Une Agence française du numérique prévue début 2015

Une Agence française du numérique prévue début 2015

Axelle Lemaire a répondu à une question d'un député à propos de la création annoncée de l'Agence Française du Numérique qui regroupera plusieurs institutions existantes. Son lancement est prévu pour le début de l'année 2015.

L'Agence française du numérique a pour objectif de regrouper sous son aile plusieurs initiatives du ministère de l'Economie dans le domaine : la French Tech, la mission Très Haut Débit ainsi que la délégation aux usages de l'Internet. Ce projet avait déjà été évoquée en début d'année 2014 lors des premiers travaux de préparation de la grande loi numérique prévue à l'agenda du gouvernement pour 2015.
Le Figaro, qui évoquait alors la création de cette agence, avançait une création pour la fin d'année 2014 mais Axelle Lemaire, dans une réponse à une question parlementaire, à modifié le calendrier et programme maintenant la mise en place de cette agence au début de l'année 2015.

Simplification
Une simplification bienvenue alors que le gouvernement multiplie les initiatives en forme de mille-feuilles, missions et autres organismes dédiés au numérique : l'agence viendra coordonner les actions de la French Tech, de la mission THD et de la délégation aux usages de l'Internet. Cette dernière délégation, plus discrète que les deux autres, a été crée en 2003 et aura pour mission « le déploiement d'usages de proximité à l'intention des citoyens dans les territoires. » Cette délégation pilote plusieurs programmes et mission à l'échelle nationale visant à favoriser et informer les citoyens sur les enjeux numériques contemporains.
L'agence restera sous la coupe de Bercy : comme le précisait Axelle Lemaire lors d'une audition avec la commission des affaires économiques du Sénat, l'agence « n'a rien à voir avec le Conseil National du Numérique instance totalement indépendante qui rend des avis sur tous types de sujets ».

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

Source : http://www.zdnet.fr/actualites/une-agence-francaise-du-numerique-prevue-debut-2015-39811721.htm
Par Louis Adam

Face à la transformation numérique, les RH doivent se moderniser

	**Face à la transformation numérique, les RH doivent se moderniser**

Les réseaux sociaux, le big data, les technologies mobiles et le cloud vont influer sur la gestion des RH et sur la manière dont les entreprises recrutent et fidélisent leurs collaborateurs, estime l'éditeur de solutions de gestion des talents Lumesse.

L'éditeur de solutions de gestion des RH Lumesse, a identifié quelques-unes des grandes tendances qui vont marquer les DRH au cours des années à venir. Selon ses estimations, les entreprises devront d'abord faire l'effort de moderniser leur stratégie de recrutement pour séduire et identifier plus facilement les meilleurs candidats. Il leur faudra utiliser des méthodes technologiquement plus sophistiquées telles que les entretiens vidéo pour faire vivre une expérience interactive aux candidats et ne pas les décourager, à coup de dossiers à remplir, de longs questionnaires, de déplacements à des kilomètres ou d'entretiens en série.
Lumesse table également sur la disparition des entretiens individuels tels qu'on les connaît au profit de tests de compétences ou de pratiques « plus sociales » de gestion des ressources. Pour l'éditeur, les entreprises ont plutôt intérêt à envisager une approche mixte de gestion de leurs collaborateurs et à organiser des évaluations formelles plus fréquemment. A partir de 2015, les DRH devraient également commencer à examiner les manières de travailler de même que les réactions, émotions et réflexions de leurs équipes. Ce type de données pourra être collecté par des capteurs et obtenu à l'occasion de tests. Par exemple, en pondérant les réponses-type des candidats à certaines questions de recrutement ou en comprenant mieux, par l'analyse des données, quelle marque séduit le plus le cerveau, les entreprises pourront mieux affiner leurs stratégies de recrutement et de gestion des talents.

Des besoins en data scientists et en responsables de la sécurité des données
Lumesse pense aussi que 2015 sera marquée par l'avènement d'une génération d'actifs ayant de fortes compétences dans le numérique, ainsi que par un nouvel esprit d'entreprise. Dans une démarche de formation continue des salariés, les recruteurs vont devoir structurer les conditions d'apprentissage sur le long terme et encourager des poches d'innovation à court terme sur la base d'idées des collaborateurs. Les RH vont avoir un rôle crucial à jouer pour accompagner la transformation numérique de leurs produits et services. Enfin, l'éditeur s'attend à la disparition prochaine du responsable des réseaux sociaux. Pour lui, les entreprises et les professionnels, à qui cette fonction s'adressait pour les former au numérique et les encadrer, sont désormais suffisamment compétents. Les attributions du rôle ont changé au gré de l'évolution de l'environnement numérique.

