WHOIS : vos informations personnelles bientôt publiques ? | Le Net Expert Informatique

L'ICANN pourrait bientôt modifier le système du WHOIS. Le régulateur propose notamment d'interdire aux propriétaires de sites « à but commercial » de s'enregistrer via proxy, soit de façon anonyme. Le texte ne laisse pas les associations insensibles, qui y voient une menace pour ceux qui s'expriment librement sur leurs sites.

WHOIS est souvent décrit comme l'annuaire d'Internet. Lors de l'enregistrement d'un nom de domaine, un internaute doit renseigner diverses informations personnelles, de son état civil à son numéro de téléphone en passant par son adresse de domicile. Ces informations alimentent les bases de données des registres de noms de domaine, et sont consultables via l'outil WHOIS.
Pour des questions évidentes de protection de la vie privée et de confidentialité, les données fournies par le propriétaire d'un nom de domaine ne sont pas accessibles au public. Les registres de renseignement proposent fréquemment en option la possibilité de s'enregistrer via proxy. Les seules tierces personnes alors en mesure d'accéder aux bases de données non anonymisées sont celles détenant une autorisation légale, tel qu'un mandat judiciaire.
Mais cette situation connaîtrait ses derniers jours. L'ICANN prévoit en effet de modifier le système en profondeur. Le régulateur étudie actuellement un projet, lequel envisage notamment que les noms de domaine « utilisés dans un but commercial soient inéligibles à l'enregistrement proxy/privacy ». En d'autres termes, les propriétaires de sites contenant un quelconque élément transactionnel ne pourront plus s'enregistrer de façon anonyme : leurs informations personnelles devront être publiques.

L'anonymat, garant de la liberté d'expression
Alors que l'ICANN doit se prononcer le 7 juillet sur ce texte, l'Electronic Frontier Foundation appelle les internautes à s'y opposer. Selon l'EFF, le terme « but commercial » englobe un grand nombre de sites, et la vie privée de leurs propriétaires, des personnes physiques, seraient menacée. L'association prend pour exemple TG Storytime, un site destiné aux auteurs transgenres et hébergés par Joe Six-Pack, lui-même transgenre. Si l'ICANN devait modifier la régulation en vigueur, ses adresses, numéros de téléphone et mails seraient alors exposées à la vue de tous, trolls et harceleurs compris.
Le changement a été impulsé par les géants américains du divertissement, signale l'EFF, ce que l'ICANN ne cache pas. En effet, à de nombreuses reprises, le régulateur d'Internet écrit que cette proposition vise à faciliter le signalement de sites violant le droit d'auteur (ou toute autre propriété intellectuelle). Pour l'EFF, « ces entreprises veulent de nouveaux outils pour découvrir l'identité des propriétaires de sites Web qu'ils veulent accuser de violation de droit d'auteur et contrefaçon de marque, de préférence sans une ordonnance du tribunal ».
« L'avantage limité de cette évolution est manifestement compensé par les risques supplémentaires pour les propriétaires de sites, qui vont souffrir d'un risque plus élevé de harcèlement, d'intimidation et de vol d'identité ».
Il est vrai que, malgré les gardes fous prévus par l'ICANN, la plupart des informations fournies pour l'enregistrement d'un nom de domaine sont sensibles, tant IRL (In Real Life) que dans le monde virtuel. En appelant à s'opposer au texte, l'association entend faire réagir sur un recul de l'anonymat, qui affectera ceux qui portent des opinions impopulaires ou marginales mais aussi les lanceurs d'alerte et tous ceux susceptibles de dénoncer « la criminalité et la corruption ».

Source : http://www.linformaticien.com/actualites/id/37199/whois-vos-informations-personnelles-bientot-publiques.aspx
Par Guillaume Périssat

Chief Digital Officer (CDO) – Qui et pour faire quoi au juste ? | Le Net Expert Informatique

Chief Digital Officer (CDO) – Qui et pour faire quoi au juste ?

Acteur de la transformation numérique, le CDO apparaît dans l'organigramme de 22% des entreprises françaises interrogées. Ils devraient être 37% en 2016. Mais pour « transformer, fédérer et piloter », ce profil hybride n'a pas toujours la vie facile.

C'est la formule du moment : la transformation numérique. Tous les secteurs, ou presque, sont concernés ou le seront dans les prochaines années. Le « digital » n'est « plus – et ne doit plus être –un canal (de vente, de communication, de relation client), mais un outil de transformation des organisations et des métiers » écrit Novedia, partenaire du 1er baromètre des CDO (http://www.viseo.com/fr/telechargement/resultats-du-barometre-cdo-2015).

Le numérique se déploie en entreprise donc. Et pour accompagner et piloter cette transformation, celles-ci créent parfois un poste dédié : le Chief Digital Officer ou directeur du numérique. Ils ne sont toutefois pas légion, et essentiellement présents dans les grandes entreprises d'après l'étude réalisée auprès de 201 dirigeants français.

