Accès administratif aux données de connexion: rassuré avec le décret ?

Accès administratif aux données de connexion: rassuré avec le décret ?

Le décret sur l'accès administratif aux données de connexion, en lien avec l'article 20 de la LPM, a été publié le 24 décembre. La cyber-surveillance tend à se généraliser malgré la vigilance de la CNIL.

C'est un grand classique quel que soit le gouvernement : la tentation de faire passer des décrets juste avant Noël pour éviter de faire trop de bruit. Mais le tour de passe-passe n'a pas échappé à des médias vigilants sur la protection de la vie privée comme NextInpact.

Dans le JORF en date du 26 décembre, on découvre le décret 2014-1576 « relatif à l'accès administratif aux données de connexion » (qui avait été approuvé le 24 décembre).
Une belle tentative de mettre en œuvre en catimini d'ici le premier janvier 2015 ce qui avait provoqué une polémique sur la protection des droits civils à l'ère numérique dans le cadre de l'examen du projet de loi sur la programmation militaire (LPM).
Adopté en décembre 2013, le texte dense intègre un article 20 au contour flou qui a des répercussions sur la vie civile : l'accès par les autorités – sans décision judiciaire – aux données de connexion des internautes.
Une approche qui suscitait des craintes sur l'encadrement de l'accès aux données à caractère personnel. Gare à la dérive cyber-sécuritaire, estimait des associations professionnelles du secteur IT comme Renaissance Numérique ou l'ASIC à l'époque.
Ainsi, la loi prévoit initialement l'accès par l'administration aux « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques ». Le champ des données surveillées n'était pas limité aux seules données de connexion, mais pouvait concerner l'ensemble des données stockées par l'utilisateur : documents sur le cloud, mails, échanges sur les réseaux sociaux, pseudos, mots de passé, etc.

L'élargissement de la cyber-surveillance reste d'actualité avec la publication du décret associé à l'article 20 de la LPM. Le régime d'exception de l'accès administratif aux données de connexion – jusqu'ici associé principalement à la lutte antiterroriste – est généralisé : « Les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses et sont accessibles à un nombre de plus en plus important d'organismes. »
Et ce, pour des finalités très différentes » au nom de divers intérêts nationaux : « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

Le spectre du Big Brother serait écarté partiellement avec les nouveaux éléments fournis dans le décret du 24 décembre sur « l'accès administratif aux données de connexion ». Celui-ci limite la collecte d'information aux données de connexion (identité de la personne, date et heure de communication, etc.) mais il reste néanmoins à préciser l'exact périmètre des données recueillies.

Bonne nouvelle : le décret semble écarter les risques de droit de regard sur les contenus.
De même, la DGSE, la DGSI ou tout autre service de police judiciaire ne pourront pas directement installer des logiciels d'espionnage (« mouchards ») de manière intensive sur les réseaux des opérateurs.
Selon l'avis de la CNIL rendu le 4 décembre (sur ce qui était à l'époque un projet de décret) mais qui vient juste d'être publié dans le prolongement de la promulgation du décret, il en résulte que « cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes ».
L'autorité française en charge de la protection des données personnelles reste vigilante. « Elle appelle l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques. »
L'année 2015 va mal démarrer alors que le gouvernement prépare une loi sur le numérique. L'occasion d'éclaircir le débat ? Dans le cadre de la consultation gouvernementale ouverte au grand public pour élaborer cette loi, on espère un peu plus de transparence à propos de cette extension de la cyber-surveillance.

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

Source : http://www.itespresso.fr/acces-administratif-donnees-connexion-rassure-publication-decret-85710.html

Doit-on avoir peur de Facebook ?

Doit-on avoir peur de Facebook ?

Tous les jours vous utilisez Facebook et tous les jours vous donnez au réseau social de nouvelle informations sur vous. Tout ce que vous faîtes est observé de près et analysé par le site. Alors, devez-vous avoir peur de Facebook ?

