Votre smartphone vous épie à votre insu

	Votre smartphone vous épie à votre insu

Une nouvelle étude de la Cnil publiée ce lundi souligne que deux tiers des applications pour smartphones collectent des informations personnelles auxquelles elles ne devraient pas avoir accès et sans que les utilisateurs en aient conscience. L'étude démontre que nos téléphones sont devenus de vrais petits espions domestiques.

Un nouveau rapport de la CNIL (Commission nationale de l'informatique et des libertés) publié ce lundi montre que les accès aux données personnelles des utilisateurs sont massifs et peu visibles par le citoyen mal informé. Deux applications sur trois captent des informations personnelles à l'insu des utilisateurs. Et l'augmentation du temps passé par les citoyens (de 2 à 4 heures par jour) sur leur portable augmente les risques de fuites de ce type de données.
La CNIL appelle de nouveau les éditeurs d'applications et leurs fournisseurs de services ou partenaires commerciaux à intensifier leur effort d'information des utilisateurs, sans s'abriter derrière des contraintes techniques. Apple, Google, Microsoft, Mozilla seraient les premiers visés.
La CNIL soulignait déjà en 2011 que la confidentialité des données personnelles des internautes n'est pas respectée par les géants du Web. Mais la tendance se renforce. La CNIL a conduit cette nouvelle étude avec l'aide de l'Inria, qui a installé l'outil d'analyse Mobilitics sur des Smartphones que des agents de la CNIL ont utilisé à la place de leurs téléphones personnels. L'étude, menée pendant trois mois, a passé au crible 121 applications Android (plus de 70% du marché des smartphones en France). Et les résultats sont édifiants.
L'étude a permis de dégager trois éléments majeurs. Les identifiants techniques, matériels ou logiciels sont utilisés à des fins publicitaires dans plus de 50% des cas. Les smartphones sont également de vrais « GPS de poche » et certaines applications ne se privent pas d'accéder à ces données qui dévoilent où nous nous trouvons, même lorsque l'abonné n'est pas en train d'utiliser l'application en question. La géolocalisation représente 30% des données collectées chez les utilisateurs. Parmi les 121 applications scrutées par la Commission, cinq ont même accédé au numéro de téléphone de l'utilisateur et deux ont pu récupérer la liste des identifiants des points d'accès WiFi à portée de l'utilisateur.
Si vous croyez encore que le maître à bord de votre smarthpone c'est vous, ce dernier élément va achever de vous convaincre. L'éditeur du système d'exploitation définit ce que les éditeurs d'applications sont autorisés à collecter ou non. Et si la CNIL condamne de nouveau les utilisations outrancières qui sont faites des données personnelles, elle a en réalité peu d'influence face au poids économique que représente pour les géants du Web la collecte de nos données personnelles.

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

Source : http://www.francesoir.fr/societe-science-tech/votre-smartphone-vous-epie-votre-insu
par la rédaction de FranceSoir.fr

La protection des données médicales web 3.0

La protection des données médicales web 3.0

Par Murielle CAHEN – Avocat

L'avènement du web dit 3.0 laisse place à un constat évident : la quasi-totalité des objets disposent aujourd'hui d'une connexion à l'Internet. Dans cette ère du tout connecté où les flux sont incessants, une catégorie de données reste cependant sujette à une attention particulière : les données dites personnelles, regroupant en leur sein les données médicales.

Avant toute chose, il apparait plus aisé de définir plus précisément ce que l'on entend par une donnée médicale. Dans un premier temps, cette dernière n'est pas nécessairement informatique : une donnée peut en effet être archivée sous la forme d'un écrit. Il en va ainsi des certificats médicaux ou des ordonnances. Ainsi, le terme de donnée médicale englobe tout ce qui a attrait à une méthode de conservation de l'état de santé d'un patient : la question de la protection des données médicales, avec les règles de déontologie et de respect de la vie privée s'y afférant, n'est donc pas récente.

Or l'évolution fulgurante des technologies informatiques peuvent constituer un danger pour la protection des données de santé. Ainsi, ces dernières peuvent se voir perdues, corrompues, détruites voire même détournées. Ainsi, le récent cas de suicide du prévenu suspecté d'avoir volé le dossier médical de Michael Schumacher rappelle que les données médicales, du fait de leur caractère éminemment personnel, restent des données sensibles devant faire l'objet d'une protection particulière.