Les services et grandes entreprises plus concernés

22% des sondés déclarent disposer d'un CDO, dont 37% parmi les sociétés de plus d'un milliard d'euros de chiffre d'affaires – contre seulement 5% pour celles réalisant moins de 250 millions d'euros de CA. En 2016, 37% des entreprises auront un patron du numérique selon le baromètre.

Mais à quoi ressemble ou devrait ressembler ce fameux CDO ? Pour 65% des répondants, cette fonction doit être rattachée au Comex. Ils sont seulement 17% à le lier à la DSI et 14% au marketing. La stratégie numérique devrait donc se piloter d'en haut. Néanmoins, un tiers des CDO interrogés regrettent « que leur niveau hiérarchique et leur pouvoir sont inadaptés aux enjeux de leur fonction. »

Et une fois nommé, en quoi consisteront, dans les grandes lignes, les tâches du CDO ? « Transformer, fédérer et piloter » d'après les données recueillies. C'est un peu vague oui, mais il faudra faire avec. Cela semble néanmoins rejoindre les conclusions d'une autre étude soulignant le fait que les enjeux de la transformation numérique étaient organisationnels avant d'être techniques.

Existe-t-il une voie royale au poste de CDO et quelles compétences ce dernier doit-il posséder ? Ce « gendre idéal » ne paraît pas avoir de contours prédéfinis. Trois grandes sensibilités néanmoins : technologie, marketing et métiers. Dans quelles proportions ? Difficile à dire… Un peu de tout.

Un hybride pour affronter les freins culturels

Les répondants estiment donc que le CDO doit être doté d'une culture hybride. Cela se traduit par un profil caractérisé notamment par « Transversalité, compréhension des enjeux marketing et IT », « une bonne culture des métiers » et une capacité à « Expliquer et convaincre, fédérer, briser les silos ».

Mais pour cet acteur nommé pour amorcer du changement dans l'entreprise, tout n'est pas simple. Pour 43% des sondés, le CDO est confronté aux freins culturels à la transformation. 19% estiment en outre qu'il manque de budget pour remplir son office.

La problématique n'est pas franchement nouvelle : le changement provoque des résistances et se heurte à une certaine forme d'inertie héritée d'années de pratique. « C'est une relation disruptive avec les autres fonctions : le CDO remet en cause la façon dont les autres fonctionnent » commente par exemple un répondant. Bon courage donc.

Source : http://www.zdnet.fr/actualites/chief-digital-officer-cdo-qui-et-pour-faire-quoi-au-juste-39821562.htm
Par Christophe Auffray

Montres connectées : vos données personnelles sont peut-être en danger | Le Net Expert Informatiquedc

Montres connectées : vos données personnelles sont peut-être en danger

Des chercheurs en sécurité n'ont pas eu trop de mal à récupérer des données personnelles à partir des montres connectées LG G Watch et Samsung Gear 2 Neo.

Les révélations sur les possibilités d'intrusion et de récupération de données personnelles dans les téléphones portables par les agences de renseignement américaines dévoilées dans les documents d'Edward Snowden ont conduit les éditeurs de plates-formes mobiles à relever les niveaux de sécurité, notamment par le chiffrement systématique des données personnelles et documents dans les appareils mobiles.
Et pour les montres connectées, ces gadgets qui fleurissent (ou aimeraient le faire) sur les poignets ? Une publication de chercheurs de l'Université de New Haven suggèrent que si des hackers ont besoin d'information, ils feraient bien de commencer par cette porte d'entrée.
Il n'ont pas rencontré énormément de difficultés pour obtenir différentes informations personnelles, que ce soit avec la LG G Watch (agenda, contacts, adresses email, données du podomètre) sous Android Wear ou la Samsung Gear 2 Neo (messages, emails, contacts, données de santé) sous Tizen OS….d'autant plus que ces données n'étaient pas chiffrées.
Avec la multiplication des objets connectés qui seront autant de points d'entrée théoriques à différents types de données personnelles, cette petite expérience a de quoi faire réfléchir, alors que des objets comme les montres connectées ont justement besoin d'un large accès aux données personnelles pour être pleinement efficaces, comme dans le cas de Google Now sur Android Wear.
Chiffrer les données sur les montres connectées (et les objets connectés en général) serait une bonne chose, mais encore faut-il que ce soit fait correctement, préviennent les chercheurs. Un certain nombre de failles exploitées par les agences de renseignement (mais aussi les méchants hackers) sont justement des attaques de type man-in-the-middle qui outrepassent ces protections sans même avoir à les casser.
A voir si la montre Apple Watch, en cours d'analyse à l'Université de New Haven, saura mieux préserver la vie privée de son possesseur. Il vaudrait mieux, étant donné les volumes de plusieurs dizaines de millions d'unités qui son censés être écoulés dès cette année…

Source : http://www.generation-nt.com/lg-watch-samsung-gear-montre-protection-donnees-actualite-1915829.html

Protection des données personnelles : les entreprises bel et bien contraintes | Le Net Expert Informatique

	Protection des données personnelles : les entreprises bel et bien contraintes

Pensée pour protéger le citoyen, la loi Informatique et libertés est de plus en plus détournée de son objectif premier. Tant par les salariés que par les entreprises elles-mêmes, qui n'hésitent plus à s'en servir comme arme concurrentielle. L'analyse de l'avocat François Coupez.