Facebook sait tout de vous. C'est un fait. En vous inscrivant sur le réseau social, vous fournissez de nombreuses informations vous concernant à l'entreprise de Mark Zuckerberg. Votre âge, votre nom, votre ville, votre sexe, mais ce n'est pas tout puisque, à chaque fois que vous publiez un message, un statut, que vous ajoutez un ami ou aimez une publication, Facebook le sait. Si vous avez activé la géolocalisation sur votre smartphone ou sur votre tablette, Facebook sait également où vous vous trouvez. Si vous cliquez sur un lien Public Ados sur Facebook, le réseau social sait que vous avez lu tel article, à telle heure, sur tel appareil, depuis tel endroit…

A quoi servent vos données ?
Mais alors, que fait Facebook avec toutes ces données sur vous. Et bien il les revend. Car ne l'oublions pas, le seul but de Facebook est de faire de l'argent, aucunement d'être un gentil samaritain qui permet aux amis de rester en contact. Facebook revend vos données à des annonceurs, qui peuvent ainsi cibler avec précision un public donné. Si une marque de cosmétiques française souhaite faire une campagne de pub destinée aux 15-20 ans, Facebook peut lui vendre un encart publicitaire optimisé, qui s'adressera seulement à la cible visée. Facebook enverra donc cette pub uniquement aux jeunes filles qui ont entre 15 et 20 ans, qui résident en France et qui suivent déjà des actualités liées à la mode.

Facebook s'engage à vous garder anonyme.
Toutefois, lorsque Facebook vend vos données, il s'engage à vous rendre anonyme. Ainsi, il peut dire à une marque que vous êtes une femme de 17 ans célibataire qui vit à Marseille, qui aime la mode et qui a 453 amis Facebook. Mais aucunement le réseaux social n'a le droit de communiquer le fait que vous vous appelez Marie Duchnoc, que vous êtes en couple avec Martin Truc et que votre numéro de téléphone est le 06 XX XX XX XX. En vous inscrivant sur Facebook vous avez accepté ce principe.

Supprimer vos données
La seule solution pour ne plus être espionné par Facebook, c'est se désabonner du réseau social. Toutefois, il peut y avoir un délai entre votre désinscription et la suppression de vos données. Un délai de 90 jours précise le site dans sa charte de confidentialité. Et même ce délai passé, il peut rester des traces de votre passage sur le site.
En effet, le message que vous avez envoyé à votre meilleure copine Marjorie le 6 avril 2011 à 15h42 sera conservé tant que votre copine Marjorie sera inscrite sur Facebook. Car ce message fait également partie de ses données à elle. Vous l'aurez compris, le système est tentaculaire. Autant dire qu'il est très difficile d'effacer l'intégralité de vos données du réseau social.

Litige avec Facebook
Mais n'oubliez pas que vous êtes le seul et unique propriétaire de vos données. En vous inscrivant sur Facebook vous acceptez uniquement que le réseau social les utilise. Il n'en est pas propriétaire. Si vous estimez que Facebook va trop loin avec vos données, que le réseau social à manqué à l'un de ses engagements, comme vous garantir l'anonymat à la revente de vos données, vous pouvez toujours les contacter via la page d'aide du site. Si la réponse que Facebook vous apporte ne vous convient pas, vous n'aurez qu'une seule solution : contacter un avocat et engager une procédure judiciaire. Toutefois, cela risque de vous coûter très cher, et Facebook, lui, a les moyens de se payer un procès.

Récupérer vos données
Vous pouvez également télécharger vos données Facebook afin de voir ce que le site sait sur vous via l'onglet « Paramètres » > « Général » > « Télécharger une copie de vos données sur Facebook ». Vous recevrez par mail l'intégralité de vos données Facebook. Tout ceci vous appartient, vous en faîtes ce que vous voulez, à l'exception bien sûr des photos que vous n'avez pas prises vous même (si vous avez uploadé des photos prises sur Google Image par exemple). N'allez surtout pas revendre la photo de Rihanna que vous aviez mise en photo de profil, sauf bien sûr si vous l'avez prise vous même… Ne faites pas avec les données des autres ce que vous ne voulez pas que Facebook fasse avec les autres !

