la sécurité intérieure : des caméras installées sur la voie publique, des caméras installées sur des lieux non ouverts au public.

Les caméras installées sur la voie publique

Les caméras installées sur la voie publique (et dans des lieux ou établissements ouverts au public) nécessitent l'autorisation préalable du préfet après avis de la commission départementale de la vidéo protection. Donc sans passer par la CNIL.
Cependant, parfois, ce passage CNIL est nécessaire. Le ministère de l'Intérieur, épaulée par un avis du Conseil d'État (non public et concernant les caméras dans les prisons) l'estime inévitable seulement « si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment). »
Décodons : en France, lorsque le flux permet l'identification via un système de reconnaissance faciale (ou de plaque d'immatriculation), il faut passer par la CNIL. L'Intérieur en déduit naturellement que « le seul fait que les images issues de la vidéoprotection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéoprotection lui-même. »

On le voit, ce point est en exacte contradiction avec ce que vient de juger la CJUE : des personnes, une caméra, un flux, un stockage, nous voilà déjà plongé jusqu'au cou en Europe dans le règne du traitement automatisé de données personnelles. La France, pourtant un État membre, estime qu'il n'y a pas de traitement automatisé (donc pas de passage par la CNIL) faute de flux couplé à une reconnaissance faciale ou de plaque d'immatriculation. Un critère totalement surabondant !

Les caméras installées dans les lieux non ouverts au public

La circulaire précitée évoque aussi les caméras installées dans les lieux non ouverts au public (soit partout ailleurs que les voies publiques, la résidence privée ou la voiture). Ce régime n'est pas de la compétence de l'Intérieur, mais celui-ci donne malgré tout des pistes : il faut là encore l'avis de la CNIL « lorsque ces personnes sont identifiables ».

La Place Beauvau pose ici deux critères cumulatifs :
D'une part des images qui font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage.
D'autre part, une identification possible parce que le lieu est fréquenté par des personnes « dont une partie significative est connue du responsable du système de vidéoprotection ou des personnes ayant vocation à visionner les images enregistrées. »

Cependant, ces deux critères ne se retrouvent pas dans les textes fondateurs :
Si la captation n'est pas un traitement selon l'Intérieur, la loi de 1978 tout comme la directive disposent que la collecte et la transmission le sont bien.
Le critère de la « connaissance » des personnes filmées par celui derrière la caméra est quelque peu restrictif : une reconnaissance indirecte est normalement suffisante, d'autant que même si personne ne peut identifier Mme Michu sur son écran de contrôle, elle aura son image et pourra le faire par la suite.

Enfin, le critère de la « partie significative » n'est pas intégré dans les textes socles.
Bref, l'arrêt rendu ce matin par la CJUE devrait naturellement amener la CNIL à se pencher plus en profondeur sur le régime français, et l'Intérieur à revoir le périmètre de ses yeux électroniques. D'autres actualités seront à suivre en fonction des retours obtenus auprès de ces deux acteurs.

Consultez l'arrêt de la Cour de Justice de l'Union Européenne de l'affaire C-212/13

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

Source : http://www.nextinpact.com/news/91367-quand-videosurveillance-europeenne-contrarie-videoprotection-francaise.htm#/page/1
par Marc Rees

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

Parallèlement aux grands dossiers à caractère géopolitique, la World Policy Conference, dont les travaux de sa septième édition viennent de s'achever à Séoul, a planché sur un problème lié à un autre genre d'actualité : l'émergence du Big Data et ses conséquences économiques et politiques.

La situation actuelle au Moyen-Orient ainsi que la place grandissante qu'occupe l'Asie dans le nouvel ordre mondial – dossiers liés à l'actualité internationale – ont été au centre de la 7e édition de la World Policy Conference (WPC) qui s'est tenue du 8 au 10 décembre à Séoul (voir L'Orient-Le Jour des 8, 9 et 10 décembre). Mais parallèlement, et dans le but d'élargir le débat et d'étendre les échanges de connaissances à un champ plus large que la sphère purement politique, les congressistes réunis dans la capitale coréenne ont planché dans le même temps sur des thèmes à caractère sociétal en rapport avec le changement climatique, l'énergie, l'environnement, les défis que pose le phénomène de Big Data, sans compter les rapports agroalimentaires entre l'Asie et l'Afrique. Autant de sujets liés aussi à l'actualité, mais une actualité d'un autre genre. Celle qui concerne les populations dans le détail de leur vie quotidienne et qui influe sur leur niveau de vie.