La protection des données à caractère personnel est née en France avec la loi du 6 janvier 1978 dite « Informatique et libertés ». Le texte a été modifié en 2004 (à la suite de la directive européenne 95/46), et il est destiné à l'être à nouveau par le projet de loi sur le numérique annoncé en grande pompe depuis deux ans maintenant… avant d'être de toute façon complètement remplacé par un projet de règlement européen (http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do%3Freference=2012/0011(COD)%26l=fr) encore en discussion qui unifiera en 2017 ou 2018 le droit de tous les pays de l'Union européenne sur le sujet.

Si ces différents projets visent à accroître de façon très importante les sanctions financières, ils ont également pour but de permettre une application plus efficace des règles (droit à l'oubli numérique/au déréférencement, co-responsabilité des sous-traitants, etc.). Mais en parallèle, on constate depuis quelques années le développement d'une véritable instrumentalisation de cette protection légale, aux règles extrêmement formelles et aux impacts potentiellement dévastateurs[1] sur l'image des entreprises prises en faute.

Salariés et clients, quand le pouvoir change de camp

Historiquement, la CNIL a eu l'occasion d'appliquer les principes de la loi « Informatique et libertés » dans plusieurs domaines, avec la plupart du temps deux points communs : d'une part la protection des clients contre l'utilisation qui serait faite de leurs données en contradiction avec les règles applicables et, d'autre part, la protection des salariés dans des hypothèses de surveillance abusive, de discrimination ou de mode d'évaluation des performances illicites.
Dans les deux cas, l'action de la CNIL conduit souvent l'entreprise fautive à revoir beaucoup plus globalement l'ensemble de ses processus et leur conformité.
Or les difficultés pratiques concernant le respect de cette réglementation pour l'entreprise ne doivent pas être sous-estimées. Elles tiennent tant à son formalisme qu'à ses conditions d'application, étant entendu que les traitements de ce type de données se développent de façon exponentielle avec la transformation numérique. De plus, l'entreprise, confrontée à un lacis réglementaire croissant et dans tous les domaines, alloue parfois ses ressources pour se mettre en conformité en fonction de l'urgence, ou du risque réel de sanction. Les entreprises ne peuvent ainsi pas toujours prétendre réussir un sans-faute en matière de protection des données personnelles… et en sont pleinement conscientes.
En parallèle, un phénomène se développe depuis quelques années, à un point tel qu'il se généralise. Sentant la faille, des clients ou des salariés bien informés n'hésitent plus à l'utiliser, non pour faire valoir leurs droits en la matière, mais pour faire pression dans le cadre d'un contentieux ou d'une revendication autre. La réglementation devient alors un simple prétexte destiné à faire plier son opposant.
Concernant le cas des clients, cela concerne souvent les entreprises disposant de nombreux points de contact avec la clientèle (et disposant de nombreux conseillers clientèles, etc.). Dans les grands réseaux, il est toujours plus difficile de faire respecter à tous les salariés en contact avec la clientèle les règles de base (notamment concernant la zone de « bloc-note » ou de note en champ libre sur les fiches clients, propices à tous les excès), ce qui multiplie les hypothèses de manquements ;
Quant aux salariés, il est de plus en plus fréquent qu'ils fassent jouer leurs droits en la matière. Par exemple, l'une des pratiques les plus fréquentes est de systématiquement avoir recours au droit d'accès aux données personnelles que leur employeur collecte sur eux, lorsque le contrat de travail arrive précocement à son terme, ou que les deux parties se retrouvent aux Prud'hommes. La pratique montre ainsi que, sur l'ensemble des personnes pouvant faire valoir leur droit d'accès dans le cas de traitements réalisés par une entreprise, près de 75% des demandes proviennent de l'interne et donc des salariés. Ainsi, il n'y a qu'à regarder la jurisprudence en droit social ces dernières années pour s'apercevoir qu'il est devenu aussi courant d'alléguer un traitement de données personnelles contraire à la loi, et donc de l'illicéité du moyen de preuve opposé à un salarié, que d'en appeler aux pages Facebook en matière de divorce. Un exemple récent nous vient de l'arrêt de la Cour d'appel de Rouen rendu le 12 mai 2015 qui invalide les preuves concernant d'une part un système de badgeage (pas d'information du comité d'entreprise) et d'autre part un logiciel permettant de contrôler les horaires des salariés (pas de formalités CNIL) : le licenciement est ainsi considéré comme étant sans cause réelle ni sérieuse.

Maintenant les contentieux… entre entreprises ?