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

Source : http://actu.ados.fr/news/facebook-confidentialite-charte-donnees-vente_article6861.html
Par Edouard Riaud

Confidentialité et cryptage récompensés

Confidentialité et cryptage récompensés

Sophia Genetics. La société lausannoise devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.

Sophia Genetics, leader européen en génomique clinique et séquençage ADN de nouvelle génération (NGS), devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.
D'après un communiqué, l'entreprise précise que les certifications du groupe BSI récompensent, entre autres, l'approche de Sophia Genetics du traitement de l'information et du cryptage des données de patients. Cette dernière, en instance d'obtention de brevet, vise à protéger la confidentialité des informations génomiques.
Les serveurs redondants installés par Sophia Genetics dans divers sites hautement sécurisés, offrent à ses clients la confiance nécessaire afin de traiter, analyser et stocker les données de milliers de patients suspectés ou atteints de maladies chroniques.
La certification ISO 27001 a été attribuée à la plateforme Information Security Management System de Sophia pour toutes les informations sécurisées internes et externes de ses clients.
Sophia Genetics se charge à l'heure actuelle de l'analyse, du stockage et du traitement des données de plus de 30 hôpitaux et laboratoires de pointe en Europe.

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

S o u r c e :
http://www.agefi.com/une/detail/archive/2014/december/artikel/sophia-genetics-la-societe-lausannoise-devient-la-premiere-entreprise-doublement-certifiee-iso-13485-et-iso-27001-388417.html

Attention à bien déclarer à la CNIL le traitement de vos fichiers clients, salariés, patients…

Attention à bien déclarer à la CNIL le traitement de vos fichiers clients, salariés, patients…

S'il n'a pas été déclaré à la CNIL, votre traitement de données personnelles est illicite. Tout comme les éléments qu'il vous fournira pour justifier le licenciement d'un salarié.

Tout traitement de données personnelles est illicite s'il n'a pas été préalablement et correctement déclaré à la Cnil (sauf si ces moyens de traitement sont couverts par l'une des 19 dispenses prononcées par la commission). Conséquence : la chambre sociale de la Cour de Cassation a cassé l'arrêt de la Cour d'Appel de Douai, qui avait approuvé le licenciement d'une salariée pour cause réelle et sérieuse alors que ce dernier était fondé uniquement sur le système de contrôle du nombre et du contenu des courriels des salariés mis en place par la société.

Cette dernière n'ayant pas déclaré ce système (qui constitue un traitement de données personnelles) auprès de la Cnil, ce système était illégal et la société ne pouvait donc pas utiliser les preuves qu'elle s'était ainsi constituées. Il convient de rappeler que la déclaration auprès de la Cnil n'est pas la seule condition de la légalité d'un traitement de données personnelles, cette légalité étant également conditionnée, en particulier, par l'information préalable des personnes concernées.

Non respect de la Loi Informatique et Libertés du 6 janvier 1978 :
Peines encourues : 5 ans de prison et 300 000 euros d'amende
Articles sur le même thème :
Se mettre en conformité avec la CNIL – Oui mais comment ?
Est-ce que votre site Internet est en règle avec la CNIL ?

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

Source : http://www.chefdentreprise.com/Thematique/management-rh-1026/droit-social-10119/Breves/Jurisprudence-Attention-declarer-CnIL-votre-systeme-controle-donnees-personnelles-248669.htm

---

Wifi en libre accès : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

Wifi en accès libre : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

La Commission nationale de l'informatique et des libertés (Cnil) a de bons côtés, parmi lesquels sa volonté inébranlable de garder la pêche. Chaque jour que Dieu fait, elle constate des entorses aux règles qu'elle est censée faire respecter, mais ne se décourage pas.

