Les Français s’intéressent enfin à leur réputation sur Internet | Le Net Expert Informatique

	Les Français s’intéressent enfin à leur réputation sur Internet

Le rapport d'activité 2014 de la CNIL met en lumière l'intérêt de plus en plus fort des Français pour leurs données personnelles. Sur les 5.825 plaintes reçues, près de 40% concernent l'e-reputation.

La place de plus en plus large des technologies dans la société à des conséquences directes sur la Cnil. Après les données laissées sur Internet via les moteurs de recherche ou les réseaux sociaux, les objets et les voitures connectés et les données santé sont autant de champs qui, comme le dit Isabelle Falque-Pierrotin, sa présidente , « élargit notre terrain de jeu ».

A tout cela s'ajoute les nouveaux dispositifs légaux, français ou européens, qui étendent encore plus le périmètre des équipes de la rue Vivienne.

Mais, cette effervescence a tout de même un effet positif. « **Il y a une prise de conscience. Désormais, les internautes ont la ferme intention de maîtriser l'usage qui est fait de leurs données.** » Et, pour Isabelle Falque-Pierrotin, « ça, c'est une nouveauté ! ».

En 2014, 5.825 plaintes ont été envoyées à la Cnil. La hausse par rapport à 2013 est de 3%. Mais, ce qui est significatif, c'est que désormais 39% des réclamations reçues concernent des problématiques d'e-reputation.
Mais aussi, les demandes de droit d'accès indirect, celles qui concernent les fichiers fiscaux (Ficoba), judiciaires (police et gendarmerie) ou de renseignements, explosent littéralement. Avec 5.426 plaintes reçues, la hausse par rapport à 2013 est de 22%.
Pour ne pas être asphyxiée par ces demandes, la Cnil a dû prendre des mesures. « Nous avons recruté 6 nouveaux agents, mais nous avons aussi allégé et simplifié les procédures pour fluidifier notre travail », précise la présidente de la Cnil. Elle ajoute aussi que, dans un souci d'économie, un programme de réduction des coûts a été mis en place. « Nous avons commencé par renégocier notre bail ».

Surveillance de masse : un dossier à risque
Mais actuellement, le sujet chaud reste la loi de renseignement qui n'en finit plus d'ébranler de nombreux internautes convaincus que ces mesures sont la version française du Patriot Act américain. Et qu'elles finiront tôt ou tard par se retourner contre les citoyens. Pour la présidente de la Cnil, « la crainte d'une surveillance de masse se confirme comme nous le redoutions depuis les révélations d'Edward Snowden. »
La Cnil a été l'une des premières institutions à réagir et ce, dès l'avant -projet de la loi renseignement. « Les données personnelles et la protection de la vie privée sont des droits fondamentaux et notre mission est de les protéger, a réaffirmé la présidente. Si la surveillance de masse enfreint la morale, elle enfreint surtout le droit français et européen. »
Elle a également insisté sur la cohérence de sa mission avec l'économie et l'innovation. « On nous a souvent reproché de freiner à la fois l'innovation et le développement des entreprises. C'est tout le contraire. En rassurant les internautes, nous leur redonnons confiance dans les services et les institutions. » Pour appuyer cette affirmation, la présidente de la Cnil s'est appuyée sur la réaction des hébergeurs qui craignent de lourdes retombées économiques si la loi est adoptée.
« Il ne s'agit pas de de s'opposer à des mesures qui peuvent être nécessaires, mais si la surveillance s'accroit, le contrôle doit s'adapter. » Un argument qui a été contesté avec le rejet des amendements proposés par la Cnil au motif que son action serait « contradictoire avec l'action de l'Etat. »
Malgré tout, la Cnil veut toujours des informations sur le devenir des données qui seront récoltées par les autorités. Un point qui reste toujours sans réponse. « J'ai appris à être patiente et à ne jamais abandonner », conclut la présidente.

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

Source : http://bfmbusiness.bfmtv.com/entreprise/les-francais-s-interessent-enfin-a-leur-reputation-sur-internet-878131.html
Par Pascal Samama

Données médicales publiques : que faut-il craindre ? | Le Net Expert Informatique

	Données médicales publiques : que faut-il craindre ?