Ce qui est plus marquant encore, c'est que ce phénomène est en passe de gagner les relations entre entreprises.
Alors que l'on s'attend à ce que ce soit la victime (client, salarié, etc.) qui fasse valoir les droits qui lui sont reconnus, les tribunaux sont en effet saisis de façon croissante de manquements à cette réglementation allégués par… des sociétés concurrentes.
Pour mettre fin à un partenariat commercial, annuler une vente, tenter de prouver une rupture abusive des relations commerciales ou empêcher un concurrent de commercialiser un service innovant, les hypothèses se multiplient dans lesquelles des tribunaux de tout type sont confrontés à cette situation.

En voici quelques exemples :

le 25 juin 2013, la Cour de cassation a rendu une décision conduisant à l'annulation de la vente d'un fichier de clients informatisé. Dans cette affaire, les associés d'une entreprise avaient vendu pour 46 000 € le seul fichier des clients de l'entreprise, fort de 6 000 clients référencés depuis 1946. Or pour l'acheteur ayant utilisé quelques semaines cette base, celle-ci était une coquille vide de 1 950 clients actifs seulement. Il en demandait donc le remboursement… qu'il obtint : pour la Cour de cassation, l'absence du respect des formalités CNIL rend toute commercialisation du fichier impossible, la vente ayant nécessairement un objet illicite.
À la suite d'une décision de la CNIL du 8 septembre 2011 autorisant pour la première fois une entreprise à traiter pour des raisons commerciales le numéro NIR (aussi appelé « numéro de sécurité sociale »), une entreprise concurrente a formé un recours considérant que l'interprétation était contestable au sens de la loi Informatique et libertés et qu'elle conduisait à un avantage concurrentiel injustifié. C'était le premier recours intenté à l'encontre d'une décision d'autorisation, alors qu'en général – et logiquement – les recours sont formés en cas de refus de la CNIL. Or, le Conseil d'État, s'il a confirmé la décision de la CNIL le 26 mai 2014, a surtout reconnu le droit à agir de la société concurrente dans cette affaire (voir, à ce sujet, l'excellent article de Guillaume Desgens-Pasanau dans Expertises N° 397 de Décembre 2014: « Données personnelles : ouverture de l'usage du NIR au secteur privé »).
Dans une affaire récente de rupture abusive alléguée de relations commerciales, la société se plaignant de la rupture (société B) proposait à l'autre société (A) de numériser pour elle des documents dans lesquels figuraient des données personnelles, et d'effectuer cette prestation depuis le Vietnam. La société A aurait donc dû demander l'autorisation de la CNIL du fait des flux de données vers ce pays, ce qu'elle n'a pas fait. Inaction qui, pour la société B, constitue un élément de preuve que la société A ne croyait en réalité pas au projet et ne comptait pas sérieusement contracter avec elle. La Cour d'appel de Paris toutefois, pour des raisons de défaut de preuve, n'a pas suivi cette analyse et a considéré le 10 avril 2015 qu'il n'y avait pas de rupture abusive.

Le grand classique des contentieux de demain ?

On le voit à travers ces quelques exemples jurisprudentiels récents, le phénomène va croissant. Il est surtout appelé à prendre encore de l'ampleur avec le futur projet de règlement européen, qui conduit à remplacer les formalités préalables par un contrôle constant de conformité et oblige donc à documenter la façon dont les traitements sont opérés à toutes les étapes. Or toutes ces informations forment un vivier de preuves de ce qui a été fait (ou pas), destinées au régulateur… et qui pourraient facilement être utilisées par une société concurrente dans le cadre d'un procès.
Plus globalement, les entreprises doivent prendre conscience de cette évolution et en saisir toutes les opportunités, mais également tous les risques : il semble logique que les études de risque, réalisées préalablement à la mise en œuvre de traitement de données à caractère personnel, aient également à prendre en compte cette nouvelle donne…

A terme en effet, en cas de contentieux et dès que l'on parlera de près ou de loin de données, la vérification de la licéité des traitements de données personnelles de l'entreprise adverse pourrait devenir un préalable aussi convenu que la vérification des pouvoirs du signataire d'un acte.

Si cette évolution peut paraître critiquable car compliquant encore les dossiers en justice, elle est malgré tout le signe que la réglementation sur les données personnelles s'ancre profondément dans les habitudes. Un réel progrès, et qui n'était pas chose évidente il y a encore quelques années…

[1] Certes, 17 textes pénaux prévoient une sanction de 5 ans d'emprisonnement et de 1 500 000 € d'amende pour les entreprises qui enfreindraient les règles en la matière, mais les applications jurisprudentielles sont rarissimes. Les sanctions de la CNIL sont quant à elles beaucoup plus fréquentes, avec des montants financiers pour le moment limités à 150 000 € (le double en cas de récidive), seul Google inc. ayant été condamné à une telle peine. Leur efficacité est fortement renforcée par leur publication (fort effet d'image sur les grandes entreprises).