Nouvel exemple : l'autorité administrative indépendante a contrôlé des points où internet est disponible en libre accès – restaurants, hôtels, bibliothèques – via le wifi ou des postes informatiques dédiés. Sans surprise, elle a découvert « des manquements récurrents » :
• de nombreux opérateurs « conservent des données portant sur le contenu des correspondances échangées ou des informations consultées (URL) alors qu'ils ne sont pas autorisés à le faire » ;
• ils ne doivent conserver que les données de connexion, pendant un an. Or, la plupart les gardent indéfiniment ;
• les utilisateurs sont mal informés ;
• plusieurs opérateurs utilisent « des outils de surveillance » des postes informatiques comme la « prise en main à distance » et le « contrôle de l'historique de navigation ». C'est-à-dire qu'ils ont accès, de fait à des données sensibles : « identifiants-mots de passe, numéros de compte bancaire, etc ». La Cnil aimerait qu'ils arrêtent.
• les réseaux wifi, sans chiffrement et facilement accessibles, sont de vraies passoires. Il n'est pas difficile d'en prendre le contrôle.
Plutôt que de paniquer devant tant d'amateurisme, la Cnil garde le cap et donne cinq conseils pour améliorer les choses.

Au restaurant, à l'hôtel ou dans les bibliothèques, il est souvent possible d'utiliser un réseau internet wi-fi ou des postes informatiques en libre accès.
La CNIL a décidé d'intégrer dans son programme annuel des contrôles la thématique de l'internet en libre accès. Elle a effectué plusieurs contrôles des modalités de mise en œuvre de ce type de service auprès d'organismes privés et publics.

Lors de ces contrôles, l'attention de la CNIL a principalement porté sur :
• le type de données collectées,
• leur conservation,
• le niveau d'information des utilisateurs
• la qualité des mesures de sécurité qui y sont associées.

Plusieurs manquements récurrents ont été identifiés lors de ces contrôles. Au vu de ces constations, la CNIL rappelle aux fournisseurs de services d'internet en libre accès les mesures à adopter pour se mettre en conformité.

1. Conserver seulement les données de trafic
Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues à l'article L. 34-1 du code des postes et des communications électroniques (CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux » besoins de la recherche, de la constatation et de la poursuite des infractions pénales » et destinées aux autorités légalement habilitées.
La CNIL a constaté lors des contrôles que de nombreux opérateurs de communication électronique conservaient des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) alors qu'ils ne sont pas autorisés à le faire (article L. 34-1 VI du CPCE consultable sur http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid).
Les fournisseurs de service ne doivent pas collecter de telles données et supprimer celles qui auraient été conservées.

2. Définir une durée de conservation des données limitée et proportionnée
La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.
Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques consultable sur http://legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006466369&cidTexte=LEGITEXT000006070987&dateTexte=20110909&oldAction=rechCodeArticle)
Les autres données collectées dans le cadre de l'offre d'internet en libre accès, telles que les informations d'abonnement, etc. doivent être supprimées régulièrement (article 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée consultable sur http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/#Article6) lorsqu'elles ne sont plus nécessaires (désinscription ou inutilisation prolongée de l'abonnement).

3. Fournir une information complète sur les traitements de données :
Les contrôleurs de la CNIL ont observé que l'information fournie aux utilisateurs des services d'internet en libre accès, ne s'avérait pas toujours satisfaisante, voire inexistante.
Les opérateurs de communication électronique doivent délivrer une information aux utilisateurs de leur service sur les modalités de traitement de leurs données (article 32 de la loi n°78-17 du 6 janvier 1978 modifiée). Le support de cette information doit être le formulaire d'inscription au service. A défaut, l'information doit être fournie par voie d'affichage, dans une charte informatique, etc. (Voir les modèles de mention d'information sur http://www.cnil.fr/vos-obligations/informations-legales/).
Par ailleurs, les opérateurs de communication électronique doivent prévoir des procédures de gestion des demandes d'accès, de rectification et de suppression des données par leurs utilisateurs (art. 38 à 40 de la loi n°78-17 du 6 janvier 1978 modifiée).