Une immense base de données pourrait bientôt être créée pour centraliser toutes nos données médicales. Faut-il s'en inquiéter ?

Les députés débattront jeudi de l'article 47 du projet de loi santé. Cette discussion pourrait bien être déterminante pour la recherche médicale puisque le texte prévoit de rendre publiques les données médicales françaises. Les fiches d'hospitalisation mais aussi les feuilles de soins ou les causes de décès sont autant de documents qui, après avoir été rendues anonymes, pourraient être réunies à l'avenir dans le « système national des données de santé » (SNDS).

« Intéressant de disposer de ces données ». « Dans la démocratie sanitaire, l'open data permet à chacun d'accéder à des informations sur son médecin ou sur la qualité d'un établissement », explique à Europe 1 Emmanuel Hirsh, professeur d'éthique médicale à l'université Paris Sud. « C'est extrêmement intéressant de disposer de ces données. Mais les questions de santé sont des questions sensibles et la confidentialité doit être assurée ». Et de soulever une question primordiale : « que faut-il faire de ces informations sensibles si, à un moment donné, la confidentialité est rompue ? »

Emmanuel Hirsh : « La confidentialité doit être… *par Europe1fr*

« La Cnil est déjà dépassée ». « Un institut (le SNDS) va superviser ces données personnelles de santé. La Cnil (Commission nationale de l'informatique et des libertés) va également intervenir » pour donner ou non son feu vert, détaille Emmanuel Hirsh. « Mais on voit déjà que la Cnil est dépassée pour de nombreuses questions sur internet », s'inquiète une nouvelle fois le professeur d'éthique médicale. Il y a tout un ensemble de protections, de lois en France en matière de bioéthique. Mais dans la pratique, comment ça va se passer ? »

Quelles sont les dérives possibles ? Après avoir souligné une nouvelle fois le fort potentiel de recueillir toutes ces données, notamment pour la recherche médicale, Emmanuel Hirsh s'inquiète des mauvaises utilisations potentielles. « En matière génétique, par exemple, on aura à l'avenir beaucoup plus d'informations sur le devenir d'une personne, sur les maladies qu'elle développera dans son futur. Qu'est-ce qu'on va faire de ces données ? Il ne faudrait pas qu'elles soient détournées à des fins politiques », explique-t-il à Europe 1. Et de donner un conseil avant la discussion de la loi à l'Assemblée nationale : « il faut absolument renforcer les garde-fou et la partie éthique de la loi pour améliorer la démocratie sanitaire ».

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

Source : http://www.europe1.fr/sante/donnees-medicales-publiques-que-faut-il-craindre-2421231
Par Victor Dhollande-Monnier

Les 6 plaintes les plus courantes reçues par la CNIL | Le Net Expert Informatique

Les 6 plaintes les plus courantes reçues par la CNIL

Que faire quand on vous refuse la suppression d'une information personnelle qui se retrouve sur Internet ? Contacter la Commission nationale informatique et libertés (CNIL), le « Zorro » des internautes dont la e-réputation est en péril. Daniela Parrot, chef du service des plaintes de la commission, a établi le top 7 des plaintes les plus courantes, concernant les données des internautes.

e-réputation : comment effacer vos casseroles numériques

1 – Les photos et commentaires mis en ligne sans votre accord sur les réseaux sociaux

Certes les procédures mises en place par les administrateurs des réseaux sociaux sont efficaces. « Par exemple sur Facebook, il est facile de demander la suppression et/ou de signaler les abus », confirme la Commission nationale informatique et libertés (CNIL). Mais pour éviter les mauvaises surprises, le bon réflexe c'est de paramétrer votre profil en soumettant par exemple les photos et les écrits de vos amis à votre validation avant publication.

2 – Les faux profils ou le piratage

Pour vous prémunir des faux profils, mettez en place une « google alert » qui vous avertira par mail dès que votre nom sera cité sur la toile. Si vous avez été piraté, contactez là encore la CNIL, compétente pour l'ensemble des litiges lié à vos données personnelles sur Internet. Dans un cas extrême, la CNIL pourra faire appel au procureur de la République qui diligentera une enquête.