Source : http://www.silicon.fr/protection-donnees-personnelles-loi-instrumentalisee-116895.html
Par François Coupez, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies

---

L'employé, la première faille de sécurité | Le Net Expert Informatique

L'employé, la première faille de sécurité

Si les entreprises se concentrent toujours sur leur protection informatique vis-à-vis des intrusions externes, se méfient-elles assez de leurs propres employés ? Pas toujours à en croire certaines histoires de ces dernières années.

L'ennemi a beau souvent être à l'extérieur de l'entreprise, il n'en reste pas moins que les employés eux-mêmes peuvent devenir de véritables problèmes, à plus ou moins grande échelle. Bien entendu, les plus grands risques internes sont faits à l'insu du collaborateur, du fait de son manque de technique et/ou d'attention, mais parfois, l'acte malveillant est réellement sciemment.

L'affaire Coca Cola

Fin 2013, le géant Coca Cola, qui compte tout de même près de 130 000 employés, s'est par exemple rendu compte qu'elle avait été victime durant de longues années d'un voleur d'ordinateurs portables. L'employé en question a ainsi dérobé 55 ordinateurs sur plusieurs années, volant ainsi des données sur environ 74 000 personnes, la plupart étant des employés du géant américain ou des collaborateurs reliés à la firme.

Réalisé par un employé (au nom inconnu) ayant en charge les équipements informatiques, non seulement l'acte en lui-même a sonné comme une véritable claque pour la firme US, mais surtout, parmi toutes les données concernées, 18 000 concernaient les numéros de sécurité sociale, données particulièrement sensibles outre-Atlantique.

Pire encore, selon un mémo de Coca Cola envoyé aux employés et révélé par le Wall Street Journal, aucune des données volées n'était chiffrée. Nous apprenons aussi qu'afin d'éviter la panique, le spécialiste de la boisson gazeuse a tenté de résoudre le problème en secret durant plusieurs semaines. Les vols ont ainsi été remarqués en décembre 2013, mais la firme a attendu le 24 janvier pour en informer ses employés.

Plus que le côté technique, cette histoire nous montre donc que la sécurité est aussi (surtout ?) une question de processus. La « faille » de Coca Cola ainsi été humaine et organisationnelle plus qu'autre chose.

Boeing aussi

Coca n'est toutefois pas la seule très grande compagnie concernée par ce genre de problématique. En 2006, un employé de Boeing a par exemple été licencié non pas pour avoir dérobé du matériel et des données, mais du fait de sa responsabilité dans un vol d'ordinateur. Le collaborateur a ainsi enfreint les règles de l'entreprise en téléchargeant des informations confidentielles sur son PC portable sans même les chiffrer.

Problème, l'employé avait téléchargé des données personnelles de 380 000 employés actuels et passés de la compagnie, comme des numéros de sécurité sociale, des noms, des adresses, etc. Le tout fut ensuite volé en décembre 2006, entraînant le licenciement du collaborateur.

Cette faute grave n'était pas une première, puisque selon le porte-parole de Boeing, deux autres vols d'ordinateurs portables contenant des données sur les employés ont été dérobés entre 2005 et 2006. « Nous encourageons les gens à travailler hors du serveur, ce qui permettrait de garder l'information derrière le pare-feu. Si vous téléchargez des informations sur votre ordinateur portable, cela est censé être temporaire et l'information est censée être cryptée » a bien insisté Boeing à l'époque. Du simple bon sens a priori peu respecté par certains de ses employés.

Moralité de ces deux histoires : la sécurité est avant tout une affaire d'organisation, de processus et de règles. S'il est évident qu'il faut se prémunir des actions malintentionnées extérieures, « l'ennemi » peut aussi être à l'intérieur, que ce soit du fait d'actes réalisés délibérément ou non. BYOD ou non, les comportements des employés peuvent être cruciaux pour la sécurité de l'entreprise. Rédiger une politique stricte et mettre en place des systèmes de surveillances (ou au moins de vérification), notamment pour ceux manipulant des données sensibles, est ainsi indispensable si l'on veut éviter de lourdes déconvenues…

Source : http://www.zdnet.fr/actualites/l-employe-la-premiere-faille-de-securite-39819662.htm

Protection des données. Un accord européen possible le 15 juin | Le Net Expert Informatique

Un accord pour adapter la législation européenne sur la protection des données personnelles à l'essor de l'internet est à portée de main et peut être conclu le 15 juin.

Jeudi soir à Bruxelles, l'Allemagne, la France, le Luxembourg et la Commision européenne ont assuré qu'un accord sur la protection des données pourrait voir le jour d'ici à trois semaines.
« Nous sommes dans la dernière ligne droite et nous voulons aboutir », a déclaré le ministre allemand de l'Intérieur, Thomas de Maizière, au cours d'un débat sur la protection des données avec les ministres de la Justice de la France, du Luxembourg et la commissaire européenne Vera Jourova.
« Nous sommes sur la voie d'un accord général. Le texte est inachevé, mais il est bon », a confirmé Mme Taubira. « Nous avons en perspective un accord le 15 juin » lors de la réunion des ministres européens de la Justice à Luxembourg, a renchéri la commissaire Jourova.