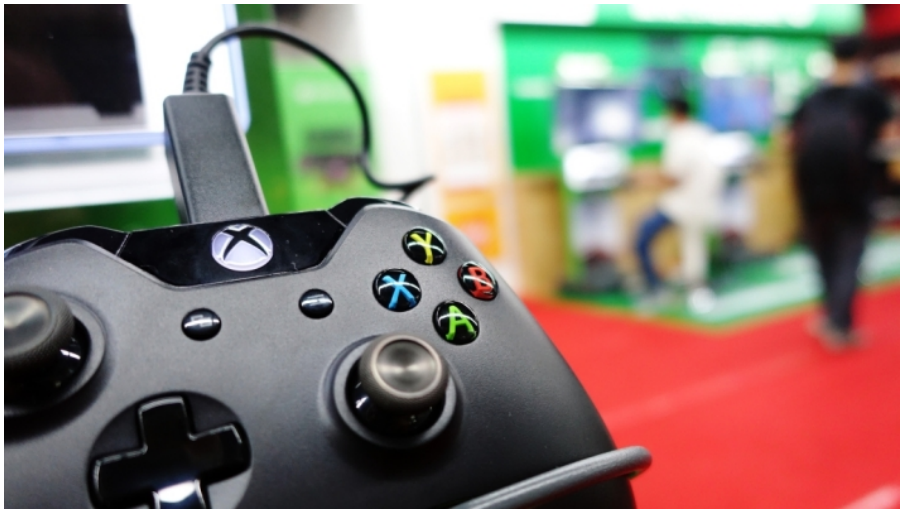
A présent, ce sont de data scientists et de responsables de la confidentialité des données dont les entreprises ont besoin. « 2015 promet d'être une année chargée pour les responsables des RH », a commenté Eric Gellé, directeur de Lumesse pour l'Europe de l'Ouest. « Au lieu d'y voir une menace, les DRH doivent envisager l'évolution du marché comme une formidable occasion de stimuler l'innovation et de s'en emparer, surtout dans les secteurs les plus compétitifs » , a-t-il conclu.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-face-a-la-transformation-numerique-les-rh-doivent-se-moderniser-59729.html
Par Véronique Arène

PlayStation et Xbox victimes d'une panne après une cyber-

attaque



PlayStation et Xbox victimes d'une panne après une cyber-attaque

PlayStation et Xbox victimes d'une panne après une cyber-attaLes joueurs de Xbox (ci-dessus) et de Playstation ne peuvent actuellement plus connecter leur console aux services en ligne en raison d'un piratage.

Les services en ligne de Sony et Microsoft connaissent depuis hier de lourds problèmes techniques. Des hackers revendiquent la responsabilité de ces pannes qui ont gâché la fête de milliers de joueurs.
Noël difficile pour les fans de jeux vidéo qui ont connu la joie et aussitôt la frustration. Une fois leur nouvelle console fraîchement déballée et branchée à la télé, impossible de se connecter au Playstation Network et au Xbox Live, les services en ligne qui permettent notamment de télécharger des jeux pour les consoles de Sony et Microsoft. La mise hors ligne de ces réseaux a commencé le jour de Noël et perdurait vendredi, ont annoncé les deux géants du divertissement sur leurs comptes Twitter, précisant qu'ils tentaient de trouver une solution.
Mais qu'est-ce qui a pu transformer ces machines flambant neuves en boîtes de plastique inutiles. Gros bug technique ? Ou plus probablement, attaque informatique.
Car ces pannes simultanées sur deux grands services de jeux en ligne ont été revendiquées par Lizard Squad, un groupe de hackers habitué à ce genre d'action. Ils s'en étaient déjà pris aux serveurs de jeux célèbres, comme League of Legends ou World of Warcraft.