3 – La diffusion des données personnelles

Sachez-le, les forums ne sont pas si privés. Certains de vos commentaires sont indexés et remontent sur les moteurs de recherche. Soyez vigilant y compris lorsque vous diffusez votre CV sur le web. N'oubliez pas qu'il contient votre téléphone, adresse et mail ! « Si vous souhaitez faire disparaître ces données, adressez-vous au responsable du site et/ou vérifiez la procédure de référencement », indique la CNIL qui pourrait être votre dernier recours.

4 – Les vidéos

Soyez attentif, le pouvoir de YouTube est immense car il y a une très forte viralité. En cas de problème, adressez-vous au plus vite au site pour supprimer le contenu. Si cela ne marche pas, contactez la CNIL.

5 – Les journaux en ligne

Un article vous cite sans raison valable ? Contactez le journal et indiquez les motifs justifiant votre requête. « L'article peut être supprimé, anonymisé ou déréférencé », explique Daniela Parrot. Si le journal ne motive pas son refus, la CNIL renvoie l'affaire devant les tribunaux.

6 – Les décisions de justice

Faites attention, les décisions de justice sont parfois référencées sur la toile. Selon le délit, cela peut être gênant ! Contactez la CNIL pour demander à ce que la décision soit rendue anonyme.

---

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

Contactez-nous

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

Source : http://actualites.cadremploi.fr/editorial/conseils/droit-du-travail/detail/article/e-reputation-les-7-plaintes-les-plus-courantes-recues-par-la-cnil.html#xtor=CS2-1016

Votre employeur peut

espionner vos communications chiffrées, et la CNIL est d'accord | Le Net Expert Informatique

Votre employeur peut espionner vos communications chiffrées, et la CNIL est d'accord

La Commission nationale informatique et libertés donne sa bénédiction au déchiffrement des flux HTTPS des salariés, à condition que cette pratique soit encadrée. Il reste néanmoins une zone de flou juridique côté pénal…

Saviez-vous que certains employeurs déchiffrent systématiquement les flux HTTPS de leurs salariés lorsqu'ils surfent sur Internet ? Ils disposent pour cela d'un équipement appelé « SSL Proxy » qui se place entre l'utilisateur et le serveur Web. Cette boîte magique déchiffre tous les échanges en usurpant l'identité du service interrogé (google.com, par exemple), par l'utilisation d'un certificat bidon. La pratique n'est pas du tout récente, mais se fait de manière un peu cachée en raison d'incertitudes juridiques et de l'impopularité de cette mesure auprès des salariés. Les directeurs informatiques n'ont, par conséquent, pas une folle envie d'en faire la publicité.
Mais l'employeur peut se rassurer : la CNIL vient de publier une note qui clarifie les choses. Ainsi, la Commission estime que le déchiffrement des flux HTTPS est parfaitement « légitime », car elle permet à l'employeur d'assurer « la sécurité de son système d'information », en bloquant les éventuels malwares qui s'y trouveraient. Evidemment, ce n'est pas la seule raison : ces équipements sont également utilisés pour prévenir les fuites d'informations. Un salarié qui enverrait des documents confidentiels à un concurrent pourrait, ainsi, être facilement repéré.

Infraction pénale ou pas ?
Toutefois, la CNIL met un (petit) bémol. L'utilisation de cette technique de surveillance doit être « encadrée ». Ainsi, les salariés doivent être informés en amont et de manière « précise » sur cette mesure : raisons invoquées, personnes impactées, nature de l'analyse effectuée, données conservées, modalités d'investigation, etc. L'employeur doit également mettre en place une « gestion stricte des droits d'accès des administrateurs aux courriers électroniques ». Autrement dit : éviter que tous les membres du service informatique puissent fouiller dans les messageries. Par ailleurs, les « traces conservées » doivent être réduites au minimum.
Il reste néanmoins une petite zone de flou juridique, nous explique la CNIL. En effet, le Code pénal interdit théoriquement « d'entraver ou de fausser le fonctionnement d'un système de traitements automatisés de données (STAD) ». Or, quand l'entreprise déchiffre les flux Gmail de ses salariés, on peut estimer que cela fausse le fonctionnement du STAD d'un tiers, à savoir Google. Cela pourrait donc constituer une infraction. Conclusion de la CNIL : il faudrait peut-être modifier le Code pénal pour que l'employeur puisse réellement surveiller ces flux chiffrés en toute tranquillité. Décidément, la situation n'est pas encore totalement claire…