4. Veiller à la conformité des outils utilisés, notamment aux outils de surveillance :
Plusieurs opérateurs de communication électronique contrôlés utilisaient des outils de surveillance afin d'assurer la sécurité des postes informatiques, la gestion des tarifications, les impressions, etc.
L'utilisation de tels outils (consultation ou prise en main à distance, contrôle de l'historique de la navigation, etc.) est susceptible de donner accès à un grand nombre d'informations excessives au regard de la finalité pour laquelle elles sont collectées (identifiants-mots de passe, numéros de compte bancaire, etc). Le recours à de tels outils doit être évité ou un paramétrage limité doit être mis en place.

5. Assurer la confidentialité et la sécurité des données :
Plusieurs lacunes en termes de sécurité et de confidentialité ont été révélées lors des contrôles :
• L'absence de chiffrement des réseaux wi-fi ;
• L'accessibilité du BIOS (absence ou faiblesse du mot de passe) permettant de modifier la configuration basique du système ;
• La possibilité de prendre le contrôle de la machine en démarrant un système d'exploitation depuis une clé USB ; etc.
Pour y remédier, les opérateurs de communication électronique doivent inclure une clause relative à la sécurité des données dans le contrat conclu avec le prestataire réseaux (voir le modèle de clause de confidentialité sur http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/sous-traitance-modeles-de-clauses-de-confidentialite).
Par ailleurs, ils doivent adopter des mesures de sécurité afin de (voir les guides sur » La sécurité des données personnelles » sur http://www.cnil.fr/documentation/guides/) .

Au travers de missions de mise en conformité ou de formation d'un futur correspondant CNIL (Correspondant Informatique et Libertés dit aussi CIL), Denis JACOPINI se charge de mettre en conformité votre établissement avec la Loi Informatique et Libertés auprès de la CNIL.
Vous souhaitez vous mettre en conformité avec la CNIL, contactez-nous

---

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

Source : http://rue89.nouvelobs.com/2014/12/22/wifi-libre-acces-cnil-epingle-manquements-recurrents-256697

Live streaming illégal : un coût considérable pour l’économie mondiale

Live streaming illégal : un coût considérable pour l’économie mondiale

Une étude du Center for Strategic and Internationals Studies (CSIS) faisait grand bruit lors de sa sortie, en juin dernier. Elle évaluait à 445 milliards de dollars, soit 327 milliards d'euros, le coût global de la cybercriminalité sur l'économie mondiale. S'il semble compliqué de lutter contre ce fléau sans visage, la limitation de certains comportements à risque permettrait de réduire substantiellement la note pour les industries du secteur, mais aussi et surtout pour les internautes. Ainsi en va-t-il du live streaming illégal, plébiscité mais toxique.

Radiographie de la cybercriminalité mondiale

Sans surprise, les pays les plus exposés aux méfaits des cybercriminels sont les grandes puissances. A eux seuls, Etats-Unis, Chine et Allemagne concentrent 200 milliards de pertes dues à des piratages en tout genre, même si essentiellement par vol de propriété intellectuelle.

L'importance des dégâts commis par les hackers est inversement proportionnelle au nombre d'entre eux capables de conceptualiser des programmes permettant d'exploiter des failles logicielles connues (exploits). Selon le Centre de lutte contre la Cybercriminalité d'Europol, seule une centaine de personnes serait responsable de la cybercriminalité dans le monde. Autrement dit, si d'innombrables réseaux cybercriminels s'approprient les kits d'exploits et malwares créés par d'autres, ils ne sont qu'une poignée à pouvoir être considérés comme les cerveaux du hacking international.