Le développement exponentiel de la révolution numérique est à n'en point douter l'un des principaux domaines qui touche de près le citoyen lambda. À l'ouverture de la session consacrée aux conséquences économiques et politiques du Big Data, le modérateur du débat, Nicolas Barré, directeur adjoint du quotidien Les Échos, indiquait, en guise d'entrée en matière, qu'en l'an 2000, un quart des données dans le monde étaient sous forme numérique. Aujourd'hui, cette proportion est quasiment de 100 pour cent. Et dans ce bouleversement vertigineux, l'Asie joue un rôle central. C'est du moins ce qu'affirme Chang Due Whan, président d'un géant médiatique en Corée du Sud, le Mackyung Media Group, qui possède, notamment, un quotidien, qui tire à un million d'exemplaires, ainsi que quinze de chaînes de télévision.

Évoquant les circonstances de cette révolution du XXIe siècle, Chang Due Whan souligne que la plupart des nouvelles inventions dans le domaine numérique viennent d'Asie. Il en déduit que cette zone sera la force motrice du secteur des appareils numériques, tels que les smartphones ou les phablets (combinaison du téléphone et de la tablette). Le développement dans ce domaine est tellement rapide que nombre d'utilisateurs estiment déjà que le PC est devenu obsolète et qu'il est de plus en plus évincé par la nouvelle génération de téléphones portables. Et dans ce cadre, souligne Chang Due Whan, la nouvelle technologie 5G va accroître considérablement le flux d'informations.

C'est précisément sur ce plan qu'intervient le problème du Big Data, en ce sens qu'il représente la capacité d'avoir accès, d'analyser et d'exploiter la quantité gigantesque de données disponibles, ce qui implique la création et l'utilisation efficace des outils permettant l'exploitation des données versées sur le marché un peu partout dans le monde. « Le Big Data est le nouveau pétrole », affirme à cet égard Chang Due Whan.
Le rythme de l'expansion de ce secteur d'activité a été mis en évidence par Luc-François Salvador, président exécutif pour l'Asie-Pacifique du groupe Capgemini, qui affirme que 90 pour cent des données actuelles ont été créées ces deux dernières années, et ce volume de données disponibles double chaque année. Conséquence prévisible : de nouveaux outils sont créés pour analyser et exploiter ces data. À titre d'exemple, Google a mis en place un système de gestion des maladies de manière à prévoir les dates, ou plus précisément les périodes, auxquelles apparaissent les grippes dans une région déterminée. Autre exemple dans ce domaine : au Japon, des chercheurs planchent sur l'analyse des données que l'on peut tirer de la façon de… s'asseoir ! La manière de s'asseoir devient ainsi une sorte de « signature » propre à la personne considérée.

La protection des données
Cette accumulation des données, notamment personnelles, à un rythme exponentiel, ainsi que la capacité grandissante d'analyser et d'exploiter de telles informations posent, à l'évidence, le problème de la protection des données personnelles et les craintes d'un fâcheux impact qui pourrait se manifester au niveau de la liberté de l'individu. Plusieurs intervenants ont évidemment soulevé ce point précis lors du débat. M. Salavador a ainsi relevé que le Big Data permet d'enregistrer des progrès énormes au niveau du traitement de certaines maladies ou aussi dans les projets d'urbanisme, mais dans le même temps, il pose le problème de la protection des données personnelles, ce qui implique la nécessité de concevoir les moyens dont devrait bénéficier le citoyen pour s'assurer une protection adéquate face au Big Data.

Cette question a été soulevée par un expert et consultant américain, Ben Scott, qui a affirmé qu'il se profile à l'horizon, du fait de ce problème, une perte de confiance de la population dans les gouvernements et les pratiques démocratiques, et, surtout, dans les outils informatiques, ce qui risque de pousser les individus à hésiter de trop s'engager dans l'utilisation des nouveaux outils ou applications numériques.