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

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

Source : http://www.01net.com/editorial/651057/votre-employeur-peut-espionner-vos-communications-chiffrees-et-la-cnil-est-d-accord/
Par Gilbert Kallenborn

Vote électronique : précisions sur la sécurité et la confidentialité | Le Net Expert Informatique

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Vote électronique : précisions sur la sécurité et la confidentialité

Opter pour un prestataire pour l'organisation des élections professionnelles par vote électronique ne dédouane pas l'employeur de sa responsabilité en cas d'irrégularités. C'est ce que rappelle le Conseil d'Etat dans cette affaire. Il en profite pour apporter quelques précisions sur les garanties essentielles gouvernant ce dispositif en termes de confidentialité et de sécurité des données (Conseil d'Etat, 11.03.15, n°368748).

Pour élire ses délégués du personnel, la société X a décidé de mettre en place le vote électronique. Ayant déjà recouru à ce dispositif lors des précédentes élections professionnelles (en 2012), elle s'adresse au même prestataire extérieur.
Mais voilà qu'un syndicat conteste le bon déroulement des opérations et saisit la CNIL d'une plainte. Après enquête, cette dernière relève effectivement un certain nombre d'irrégularités. Aussi, elle prononce à l'encontre de l'entreprise, un avertissement et rend publique cette décision sur internet.
Contestant les manquements reprochés, et non contents de cette (mauvaise) « publicité », l'entreprise et le prestataire saisissent le Conseil d'Etat pour demander l'annulation la délibération de la CNIL.
Mais le Conseil d'Etat va approuver en tous points les manquements soulevés par la CNIL, et confirmer ainsi la sanction prise à l'encontre de la société requérante.

La pleine responsabilité de l'employeur, même en présence d'un sous-traitant

Pour rappel, l'employeur a la possibilité de confier à un prestataire la mise en place du système de vote électronique dans son entreprise. C'est l'option retenue par la société en l'espèce et c'est précisément grâce à ce sous-traitant qu'elle va tenter de s'affranchir de sa responsabilité. Elle estime en effet que le prestataire présentait des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Pour résumer, sa responsabilité se limitait au choix d'un « bon » prestataire. Elle n'était donc pas responsable des irrégularités commises par ce dernier.
Le Conseil d'Etat ne l'a pas entendu ainsi. Il considère au contraire que « la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de réserver la sécurité des données ». Le sous-traitant agissant « sur instruction du responsable de traitement », c'est bien sur ce dernier que repose l'obligation de veiller au respect de la sécurité et de la confidentialité des données personnelles. Les manquements constatés étaient donc imputables à la société requérante en sa qualité de responsable de traitement.

L'exigence d'une expertise préalable indépendante à chaque scrutin

Le Code du travail (1) soumet le système de vote électronique à une expertise indépendante préalable à sa mise en place ou à toute modification de sa conception. En l'espèce, le système ayant déjà été utilisé lors des dernières élections, et n'ayant fait l'objet d'aucune modification depuis, il n'a pas été jugé nécessaire de renouveler cette expertise préalable. Première erreur, car le Conseil d'Etat a interprété un peu plus largement les dispositions légales : si la réalisation d'une expertise indépendante est nécessaire au moment de la conception initiale du système et à chaque modification de la conception de ce système, elle l'est également « avant chaque scrutin recourant au vote électronique ». Afin de garantir la sincérité des opérations électorales par voie électronique, l'expertise aurait donc dû être renouvelée avant le scrutin.