Europol précise que ces kits et malwares sont à ce point élaborés qu'ils peuvent facilement être adaptés aux cibles spécifiques des cybercriminels. Des cibles qui sont souvent des entreprises dont les solutions de sécurité laissent à désirer, mais aussi des particuliers, notamment via leur utilisation du live-streaming illégal, véritables supermarchés pour les hackers, qui n'ont qu'à se pencher pour se servir.

Le live streaming illégal, tête de pont de la cybercriminalité mondiale

Début octobre, l'Association of Internet Security Professionals (AISP) se fendait d'un rapport alarmant. Intitulé « Illegal Streaming and Cyber Security Risks : a dangerous status quo ? » il montrait que 500 millions d'ordinateurs étaient infectés dans le monde, soit une infection toutes les 18 secondes.

Concernant les sites de live streaming illégaux, type retransmission de matchs de sport, le rapport de l'AISP se fait très précis. Selon lui, 80 % de ces plateformes hébergeraient des malwares, visant à subtiliser des données confidentielles aux personnes les fréquentant. Avec pour but, in fine, de bombarder leurs boites mails de spams, de subtiliser leurs codes bancaires ou encore d'usurper leur identité.

67 milliards de dollars sont dépensés par an en achat de services de sécurité sur Internet. Cette somme pourrait être considérablement réduite si les internautes prenaient conscience des risques encourus en surfant, par exemple, sur des sites de live streaming illégaux.

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

Source : http://www.actu-economie.com/2014/12/18/live-streaming-illegal-cout-considerable-leconomie-mondiale/
Par Christophe Fourrier

Protection de la vie privée : pas avant 2025, au mieux !

Protection de la vie privée : pas avant 2025, au mieux !

Une étude menée par Pew Research Center a posé la question a plus de 2500 experts et politiciens sur la création d'un cadre unique pour garantir la protection des données privées tout en facilitant l'innovation et le business des entreprises.

Le Pew Research Center a mené une enquête originale pour connaître l'opinion de plus de 2500 experts techniques et des politiciens sur l'avenir du respect de la vie privée. Concrètement, l'étude s'interrogeait sur la capacité des législateurs et développeurs à créer un cadre capable de garantir la vie privée d'ici 2025. Ce cadre devra à la fois simplifier l'innovation et la monétisation des applications, tout en offrant aux utilisateurs des options de sauvegarde de leurs données personnelles.
L'opinion des experts est divisée. 55% des répondants ne croient pas qu'un tel cadre puisse voir le jour dans la prochaine décennie. Mais 45% sont plus optimistes sur sa création et son acceptation. Par ailleurs, si les avis sont tranchés sur l'avenir de la confidentialité des données personnelles, il existe un consensus pour souligner que la vie en ligne est par nature publique. Il s'agirait donc bien d'un problème d'éducation de l'utilisateur, mais aussi du comportement des sites qui promettent plus de facilité contre des informations privées. L'étude qui cite Bob Briscoe, chercheur sur l'infrastructure et le réseau chez British Telecom, estime que cette facilité et ce confort sont à l'origine de l'absence de préoccupations des utilisateurs sur leurs données personnelles.

Un souci de définition, des outils de chiffrement nécessaires
Pour Joe Wilbanks, responsable de Sage Bionetworks revient sur le cadre général en constatant que 10 ans c'est trop court pour le législateur d'ajuster les règlements face à la rapidité des évolutions technologiques. D'autres comme Nick Arnett, expert en BI chez Buzzmetrics, confie que les définitions de « liberté » et de « vie privée » vont changer dans la société d'ici 2025 et il y aura souvent des désaccords sur ces transformations. Idem pour Homero Gil de Zuniga, directeur de recherche Digital Media à l'Université du Texas à Austin qui pense que « l'information sera encore plus omniprésente, plus fluide et portable. Les sphères publiques et privées numériques vont probablement se chevaucher ». Ce qui lui fait dire que ce qui est privé aujourd'hui ne le sera peut-être pas demain.
Peter Suber, directeur d'un projet d'accès illimité à la recherche (Open Access), prévient que pour créer un cadre unifié et acceptable, il y aura au préalable une course aux technologies qui favorisent la vie privée et la sécurité. Il ajoute que cette phase est en cours aujourd'hui avec le développement du chiffrement. Il reste des efforts à mener néanmoins sur la sécurité des données personnelles qui n'est pas du seul fait des entreprises.