Un professeur universitaire américain, Joseph Nye, a relevé dans ce cadre que la capacité de traitement des données double chaque deux mois, de sorte que les citoyens vivant dans des pays démocratiques finissent par exprimer leurs appréhensions concernant l'exploitation des données personnelles. Certes, certaines personnes soulignent qu'au nom de la sécurité, face aux menaces terroristes, notamment, elles sont disposées à sacrifier de leur liberté ou de leur confidentialité. Cela pose, relève Joseph Nye, le problème de l'absence, au stade actuel, de contre-pouvoirs dans ce domaine.

Le Big Data risque-t-il ainsi de rendre quelque peu réel le danger de l'émergence d'un Big Brother ? Intervenant dans le débat, le député israélien de gauche Meir Sheetrit a apporté une nuance dans la nature du danger qui plane à cet égard, soulignant que le Big Data n'est pas exclusivement contrôlé par les gouvernements, mais il est aussi contrôlé et exploité surtout par les grandes entreprises, d'où la nécessité de protéger également les populations contre certaines grandes entreprises privées. Joseph Nye relèvera à ce propos que c'est dans la mesure où les données sont partagées entre plusieurs entreprises puissantes que le danger se fait plus grand au niveau de la confidentialité et de la liberté de l'individu.
Le débat sur ce plan est donc ouvert à l'échelle planétaire. Les experts et hauts responsables qui planchent sur la question feraient bien de proposer sans trop tarder des mesures concrètes en termes de protection des libertés individuelles avant que la situation dans ce domaine n'échappe à tout contrôle.

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

Source : http://www.lorientlejour.com/article/900564/la-wpc-participe-au-debat-le-big-data-debouchera-t-il-sur-un-big-brother-.html
par Michel TOUMA

Un label qualitatif pour le Cloud

Un label qualitatif pour le Cloud

Le 9 Décembre 2014, le label « Cloud Confidence » a officiellement été lancé par l'association du même nom. Cette certification est destinée à certifier la qualité d'un service Cloud en matière de sécurisation et de confidentialité des données et ne sera délivrée qu'à des offres à destination d'un des pays de l'Espace Economique Européen (EEE).

L'association « Cloud Confidence », fondée en Juillet 2014, est une association française qui regroupe 15 membres fournisseurs de services et de solutions cloud. Son but étant « de promouvoir la confiance dans les activités de Cloud entre professionnels et utilisateurs ».
Ce label « Cloud Confidence », centré sur la protection et la confidentialité des données clients, n'est pas la seule certification Cloud sur le marché français. Le réseau de clusters numérique « France IT » certifie depuis un an, les offres avec un point de vue généraliste. Plus proche du Cloud Confidence, le référentiel online publié par l'Agence Nationale de la Sécurité des Systèmes d'Information qui évalue le niveau sécuritaire des prestations Cloud.

Cette multiplication de labels prouve une nouvelle fois la place de plus en plus importante prise par le Cloud sur le marché des Télécoms depuis quelques années. Il est désormais presque indispensable pour une entreprise de sécuriser au maximum ses données et ce, en passant par une solution Cloud. Les nuages ne sont donc pas forcément annonciateurs de mauvais signes…

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

Source : http://www.categorynet.com/communiques-de-presse/internet/un-label-qualitatif-pour-le-cloud-20141211224524/

Un système de traitement automatisé de données personnelles non déclaré à la Cnil ne peut servir de preuve à l'appui d'un licenciement

Un système de traitement automatisé de données personnelles non déclaré à la Cnil ne peut servir de preuve à l'appui d'un licenciement

Les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la Cnil constituent un moyen de preuve illicite, qui doit dès lors être rejeté des débats et par lequel l'employeur ne saurait ainsi justifier un licenciement.

Une assistante en charge de l'analyse financière a été licenciée pour cause réelle et sérieuse, l'employeur lui reprochant une utilisation excessive de la messagerie électronique à des fins personnelles.

La cour d'appel d'Amiens a jugé le licenciement justifié par une cause réelle et sérieuse.