Une transmission des moyens d'identification aux électeurs sécurisée

Au moment de voter électroniquement, l'électeur doit se connecter et se faire connaître par le moyen d'authentification qui lui a été transmis selon des modalités garantissant sa confidentialité (2). Ce moyen permet au serveur de vérifier l'identité de l'électeur et de garantir ainsi l'unicité de son vote. Il se trouve qu'en l'espèce, la transmission aux électeurs des identifiants et mots de passe, leur permettant de participer au vote, a été faite par simple courriel. Seconde erreur.
La CNIL a estimé que ce mode de transmission n'avait pas fait l'objet de mesures de sécurité spécifiques permettant de s'assurer que les électeurs en étaient les seuls destinataires(3).

Un chiffrement des bulletins de vote ininterrompu

Enfin, un arrêté ministériel (4) impose que le chiffrement (ou cryptage) et l'anonymat des bulletins de vote soit ininterrompu de l'émission du vote sur le poste de l'électeur, jusqu'à la transmission au fichier dénommé « contenu de l'urne électronique ». Voici donc le troisième manquement commis par la société : la CNIL a relevé que le système de chiffrement ayant été interrompu à un moment donné, il ne présentait pas un niveau de sécurité suffisant.

Ce rappel des règles était nécessaire. On peut ajouter que le Conseil d'Etat pousse plus loin encore la responsabilité de l'employeur dans le respect des règles relatives au vote électronique en approuvant la sanction infligée par la CNIL alors même que ces irrégularités n'ont entraîné ici aucune atteinte effective aux données personnelles des électeurs, ni aux principes du droit électoral ou encore aux libertés publiques.

(1) Art. R. 2314-12 du Code du travail.
(2) Art. R. 2324-5 du Code du travail.
(3) Cette solution n'est pas nouvelle, elle avait déjà été retenue par la chambre sociale de la Cour de Cassation dans un arrêt du 27 février 2013, n°12-14.415.
(4) Art. 2 de l'arrêté du ministre de l'Emploi, de la cohésion sociale et du logement pris en application du décret n°2007-602 du 25 avril 2007.
[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Source : http://www.cfdt.fr/portail/le-carnet-juridique/fil-d-actualites/vote-electronique-precisions-sur-la-securite-et-la-confidentialite-srv1_255996

La Commission européenne conseille de quitter Facebook | Le Net Expert Informatique

La Commission européenne conseille de quitter Facebook

Un avocat de la Commission européenne a conseillé au procureur général de la Cour de Justice de l'Union Européenne (CJUE) de fermer son compte Facebook pour éviter que ses données personnelles soient exploitées aux Etats-Unis.

« Vous devriez envisager de fermer votre compte Facebook si vous en avez un » a conseillé Bernhard Schima, l'avocat de la Commission européenne, au procureur général de la JUE Yves Bot la semaine dernière. Une recommandation lancée dans le cadre d'une audience concernant la confidentialité des données des Européens vis-à-vis de l'utilisation qu'en fait le géant américain. La question avait été soulevée il y a plusieurs années par Max Schrems, un étudiant en droit autrichien qui a déclenché en août 2014 une procédure d'action collective mondiale à l'encontre de Facebook.
Mais le procès actuellement en cours oppose Max Schrems à l'équivalent irlandais de la CNIL, contre laquelle l'Autrichien a porté plainte, refusant de voir ses données personnelles stockées par Facebook – dont le siège européen se trouve en Irlande – transférées aux Etats-Unis pour alimenter le ciblage publicitaire de l'entreprise. Le réseau social n'est pas le seul concerné : Microsoft, Apple ou encore Yahoo sont également pointés du doigt.

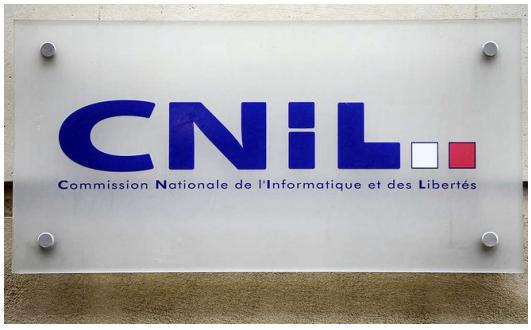
Ciblage et espionnage
Max Schrems considère que les révélations d'Edward Snowden concernant l'espionnage des données pratiqué par la NSA met les Européens en danger à partir du moment où leurs données personnelles transitent aux Etats-Unis. Une accusation qui remet en question l'application du Safe Harbor, un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises qui adhèrent à ces principes peuvent recevoir des données en provenance de l'UE, mais la surveillance généralisée de la NSA remettrait en question l'application de ces règles.
On comprend mieux en quoi la petite phrase de l'avocat de la Commission européenne est lourde de sens : elle semble donner raison à la théorie de Max Schrems, engagé depuis longtemps contre la collecte d'information, jugée abusive, par Facebook.
Le commissaire irlandais à la protection des données considère quant à lui qu'il n'existe aucune preuve que le transfert des données de Max Schrems aux Etats-Unis lui a porté préjudice. « Ce n'est pas étonnant dans la mesure où la NSA n'est pas intéressée par les essais écrits par les étudiants en droit autrichiens » a-t-il ironisé. L'avocat général devrait rendre son avis sur l'affaire le 24 juin prochain.