Protéger les citoyens européens

L'objectif de cette nouvelle législation est d'empêcher les données personnelles des citoyens de l'UE de quitter l'espace européen sans leur consentement explicite.
Thomas de Maizière a préconisé une longue journée de discussion pour aboutir. « Il va falloir faire des compromis et tempérer les attentes », a-t-il insisté.
Deux textes sont en discussion depuis février 2012: un règlement pour les données personnelles à caractère civil et commercial, et une loi pour les fichiers du secteur privé.

Source : http://www.ouest-france.fr/un-accord-europeen-possible-le-15-juin-3436970

Attention à l’usage abusif de la géolocalisation | Denis JACOPINI

Pour les besoins de leurs activités, certains opérateurs de transport et logistique surtout utilisent la géolocalisation. Technologie qui permet de pister un véhicule de service par exemple (voir encadré). Malgré la légitimité de leur prétention, ses utilisateurs sont-ils pour autant en règle avec la loi?

Le traitement de données peut porter atteinte à la vie privée. D'où l'interdiction par exemple de suivre les déplacements d'un salarié hors service. La réglementation en vigueur prévoit des garde-fous: finalité du traitement, nature des données collectées, durée de leur conservation, droits des personnes concernées, consentement des salariés… Une formalité de grande importance à respecter. L'entreprise doit notifier le traitement à la #Commission nationale de contrôle de protection des données à caractère personnel (#CNDP), en France, la Commission Nationale Informatique et Libertés (CNIL). Une demande de déclaration-type est mise à leur disposition. Une demande d'autorisation (et non de déclaration) distincte s'impose à la société qui procède à l'interconnexion ou au recoupement avec d'autres fichiers dont les principales finalités sont différentes. L'employeur doit donc se conformer à toutes ces règles.

Par quoi doit-il commencer?
La finalité du traitement impose que le dispositif de géolocalisation ne soit installé que dans un véhicule à usage professionnel. Une société est en droit de rationaliser la gestion de son parc automobile, d'assurer le secours de son personnel en cas d'incident ou d'accident, facturer une prestation au juste prix (kilométrage, consommation, temps…).
Garantir la sécurité des marchandises et des véhicules est également un motif légitime. L'évaluation du rendement des conducteurs est aussi envisageable. Ce cas-là est verrouillé par l'autorité de contrôle (CNDP ou CNIL): la géolocalisation n'est justifiable que «lorsqu'il n'y pas d'autres moyens» pour juger la productivité d'un salarié. Cette exception ouvre la porte au débat: un syndicat qui, tout en cautionnant l'installation du système, s'oppose à sa prise en compte dans le rendement des salariés.

Que valent aussi les données emmagasinées et utilisées dans une procédure de licenciement pour faute grave?
La géolocalisation «ne doit être activée que si le véhicule est utilisé à des fins professionnelles», précise la CNDP dans sa Délibération n°17-2014. Voilà qui réduit sensiblement la marge d'exploitation de ce système par un employeur.
Celui-ci doit aussi être particulièrement prudent sur la nature des données collectées. Elles sont réparties en deux rubriques. Nom, prénom, coordonnées professionnelles, sont des informations liées directement au salarié. Il y a ensuite des données qui renseignent plutôt sur le véhicule suivi: numéro de plaque d'immatriculation, position géographique, kilométrage parcouru, horaire et durée d'utilisation du véhicule et de conduite, nombre d'arrêts et la vitesse moyenne de circulation. La durée de conservation est limitée à un an. Au-delà, l'exploitation de ces informations serait illégale. Annulant ainsi leur portée dans une procédure disciplinaire ou judiciaire par respect notamment du principe de la loyauté de la preuve.
Le droit d'information pèse dans la mise en place du système de géolocalisation. Au même titre que l'utilisation des caméras de surveillance, une notice s'impose pour informer les salariés: nom du responsable du traitement, nature et destinataires des données, finalité de la collecte…
A moins de justifier «l'existence d'une dérogation», le consentement «libre et éclairé» des conducteurs est indispensable. Exemple: l'insertion d'une clause «géo-localisation» dans le contrat de travail des futures recrues. Toutefois, l'information préalable des instances représentatives des employés demeure la règle. Une obligation à respecter avant l'installation du dispositif de géolocalisation. Seul le gestionnaire du parc automobile et le service ressources humaines, éventuellement, peuvent accéder aux données. Les responsables de traitement doivent donc être identifiables au sein de l'entreprise et sont, en cas de contrôle, les interlocuteurs des agents assermentés de la CNDP. Ils ont pour charge de veiller à la sécurité et à la confidentialité des données. La divulgation d'une information ou son exploitation abusive engagent la responsabilité civile, voire pénale, du dirigeant et des responsables de traitement.