La France est pionnière en la matière puisqu'elle dispose de ce fait d'un régime juridique protégeant l'ensemble des données personnelles. Ce régime date de la loi du 06 janvier 1978. L'objectif principal de cette loi est d'assurer la sécurité du traitement des données à caractère personnel. Parmi ces dernières on y trouve les données médicales qui font également l'objet de dispositions particulières : le code de la santé publique protège les données médicales, et notamment leur traitement par les professionnels de santé.
Cependant, une donnée informatique est, par définition, immatérielle. Elle suppose donc une localisation sur un serveur. Hélas, dans le cas où un ressortissant français tombe malade dans un pays étranger et est soigné là bas, ses données médicales ne seront pas situés sur le territoire national. La loi française ne s'appliquant que sur le territoire français, le régime de protection des données médicales pourra se voir alors modifié, et certaines atteintes à la confidentialité de données de santé seront peut être tolérées alors qu'elles constituent une infraction au droit français. Dès lors, quelle est la réelle portée juridique de la protection des données médicales à la fois au plan national et international? L'évolution récente de certaines technologies informatiques peut elle rentrer en contradiction avec la confidentialité de données si sensibles?

I. Une protection des données médicales encadrée au plan national.
Il en va de soit, mais la France possède un régime juridique particulier sur la protection des données médicales, ce dit régime étant particulièrement efficace. De plus, la CNIL assure une surveillance particulière des dites données et elle délivre régulièrement des informations pratiques destinés à renseigner les professionnels de la santé.

A. Un cadre juridique et réglementaire efficace.
Comme dit précédemment, la France s'est dotée la première d'un régime juridique spécifique aux données personnelles et à l'utilisation des données personnelles. En effet, la loi dite Informatique et Liberté promulguée le 06 janvier 1978 a pour objet spécifique de protéger le traitement des données à caractère personnel. Comme indiqué ci-dessus, le caractère sensible de cette catégorie de données, qui permet ainsi de catégoriser les individus en fonction de leur ethnie, sexe, état de santé, etc., justifie à lui seul la mise en place d'une protection. Si cette loi s'attache à traiter de la protection de l'ensemble des données dites à caractère personnel, la loi dite « Kouchner » promulguée le 4 mars 2002 a pour objet de s'intéresser particulièrement aux données médicales. Ainsi, l'article L1111-7 du Code de la santé publique met en place pour les patients les conditions d'accès à leurs données relatives à leur santé. Lorsqu'un individu souhaite avoir accès à n'importe quel document dont le contenu est relatif à son état de santé (par exemple une feuille de consultation ou une ordonnance médicale), ce dernier peut demander directement ou par le biais d'un médecin l'accès à ce document.
Cependant, l'article L1111-8 du Code de la santé publique s'attache plus précisément à la licéité de l'hébergement et du traitement de données de santé. Ainsi, dans le cadre d'opérations de soins ou de diagnostic, les données de santé récupérées peuvent uniquement être hébergées auprès de personnes physiques ou morales qui sont agréées à cet effet. De plus, cet hébergement de donnée de santé ne peut être effectué qu'après consentement exprès de la personne concernée. Enfin, les dispositions du code de la santé publique rappellent que le traitement de telles données doivent évidemment respecter les conditions posées parla loi Informatique et Libertés. Les professionnels de la santé sont encadrés lorsqu'ils sont amenés à traiter avec des données médicales. De plus, le secret médical imposé par la déontologie des professions relatives au milieu de la santé interdit toute divulgation de donnée médicale à autrui sans accord de ce dernier ou au détriment des conditions posées par la loi.