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

Source : http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-760937-protection-donnees-personnelles-commission-europeenne-conseille-quitter-facebook.html

---

Les réserves de la CNIL sur le projet de loi renseignement | Le Net Expert Informatique



Les réserves de la CNIL sur le projet de loi renseignement

Il n'y aura pas de surveillance généralisée du citoyen, assure-t-on à Matignon, alors que le projet de loi renseignement doit être présenté jeudi en Conseil des ministres. Cela n'a pas empêché la Commission nationale de l'informatique et des libertés (CNIL) d'émettre un certain nombre de réserves sur ce texte, dont le calendrier a été accéléré après les attentats contre Charlie Hebdo et le supermarché casher de la porte de Vincennes.

Le projet de loi va permettre « une surveillance beaucoup plus large et intrusive », estime un pré-rapport dont « Les Echos » ont pu prendre connaissance. Si les objectifs du gouvernement paraissent « justifiés », « les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire », écrit la CNIL.

Trois dispositifs nouveaux (collecte automatique d'informations sur les réseau, pose de sondes, sorte de mouchard permettant de collecter des informations en direct sur des personnes surveillées, et pose d'antennes à proximité de suspects) permettent de « collecter de manière indifférenciée un volume important de données » sur « des personnes relativement étrangères » aux suspects. « Ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles », avertit la CNIL.

« Aspiration massive de données »

Dans le détail, la détection « par un traitement automatique » des comportements suspects ressemble fort à de la surveillance généralisée. A Matignon, on se montre soucieux de faire de la « pédagogie » sur le sujet. L'objectif de la mesure, explique-t-on, est de détecter « les signaux faibles » permettant d'identifier des individus susceptibles de basculer dans le terrorisme. « Aujourd'hui, ceux qui partent n'ont pas été détectés avant leur départ [vers la Syrie, etc., ndlr]. Or, 89 sont morts, dont un garçon de 14 ans », rappelle-t-on à Matignon.

Pour détecter ces inconnus, les agents veulent pouvoir analyser les flux de données, savoir qui communique avec qui, et quels sont les sites jihadistes visités. Pas d'autres moyens donc que de faire de la surveillance sur le réseau des opérateurs. « Nous voulons insérer dans les équipements des opérateurs des boîtes noires contenant des algorithmes identifiant des comportements marqueurs », précise Matignon. Si en théorie, la disposition pourrait s'appliquer aux géants du Net, les agents de l'Etat préfèrent d'abord aller traiter avec les opérateurs télécoms, considérant qu'ils sauront se montrer plus ouverts à leurs requêtes.

Inévitablement, une partie des flux échappera aux services, Google ayant depuis les révélations d'Edward Snowden chiffré l'ensemble des connexions de ses utilisateurs.

Quant à la captation en temps réel des données géolocalisées de personnes mises sous surveillance (3.000 personnes environ), elle est assimilée par la CNIL à un dispositif « d'aspiration massive et directe des données par l'intermédiaire de la pose de sondes ». Enfin, le système « IMSI Catcher » (pose d'antennes relais à proximité d'un suspect) permet aussi d'intercepter des informations sur des personnes n'ayant rien à voir avec les faits, regrette la CNIL.