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

Source : http://www.silicon.fr/donnees-personnelles-un-cadre-unique-en-2025-est-il-utopique-104490.html
Par Jacques Cheminat

Confidentialité des donnés : 71 % des employés déclarent avoir accès à des informations qu’ils ne devraient pas voir

Confidentialité des donnés : 71 % des employés déclarent avoir accès à des informations qu’ils ne devraient pas voir

Une enquête de Ponemon Institute pour la société Varonis systems Inc révèle que les employés disposant d'accès excessifs aux données de l'entreprise représentent un risque de fuites. Cependant, moins d'un collaborateur sur quatre estime que leur entreprise accorde une priorité très élevée à la protection de ses données.

Une étude* commandée par Varonis Systems Inc, une société qui fournit des solutions logicielles pour les entreprises, et réalisée par le Ponemon Institute, un centre de recherche sur la confidentialité, la protection des données et les politiques de sécurité de l'information, révèle que la plupart des entreprises rencontrent des difficultés à trouver l'équilibre entre un besoin de sécurité renforcée et les exigences de productivité des salariés. L'étude précise que les employés qui disposent de privilèges excessifs d'accès aux données représentent un risque croissant pour les entreprises en raison de l'exposition accidentelle et intentionnelle d'informations sensibles ou critiques. 71 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient pas pouvoir consulter et 54 % de ces utilisateurs caractérisent ces accès comme fréquents ou très fréquents.

Productivité contre sécurité

Les informaticiens comme les utilisateurs finaux témoignent d'un manque de contrôle en ce qui concerne l'accès aux données et leur utilisation par les employés. Les deux groupes conviennent généralement du fait que leur entreprise préférerait négliger les risques de sécurité plutôt que sacrifier la productivité. Seulement 22 % des collaborateurs ayant participé à l'enquête estiment que leur entreprise accorde une priorité très élevée à la protection de ses données. Moins de la moitié des employés pensent que leur société applique des politiques de sécurité strictes en ce qui concerne l'utilisation et l'accès aux données.

Des fuites dues à la malveillance des collaborateurs

Les conclusions de l'enquête indiquent également que les informaticiens et les utilisateurs finaux s'accordent sur le fait que les comptes d'employés détournés pouvant conduire à des fuites de données sont très probablement le fait de collaborateurs internes disposant d'accès excessifs et souvent inconscients des risques que ceux-ci représentent. 50 % des utilisateurs finaux et 74 % des informaticiens estiment que les erreurs, les négligences ou la malveillance d'employés sont fréquemment ou très fréquemment à l'origine des fuites de données. Et seulement 47 % des informaticiens indiquent que les employés de leur entreprise prennent des mesures appropriées pour protéger les données auxquelles ils accèdent.

Dans le même temps, 76 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations de l'entreprise telles que des données relatives aux clients, des renseignements sur les collaborateurs, des rapports financiers et des documents commerciaux confidentiels. Et, 76 % des utilisateurs finaux jugent qu'il est parfois acceptable de transférer des documents de travail sur leurs périphériques personnels, alors que seulement 13 % des informaticiens en conviennent.

*Le rapport d'étude intitulé "Données : actifs protégés ou bombe à retardement ?" se fonde sur des entretiens menés en octobre 2014 auprès de 2 276 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne.

Source : http://www.courriercadres.com/carriere/internet-et-l-entreprise/securite-des-donnes-71-des-employes-declarent-avoir-acces-15122014

Par Audrey Pelé

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