B. Des recommandations pratiques délivrées par la CNIL.
La CNIL accorde une attention particulière à la manière dont sont effectuées des traitements de données à caractère personnel. Pour se faire, la CNIL utilise souvent des recommandations faites aux entreprises ou aux professionnels concernés afin de rappeler les pratiques idéales à effectuer suivant la situation. Dans le cas de la protection des données médicales, la CNIL s'est prononcé sur les modalités optimales à adopter dans le cas où un professionnel de santé héberge ou traite des données médicales.
La CNIL commence par rappeler la nécessité première de maintenir le degré de confidentialité des données de santé au même rang que celui du secret médical. Pour se faire, la CNIL donne des indications d'ordre technique qui, si elles peuvent paraître acquises pour de plus en plus de gens aujourd'hui au regard de l'ouverture du milieu informatique au grand public, restent nécessaires, voire indispensables dans certains cas, pour s'assurer d'un minimum de sécurité sur les données hébergées : un mot de passe doit être mis en place sur l'ordinateur et ce dernier doit faire l'objet d'un arrêt complet à chaque absence du professionnel de santé. De plus, il est recommandé par la CNIL de ne jamais faire de copie de son mot de passe pouvant être lue ou interceptée par un tiers non autorisé à accéder au système informatique. A ce titre, rappelons simplement que la simple intrusion dans un système informatique sans autorisation constitue à lui seul un délit pénal. De plus, la CNIL recommande pour le professionnel médical de disposer de supports de sauvegardes externes permettant d'éviter la perte de données.
Dans le cas où un traitement de données médicales fait l'objet d'une mise en réseau, la CNIL recommande alors une gestion plus poussée des mots de passe : ces derniers doivent être distincts suivant l'utilisateur qui utilise l'ordinateur et trois erreurs consécutives doivent, à l'instar des erreurs lors de l'entrée d'un code PIN erroné, bloquer le système. De plus, la CNIL ne recommande pas à ce qu'un compte d'un utilisateur puisse être ouvert sur plusieurs postes différents : cela signifie ainsi que le professionnel médical n'est pas présent devant l'un de ses postes, ce qui rend accessible les données à un tiers. De plus, les données médicales doivent faire l'objet d'un cryptage : c'est obligatoire pour les données personnelles. Ainsi, outre une intégrité des données qui doit constamment être vérifiée au plan informatique, la confidentialité de ces dernières doit être assurée par un chiffrement total ou partiel des données nominatives en fonction des cas. Enfin, dans le cas où l'accès au réseau se fait via Internet, un système de pare-feu est hautement recommandé pour prévenir de toute tentative d'interception des données médicales lorsque ces dernières font l'objet d'un flux.

II. Une protection des données médicales incertaine au plan international.
La loi française n'est applicable en France, et certaines législations internationales semblent ne pas accorder autant d'importance à la protection des données personnelles. De plus, l'ouverture des réseaux au monde entier amène à un risque : le législateur n'a pas le temps d'adapter la loi à la technique informatique.

A. Une absence de concertation internationale préjudiciable.
Avant toute chose, il est à noter que la majorité des autres états étrangers n'adopte pas de position hostile par rapport à la protection des données personnelles, bien au contraire. Ainsi, concernant les états européens, la plupart de ces derniers ont adopté une CNIL (ou un équivalent) permettant ainsi une certaine uniformisation de la protection des données personnelles, et donc par ce biais des données médicales. De plus, lorsqu'un traitement de données personnelles d'un citoyen français doit être effectué dans un pays étranger, un accord de la CNIL est obligatoire. Il existe ainsi des cas de figure où des données médicales d'un ressortissant français peuvent être amenées à être traitées dans un pays étranger à l'européenne.
L'exemple des États-Unis constitue peut-être le meilleur exemple de risque potentiel d'atteinte à la protection des données médicales d'un citoyen français. Prenons le cas où lors du séjour d'un français aux États-Unis, ce dernier doit subir une hospitalisation imprévue dans un établissement de santé américain. Théoriquement, et dans la grande majorité des cas, les données médicales des patients français n'ont aucune raison d'être détournées de leur utilisation. Or il existe un principe en droit américain nommé le « Patriot Act ». Ce dernier permet au gouvernement américain de disposer librement des données personnelles d'un individu sur le fondement d'une seule suspicion de terrorisme ou d'espionnage. Si l'existence d'un tel principe est hautement compréhensible au regard de l'importance accordée par le gouvernement américain à tout ce qui concerne la sécurité nationale, le fondement d'une seule suspicion sans autre preuve apparait bien léger pour assurer une protection des données médicales. De plus, la cybercriminalité est un rempart à une bonne protection des données médicales lorsque des pare-feu ne sont pas suffisamment élaborés pour prévenir de telles attaque. Ainsi, entre les mois d'avril et juin 2014, Community Health Systems, un spécialiste de la gestion d'hôpitaux américains, a subi des cyber-attaques qui ont subtilisé plusieurs millions de données personnelles. S'il n'est fait état d'aucune subtilisation de données médicales au sein des données volées, cette possibilité relance la nécessité d'une protection informatique nécessaire pour se prémunir de ce genre de piratage.