De leur côté, les interceptions de sécurité – les fameuses écoutes – ne sont plus « exceptionnelles », note la CNIL, même si le texte « renforce les modalités de contrôle ». Surtout, la loi donne la possibilité « par réaction en chaîne » d'écouter « des personnes qui n'auraient pas été en relation avec la personne surveillée ».

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

Source : http://www.lesechos.fr/tech-medias/hightech/0204235783787-les-reserves-de-la-cnil-sur-le-projet-de-loi-renseignement-1103298.php
Par Sandrine Cassini

Laboratoire d'analyses

médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données auraient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés
Aujourd'hui, rebelotte avec le même groupe Rex Mundi et, là encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.
Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »
Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates
Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

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

Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Reste – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Puricard
Laboratoire de Saint Rémy de Provence

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

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm

---

Est-ce que l'iPhone est vulnérable ? | Le Net Expert Informatique

Est-ce que l'iPhone est vulnérable ?

Est-ce que les iPhone sont vulnérables à l'espionnage, c'est la question que l'on peut se poser en sachant que la CIA cherche à le casser depuis sa création.

Selon la récente publication de The Intercept, on sait que la CIA a tenté de « casser », percé le chiffrement, des produits Apple depuis 2006. Cela signifie que l'agence américaine a bien évidemment aussi tenté de percer les sécurités de l'iPhone vu que la première édition est sortie en 2007. La grande question est de savoir si la CIA est arrivée à ses fins.
Sans revenir sur tous les détails de cette révélation faite sur la base des documents dévoilés par Edward Snowden, on peut comprendre de nombreuses choses à partir de cette nouvelle affaire d'espionnage des utilisateurs.
Pour commencer, il n'y avait pas que la NSA qui cherchait à collecter des données personnelles des utilisateurs de smartphones. Alors que les lois américaines empêchent normalement l'espionnage des citoyens américains, on peut sérieusement se poser la question si ces textes n'ont pas tout simplement été bafoués en essayant de casser le chiffrement des iPhone alors que les Américains sont friands de produits Apple.
Si découvrir des failles dans les systèmes Apple s'explique par le fait de vouloir obtenir des données des utilisateurs, on peut se poser la question de savoir pourquoi la CIA n'a pas averti Apple de l'existence de ces failles ? Il semble évident que cela aurait été un aveu de culpabilité.
Par contre, un peu prendre cet aspect d'un autre point vu en considérant que ce que les agences américaines ont fait, d'autres agences de pays hostiles ont également pu le faire. De fait, ne pas communiquer ces failles serait une mise en danger des données personnelles des citoyens américains.
En sachant tout cela, on comprend parfaitement pourquoi les constructeurs, notamment Apple, ont renforcé la sécurité de leurs systèmes et refusent d'ouvrir des backdoors « légales » pour les autorités. En effet, comment pourrait-il exister une moindre confiance ?
En sachant tout cela, on ne comprend par contre pas la véhémence des agences américaines qui dénoncent les méthodes de cryptage mises en place par les entreprises. En effet, ces mesures ne visent que la protection des données des utilisateurs, notamment des biens appartenant à des Américains.
Au final, le débat sur la protection des données personnelles va encore faire couler beaucoup d'encre.

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

Source : http://www.linformatique.org/est-ce-que-liphone-est-vulnerable/

Quelles sont les conséquences d’un oubli de déclaration à la CNIL de données de Géolocalisation ?

Quelles sont les conséquences d’un #oubli de déclaration à la CNIL de données de #Géolocalisation ?

1- RAPPEL DES FAITS ET DE LA PROCEDURE

Un salarié a été engagé par une société en qualité de commercial par un contrat à durée déterminée.

La société a procédé à la rupture anticipée de son contrat, en invoquant une faute grave commise par le salarié.

Par jugement, le conseil de prud'hommes a considéré que la rupture anticipée du contrat pour faute grave était justifiée et a rejeté les demandes du salarié.

Celui-ci a interjeté appel de la décision prud'homale. Il conteste la faute qui lui est reprochée. Parmi les arguments, il soutient :

qu'en vertu de l'article 4 de son contrat de travail, il disposait « de toute latitude dans l'organisation de son travail » et pouvait « déterminer à sa guise les dates et amplitudes de ses journées de travail »,

que l'employeur n'aurait pas eu un comportement loyal pour avoir fait installer à son insu un « mouchard » sur le véhicule de fonction qui lui avait été confié, l'illégalité du procédé rendant irrecevable le grief établi par ce moyen.