Un droit à double tranchant
La géolocalisation permet d'identifier la position d'un objet ou d'une personne en ayant recours aux bornes wifi, antenne GSM et position de constellation satellitaire. L'une de ses utilisations les plus courantes est le suivi des véhicules de service: optimiser les déplacements, le temps, la consommation de carburant.

« «Consciente de son utilité», la commission nationale de contrôle de protection des données à caractères personnel (CNDP) définit des règles aux responsables de traitement afin que le dispositif de géolocalisation soit conforme avec la loi 09-08 protégeant les données privées. Toute infraction à la réglementation expose son auteur à de lourdes amendes, voire dans certains cas à l'emprisonnement.

Ces informations concernent le Maroc. Un équivalent pour la France Existe.
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

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.leconomiste.com/article/971816-attention-l-usage-abusif-de-la-geolocalisation
Par Faical FADOUNI

Contrôles de la CNIL en 2015 – Demandez le programme… | Le Net Expert Informatique

Contrôles de la CNIL en 2015 – Demandez le programme…

En 2015, la CNIL contrôlera des technologies ou des traitements récemment mis en œuvre et faisant partie du quotidien des Français.

En 2015, un objectif d'environ 550 contrôles est prévu (421 contrôles réalisés en 2014), se décomposant de la façon suivante :
• environ 350 vérifications sur place, sur audition ou sur pièces. Un quart des contrôles sur place portera sur les dispositifs de vidéoprotection / vidéosurveillance
• 200 contrôles en ligne.

Les thématiques prioritaires des contrôles 2015
Comme chaque année, la CNIL prévoit de dédier une part significative de son activité de contrôle à des thèmes choisis du fait de leur impact sur les libertés et du nombre important de personnes concernées.

Le paiement sans contact : le large développement de ces dispositifs en fait une thématique de première importance, eu égard notamment au nombre de personnes concernées. Outre les questions de sécurité, la prise en compte du droit d'opposition sera notamment vérifiée.

Le traitement de données personnelles dans le cadre de la gestion des risques psycho-sociaux (RPS) en entreprise : dans le prolongement de l'accord national interprofessionnel de 2008 relatif à l'amélioration des conditions de travail, de plus en plus d'entreprises diligentent des enquêtes sur les risques psychosociaux auprès de leur salariés afin d'évaluer et de mieux lutter contre le stress au travail. Ces enquêtes soulèvent des questions pratiques qui ont conduit de nombreux salariés à saisir la CNIL. Les contrôles s'opèreront auprès de prestataires et d'entreprises (publiques et privées) ayant mené une enquête RPS ces dernières années.

Le Fichier National des Permis de Conduire mis en œuvre par le ministère de l'Intérieur : ce fichier répertorie l'ensemble des permis de conduire enregistrés en France (environ 40 millions). Le solde des points restants sur le permis est consultable en ligne depuis le site telepoints.info. Le FNPC comporte également toutes les décisions relatives au permis de conduire, et notamment, les décisions administratives (retrait, suspension, annulation, restriction du droit d'en faire usage) et judiciaires (y compris les compositions pénales, amendes ainsi que les procès-verbaux des infractions constatées). Les vérifications porteront en particulier sur la fiabilité et la mise à jour des données, leurs modalités d'accès et leur sécurisation.

Les objets connectés « bien-être et santé » : un écosystème s'est développé autour d'une offre bien-être et santé comprenant des objets connectés et des services en ligne, permettant le suivi individuel et le partage de données relatives par exemple à l'activité physique ou l'évolution de la corpulence du détenteur. Ces dispositifs suscitent de nombreuses interrogations quant à l'information et au consentement des utilisateurs.

Les outils de mesure de fréquentation des lieux publics : ces nouveaux dispositifs déployés dans l'espace public (centres commerciaux, quartiers ou villes entières) permettent via les connexions aux bornes mobiles et wifi une mesure fine du trafic de données personnelles. Ces mesures permettent entre autres objectifs de monétiser l'espace publicitaire. Des contrôles sur ces thèmes permettront de renforcer la doctrine naissante.

Les « Binding Corporate Rules » (BCR) : à ce jour, 68 sociétés ont adopté des BCR. Ces dispositifs n'ont fait pour l'heure l'objet d'aucun contrôle ex-post. La réalisation de contrôles de quelques entreprises ayant adopté des BCR fournira un éclairage sur l'impact du dispositif au regard de la protection des données personnelles et du respect de la vie privée au sein des groupes concernés.

Enfin, l'année 2015 sera l'occasion pour la CNIL de continuer le travail de coopération internationale entre autorités de protection des données. Cette coopération s'effectuera notamment au travers du troisième volet du « Sweep Day » coordonnée par le GPEN (« Global Privacy Enforcement Network » – réseau international d'autorités en charge de la protection de la vie privée) qui concernera le thème de « la vie privée de la jeunesse » (« Youth Privacy »).