Pour cela, elle a retenu que la déclaration tardive à la Commission nationale de l'informatique et des libertés (Cnil) de la mise en place d'un dispositif de contrôle individuel de l'importance et des flux des messageries électroniques n'avait pas pour conséquence de rendre le système illicite ni davantage illicite l'utilisation des éléments obtenus.

Elle a ainsi considéré que le nombre extrêmement élevé de messages électroniques à caractère personnel envoyés et reçus par l'intéressée durant les mois d'octobre et novembre 2009, respectivement 607 et 621, qui ne pouvait être considéré comme un usage raisonnable dans le cadre des nécessités de la vie courante et quotidienne de l'outil informatique mis à sa disposition par l'employeur pour l'accomplissement de son travail, devait être tenu comme excessif et avait eu un impact indéniablement négatif sur l'activité professionnelle déployée par la salariée durant la même période pour le compte de son employeur, celle-ci occupant une part très importante de son temps de travail à des occupations privées.

Dans un arrêt du 8 octobre 2014, la Cour de cassation censure la décision des juges du fond
Ceux-ci ne se sont en effet fondés que sur des éléments de preuve obtenus à l'aide d'un système de traitement automatisé d'informations personnelles avant qu'il ne soit déclaré à la Cnil, qui constituent pourtant un moyen de preuve illicite et doit dès lors être rejeté des débats.
Par Clément HARIRA

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

S o u r c e : http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/198246-un-systeme-de-traitement-automatise-de-donnees-personnelles-non-declare-a-la-cnil-ne-peut-servir-de-preuve-a-lappui-dun-licenciement.html

---

La CNIL et l'Inria vont révéler les indiscrétions

d’Android

La CNIL et l’Inria vont révéler les indiscrétions d’Android

CNIL va diffuser lundi une étude intéressante montée avec l’Inria. Elle visera à informer les utilisateurs de la masse de données personnelles passant dans les mains de leur smartphone et des applications installées. Une première campagne visait l’iPhone en avril 2013. Cette fois Android sera sur le grill.

Android, passoire ou blockhaus à données personnelles ?
Après une auscultation qui aura duré 3 ans, la CNIL va publier lundi une étude menée à bien avec l’Institut national de recherche en informatique et en automatique (Inria).
L’objet ? Révéler au grand jour les données qui sont enregistrées, stockées et diffusées par les smartphones. Alors que « plus de 30 millions de Français utilisent quotidiennement smartphones et tablettes (…) les utilisateurs savent très peu de choses sur ce qui se passe à l’intérieur de ces « boites noires » » affirment les deux entités dans un communiqué commun.

L’iPhone déjà épinglé en avril 2013
Ce projet de sensibilisation baptisé Mobilitics avait déjà fait l’objet d’une première vague de résultats en avril 2013, mais les attentions s’étaient alors concentrées sur les iPhone. Lors de cette campagne précédente, la CNIL et l’Inria avaient flairé 189 applications pour récolter 9 Go de données sur une période de trois mois. L’opération dénonçait par exemple le fait que trop d’applications et jeux aient pu obtenir l’identifiant unique de l’appareil (46 %) sa géolocalisation (33 % environ) ou avoir accès au carnet d’adresses (8 %) sans toujours pleinement justifier ces indiscrétions ou du moins informer l’utilisateur. Apple avait alors réagi en modifiant certains paramètres, notamment concernant l’accès à l’UDID

« De nombreux acteurs tiers sont destinataires de données, par l’intermédiaire d’outils d’analyse, de développement ou de monétisation présents dans les applications. Les analyses permettent d’identifier plusieurs acteurs recevant des informations récupérées par l’intermédiaire de cookies spécifiques aux applications. Les acteurs classiques du traçage en ligne sont déjà très présents au sein de certaines applications, mais les chiffres montrent également l’émergence d’acteurs nouveaux dédiés au mobile » remarquait alors la CNIL. Du coup, celle-ci réclamait des magasins d’application de nouveaux modes d’information « des utilisateurs et de recueil du consentement. »

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

Source : http://www.nextinpact.com/news/91332-la-cnil-et-l-inria-vont-reveler-indiscretions-d-android.htm