2- LA DECISION DE LA COUR D'APPEL

La Cour d'appel rappelle que la faute grave est celle qui résulte d'un fait ou d'un ensemble de faits imputables au salarié qui constituent une violation des obligations résultant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible le maintien du salarié dans l'entreprise.

Que l'employeur qui invoque la faute grave pour licencier doit en rapporter la preuve.

La société produit les relevés de géolocalisation du véhicule mis à la disposition du salarié, comme preuve de la faute grave.

A ce titre, et avant d'aborder le fond, la Cour d'appel s'est prononcée sur la recevabilité de la preuve des faits fautifs apportée par l'employeur, constituée de relevés de géolocalisation.

1- En effet, les juges du fond ont vérifié tout d'abord si le salarié était informé de la mise en place du système de géolocalisation.

Ce qui était le cas en l'espèce. Car, le salarié avait contresigné un document l'informant que son véhicule était équipé d'un système de géolocalisation qui permet de localiser le véhicule en temps réel.

2- Puis, les juges ont vérifié si le système de géolocalisation a bien été préalablement déclaré à la CNIL.

Ils ont pu ainsi constaté, par le récépissé de déclaration à la CNIL, que le système avait bien été déclaré à la CNIL et que les formalités préalables exigées par la CNIL avaient été respectées.

3- Et enfin, ils ont vérifié si le système de géolocalisation a bien été utilisé conformément aux finalités déclarées auprès de la CNIL et portées à la connaissance du salarié.

En effet, la Cour d'appel rappelle: »() qu'un système de géolocalisation ne peut cependant être utilisé par l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la Commission nationale de l'informatique et des libertés, et portées à la connaissance des salariés. »

Selon les juges du fond, l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail n'est licite que lorsque ce contrôle ne peut être fait par un autre moyen.

Elle n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail.

Or, les juges ont relevé que l'unique finalité du système de géolocalisation mis en place par la société déclarée à la CNIL, était la suivante : « Géolocalisation des véhicules utilisés par les employés ».

Il avait été précisé au salarié que ce système permettait de localiser le véhicule en temps réel sans que soit évoqué l'exercice d'un pouvoir de contrôle de l'employeur.

Ainsi, l'article 4 du contrat de travail du salarié était rédigé en ces termes dépourvus de tout caractère équivoque : « Monsieur X dispose de toute latitude dans l'organisation de son travail et pouvant déterminer à sa guise les dates et amplitudes de ses journées de travail et ce, dans le respect des règles définies par la convention collective mentionnée à l'article 1 du présent contrat. Compte tenu des fonctions de M.X et de son autonomie () ».

Par conséquent, dans ces conditions, la Cour d'appel a clairement écarté des débats la pièce produite par la société, constituée par les rapports de géolocalisation utilisés de manière illicite à des fins de contrôle du salarié non déclarées à la CNIL et dont l'utilisation n'était, de plus, pas justifiée dès lors que le salarié disposait de toute liberté dans l'organisation de son travail.

L'employeur ne rapportant pas la preuve de la falsification des rapports reprochée au salarié, la rupture du contrat de travail est sans cause réelle et sérieuse.

En somme, l'arrêt de la Cour d'appel de Paris du 4 novembre 2014, ne fait que confirmer les précédentes décisions relatives à la licéité et la loyauté de la preuve en matière civile.

Ce qu'il faut retenir de cet arrêt est que, les entreprises devront être plus vigilantes lors des déclarations faites auprès de la CNIL, quant aux dispositions de contrôle et leur finalité, et ce, sans omettre d'en informer leurs salariés et de consulter préalablement le comité d'entreprise (l'article L. 2323-32 du Code du travail).

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

Source : http://www.juritravail.com/Actualite/mettre-place-cameras-surveillance/Id/191621
Cour d'appel Paris Pôle 6 Chambre 10 n°11/09352
Par Me Maître Dalila Madjid Avocat au Barreau de Paris