B. Un état technique avancé, ou le risque d'un retard juridique.
Aujourd'hui, il apparait pratiquement impossible de faire disparaitre la carte vitale du système médical français : la gestion des données de santé apparait bien trop longue au regard du nombre de patients à gérer. A ce titre, l'évolution informatique mêlée à des impératifs de gestion médicale ne pose pas de problème juridique en soit. Toutefois, des technologies nouvelles ne sont pas encore appréhendées parla loi. Il en va par exemple du Cloud computing : aucun stockage physique n'est effectué sur le disque dur de l'ordinateur et tout se retrouve localisé dans des datacenters qui peuvent être localisés dans des pays étrangers. Certaines entreprises louent d'ailleurs des services de cloud à des professionnels. Or dans le cas où un professionnel médical stockerait des données de santé de cette manière, outre un accord de la CNIL nécessaire, que se passe-t-il dans le cas où un patient souhaite avoir accès à ses données de santé ? De plus, lorsque des données, notamment personnelles, se retrouve massivement stockées en un point physique fixe, les risques de cyber-attaques se retrouvent augmentées. En 2009, le gouvernement français avait élaboré le projet « Andromède » qui prévoit de stocker sous la forme d'un « cloud souverain » les données nationales du gouvernement, de son administration et d'autres entreprises. Ce projet permettrait ainsi d'alléger considérablement les risques associées à une « volatilité » des données que l'on peut constater aujourd'hui. En effet, ces dernières se retrouveraient toutes sous l'égide de la loi française, aucun problème de localisation des serveurs ne pourrait être relevé et le travail de surveillance de la CNIL serait considérablement allégé. Pour autant, si les données médicales ne semblent pas faire l'objet d'un stockage massif dans des serveurs cloud étrangers, la question mérite néanmoins réflexion en ce que les dispositions relatives au bon traitement des données médicales par le droit français se voit d'un coup quasiment réduites à néant. Enfin, une législation numérique européenne serait la bienvenue puisque les données médicales se verraient enfin asservies à un régime juridique dans l'ensemble de l'Europe.
Par Me Murielle CAHEN
Sources :
http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-imperatif-la-securite/

http://www.ordre.pharmacien.fr/content/download/123311/645012/version/1/file/J23-Dossier-CommentGarantirSecuriteDonneesSante.pdf

http://www.ordre.pharmacien.fr/Le-patient/La-protection-des-donnees-de-sante

http://www.linformaticien.com/actualites/id/33884/4-5-millions-de-donnees-medicales-derobees-aux-etats-unis.aspx

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

Source : http://www.juritravail.com/Actualite/fichiers-libertas/Id/176621
Par Murielle CAHEN – Avocat

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…

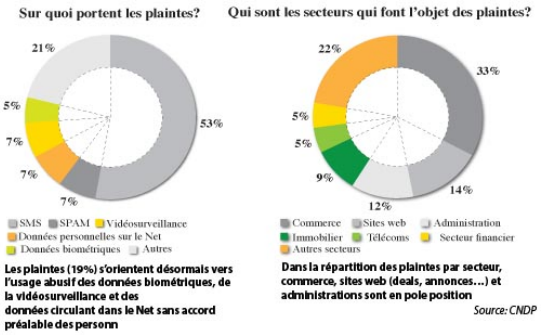
Source : http://www.industrie-techno.com/smartphones-deux-applis-sur-trois-nous-espionnent-revele-la-cnil.35111
Par Muriel de Véricourt

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

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

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

Les ministres de l’UE reviennent sur le guichet unique pour la protection des données

Les ministres de l’UE reviennent sur le guichet unique pour la protection des données

Deux ans après la proposition de s’adresser à une unique autorité pour gérer les questions de protection de données dans l’Union européenne, les ministres de la Justice de l’UE envisagent une autre solution, impliquant plusieurs autorités. Un abandon qui contrarie la coalition ICDP où l’on retrouve Google, Facebook, Microsoft, Apple et Yahoo.

Les pays membres de l’Union européenne sont revenus la semaine dernière sur une proposition de 2012 visant à diriger les fournisseurs de technologies tels que Google, Facebook, Microsoft ou Apple vers une seule autorité habilitée à gérer les questions de protection de données en Europe. L’objectif de ce projet était d’éviter de devoir s’adresser à chaque autorité de protection de données des 28 pays membres de l’UE. La question avait été débattue par les ministres de la Justice et la proposition élaborée par la Commission européenne constituait l’un des piliers de la réforme de la protection de données dans l’UE.
Mais la semaine dernière, lors d’une nouvelle réunion des ministres de la Justice et de l’Intérieur à Bruxelles, à laquelle ont assisté Christiane Taubira, ministre de la Justice, et Bernard Cazeneuve, ministre de l’Intérieur en France, une majorité s’est dégagée pour une autre proposition, suggérée par les Italiens. Ces derniers occupent jusqu’au 31 décembre la présidence tournante du Conseil européen où se rencontrent les ministres pour coordonner les différentes politiques.