Concrètement, l'audit conjoint qui sera réalisé en mai portera sur les services en ligne proposés aux mineurs (sites visant particulièrement les utilisateurs de moins de 12 ans et/ou les adolescents). Les autorités se concentreront notamment sur l'information, et le contrôle de l'âge.

En outre, des contrôles seront menés dans le cadre de la coopération européenne en matière de police (Europol, Schengen, etc.).

Source : http://www.cnil.fr/linstitution/actualite/article/article/programme-des-controles-2015/

Android : vos données personnelles impossibles à effacer ? | Le Net Expert Informatique

Des chercheurs ont mis en lumière les problèmes de sécurité du système d'exploitation mobile de Google.
Grâce à un seul petit bouton « Restaurer les paramètres d'usine », Google promet à ses utilisateurs de supprimer tous les contenus de leur smartphone Android. La mémoire du smartphone serait ainsi totalement effacée. Mais à en croire une étude menée par deux chercheurs de l'université de Cambridge, il n'en est rien : cette fonction de suppression serait inefficace sur plus de 500 millions de smartphones Android. Explications.

Quelles données ont été récupérées ?
Les chercheurs ont examiné 21 smartphones de 5 grandes marques et sous différentes versions d'Android : Samsung Galaxy S2 et S3, LG Optimus L7, Nexus 7, HTC Desire C, Motorola Razr I, etc. Cet échantillon représenterait près de 500 millions de smartphones actuellement en circulation. Sur la totalité des smartphones étudiés, les données personnelles ont pu être récupérées après avoir été effacées. Les deux chercheurs ont ainsi pu mettre la main sur les identifiants Google des utilisateurs sur tous les modèles. Puis, ils ont pu accéder aux informations des services Google associés à ces comptes : Gmail, Calendrier, Drive, etc. Enfin, les chercheurs ont pu récupérer des données de communications (SMS, e-mails, appels, etc.) et des fichiers multimédias (photos et vidéos).

Comment c'est possible ?
Comme l'explique le résultat des recherches, lorsqu'un utilisateur appuie sur le bouton pour effacer ses données, le smartphone supprime en réalité l'accès à ces données et non les informations elles-mêmes. « C'est comme pour un ordinateur : un formatage du disque dur ne suffit pas à effacer les données », explique à Europe 1 Jean-François Beuze, expert en sécurité informatique.

Comment être sûr que toutes les données sont effacées ?
« Il faut chiffrer ses données », conseille le spécialiste en sécurité. C'est à dire ajouter une étape de protection supplémentaire à ces informations personnelles. Pour cela, il faut se rendre dans les réglages du smartphone, puis dans le menu Sécurité et enfin cocher la case « chiffrer les données sur le smartphone ». Si une carte mémoire est utilisée pour étendre le stockage de l'appareil, l'utilisateur devra également chiffrer celle-ci. Pour les données les plus sensibles, « il existe des appareils émettant un champ électromagnétique pour effacer toute donnée sur le smartphone », ajoute Jean-François Beuze. Mais ces appareils restent réservés aux professionnels en raison de leur coût élevé.

Source : http://www.europe1.fr/technologies/android-les-donnees-personnelles-impossibles-a-effacer-970842

Contrôle de la CNIL aujourd'hui à France Télévisions | Le Net Expert Informatique

Contrôle de la CNIL aujourd'hui à France Télévisions

L'Express l'a révélé ce jeudi matin: le siège de France Télévisions a été fouillé mercredi par la Commission nationale de l'informatique et des libertés. Le groupe audiovisuel est soupçonné d'avoir opéré un fichage illégal de ses salariés.

France Télévisions a subi mercredi un contrôle de la Commission nationale de l'informatique et des libertés (Cnil) pour vérifier l'existence de fichiers contenant notamment des données sur les opinions politiques et l'orientation sexuelle de ses salariés, a révélé L'Express ce jeudi matin.

Dénoncé par une lettre anonyme, France Télévisions ficherait ses employés

Ce contrôle avait pour but de vérifier si, oui ou non, France Télévisions a illégalement fiché ses employés. D'après une lettre anonyme envoyée à la Cnil, le groupe audiovisuel aurait recueilli des données personnelles sur leurs opinions politiques, leur orientation sexuelle ou leur casier judiciaire.

Selon le procès-verbal de cette perquisition, les six agents de la CNIL dépêchés sur place ont effectué des recherches au sein des boîtes mails de la direction des ressources humaines du groupe audiovisuel public. D'après plusieurs sources syndicales, les enquêteurs n'auraient a priori pas trouvé « d'éléments probants » en fin de matinée, mais ils ont réalisé des copies de plusieurs fichiers internes. L'instruction, elle, « est toujours en cours ».

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

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.lexpress.fr/actualite/medias/soupcons-de-fichage-illegal-de-salaries-france-televisions-perquisitionne-par-la-cnil_1681974.html