Un processus qui risque d’être très lourd, estime l’ICDP
Cette fois, la proposition suggère un mécanisme qui se déclencherait uniquement dans les cas transfrontaliers les plus importants. Celui-ci consisterait à faire coopérer les différentes autorités de protection de données concernées afin de déboucher sur une décision conjointe. Cette proposition n’emporte évidemment pas les faveurs des fournisseurs de technologie. L’ICDP, Industry Coalition for Data Protection (qui regroupe 18 associations représentant des milliers de sociétés européennes et internationales, dont Google, Facebook, Microsoft, Apple et Yahoo), a exprimé sa déception. Dans une lettre envoyée aux ministres avant leur réunion, elle estime que cela semble créer un mécanisme plus compliqué. Pour elle, cela pourrait conduire à impliquer toutes les autorités de protection de données dans la grande majorité des cas examinés. Couplé à la possibilité que chaque autorité puisse opposer son veto à une décision, cela rendrait le processus très lourd.
Même son de cloche du côté de la CCIA (Computer and Communications Industrie Association) qui représente des sociétés Internet européennes et américaines. L’un des ses porte-parole estime qu’il faut un guichet unique qui permettrait aux grandes entreprises technologiques comme aux PME de ne s’adresser qu’à un seul régulateur, quel que soit le nombre de pays dans lesquels ils interviennent. Ces dispositions seront à nouveau abordées par le Conseil européen dans les prochains mois.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-les-ministres-de-l-ue-reviennent-sur-le-guichet-unique-pour-la-protection-des-donnees-59534.html par Loek Essers / IDG News Service (adapté par Maryse Gros)

La protection des données personnelles, un « droit fondamental »

La protection des données personnelles, un « droit fondamental »

Les régulateurs européens, réunis au sein du G29, rappellent la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».

Les autorités européennes de régulation des données ont affirmé lundi dans une déclaration commune au ton très politique que la protection des données personnelles était un « droit fondamental » sur lequel l'Union européenne ne pouvait transiger. Un an et demi après les révélations d'Edward Snowden, les régulateurs européens réunis au sein du G29 ont rappelé lors d'un colloque la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».
Faisant référence au traité de libre-échange transatlantique, les « Cnil » (Commission nationale de l'informatique et des libertés, NDLR) soulignent que « le niveau européen de protection des données ne peut être érodé (…) par des accords bilatéraux ou internationaux ». Elles demandent ainsi l'application stricte des nouvelles règles de protection des données de l'Union, en cours de négociation, qui doivent être considérées « comme des principes internationaux impératifs en droit international public et privé ».
« Tous les corpus de protection des données doivent être considérés comme des lois de police », a affirmé Isabelle Falque-Pierrotin, présidente de la Cnil française, qui appelle également à la mise en place d'actions judiciaires collectives sur le modèle des class actions. Le G29 juge par ailleurs « inacceptable sur le plan éthique (…) la surveillance secrète, massive et indiscriminée de personnes en Europe ».

« Le pétrole de demain »
« La conservation, l'accès et l'utilisation de données par les autorités nationales compétentes doivent être limités à ce qui est strictement nécessaire et proportionné dans une société démocratique », soulignent les « Cnil ». Le Premier ministre Manuel Valls a promis à ce sujet qu'un projet de loi « garantira un contrôle effectif et indépendant de l'intégralité des actes dérogatoires au droit commun accomplis par les services de renseignement ». Il a appelé également à une simplification des conditions générales d'utilisation et à un droit à l'oubli renforcé pour les mineurs.
Le stockage des données personnelles collectées par des entreprises privées doit enfin, selon les régulateurs, pouvoir être contrôlé par une autorité européenne indépendante. « Les données européennes doivent être stockées en Europe », a indiqué Thierry Breton, P-DG d'Atos et ancien ministre de l'Économie. « Il est temps de protéger ces mines d'or (…), ce sera le pétrole de demain », a-t-il ajouté.

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

Source : http://www.lepoint.fr/societe/la-protection-des-donnees-personnelles-un-droit-fondamental-08-12-2014-1887990_23.php