« Nos ingénieurs tentent de trouver une solution »
Les deux groupes n'en ont pas dit beaucoup plus sur les problèmes rencontrés par les joueurs, si ce n'est qu'ils travaillaient à les résoudre. Microsoft a fait appel à la patience des utilisateurs de Xbox. « Nous sommes conscients du problème et nous nous efforçons de trouver une solution rapidement! Nous apprécions votre patience et nous vous proposons de vous reconnecter quand vous en aurez l'occasion. Nous reviendrons vers vous quand nous en saurons plus », a précisé le groupe sur un site dédié aux clients de Xbox.
Concernant la panne affectant la Playstation de Sony, « nous sommes conscients des difficultés de certains utilisateurs à se connecter – nos ingénieurs tentent de trouver une solution », a publié @PlayStation sur Twitter.
Une épine supplémentaire dans le pied de Sony, qui vient de faire l'objet d'un vol massif de données confidentielles sur ses serveurs, au cours d'une attaque informatique sophistiquée, la plus grave cyber-attaque jamais menée contre les Etats-Unis. Washington avait alors accusé la Corée du Nord d'être responsable de ce piratage, considérant que Pyongyang serait hostile à la sortie du film « L'interview qui tue! ».
Ce n'est pas la première fois que PlayStation est victime d'une attaque. En 2011, des données personnelles concernant 77 millions d'utilisateurs de la console avaient été volées, obligeant Sony à désactiver son réseau pendant plus de trois semaines.

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

Source : http://bfmbusiness.bfmtv.com/entreprise/playstation-et-xbox-victimes-d-une-panne-apres-une-cyber-attaque-854463.html par Antony Morel

Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

	Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

Comme chaque semaine, l'Institut Marocain des Relations Internationales (IMRI) publie une chronique sur l'actualité. Cette semaine, son président Jawad Kerdoudi s'est intéressé à « La cybercriminalité, migration du crime réel vers le virtuel ».

La récente attaque aux Etats-Unis des systèmes informatiques de Sony Pictures relance le problème de la cybercriminalité. Celle-ci est définie comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication. Ces infractions concernent plusieurs secteurs tels que le « carding » qui porte sur le piratage des cartes bancaires, le « skimming » criminalité qui s'attaque aux automates, le « phising » qui est une pêche des informations bancaires et commerciales, et enfin les escroqueries sur internet de toutes sortes qui englobent la xénophobie, la pedopornographie, l'incitation à l'usage des stupéfiants, le proxenétisme, le terrorisme, et le piratage téléphonique au préjudice des opérateurs.
Ce phénomène prend de plus en plus d'ampleur avec le développement d'internet qui est certes un moyen formidable de communication, mais également un instrument puissant de pouvoir et de guerre. Selon le Computer Crime Research Center, seuls 12% des cybercrimes étaient connus par la police et la justice en 2004. Plusieurs scandales ont défrayé la chronique, dont celui de la NSA en 2013 provoqué par Edward Snowden. Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Les Etats-Unis perdent entre 17,5 à 87,5 milliards d'euros par an, et 556 millions de personnes dans le monde ont été victimes de cybercriminalité. Cette situation risque d'empirer du fait du développement extraordinaire des investissements dans le secteur technologique numérique tels que ADSL, L4G, WIFI, Cloud. Le phénomène risque de s'amplifier également par la dématérialisation des processus, le développement du e-commerce et du e-learning, la croissance des paiements en ligne, l'augmentation des utilisateurs du Web qui a enregistré un taux de croissance de 46% entre 2012 et 2013. Le haut lieu mondial de la cybercriminalité pour la création de logiciels malveillants est la Chine, suivie par la Russie, les Etats-Unis, le Brésil et le Royaume-Uni. Pour les machines détournées la première place appartient aux Etats-Unis, suivie par la Chine, la Corée du Sud, l'Allemagne et la France. Enfin par les crimes relatifs aux arnaques sur internet, la palme revient à l'Afrique en particulier la Côte d'Ivoire et le Nigeria.

MINIMISER LES CONSÉQUENCES DE L'ATTAQUE
Pour se protéger contre la cybercriminalité, il est clair que le risque zéro n'existe pas. Il faut faire en sorte que si elle arrive, les conséquences de l'attaque soient minimes. Il faut pour cela renforcer les moyens matériels et humains, procéder à une modification de la législation, développer une culture de l'informatique, et associer le secteur privé à la lutte contre ce fléau. Il faut également privilégier l'approche préventive, c'est-à-dire qu'il faut augmenter les difficultés des attaques en diminuant les profits potentiels. Cela signifié le renforcement de la robustesse des infrastructures informatiques et de télécommunications. Il faut enfin s'appuyer sur des structures de veille et d'alerte telles que le CERT/CC américain. La coopération internationale est indispensable, car les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les cybercriminels peuvent lancer des attaques informatiques ou héberger des sites illicites en toute impunité. Elle a déjà commencé par la Convention de Budapest du 23 Novembre 2001 sur la cybercriminalité qui a le mérite de régler les problèmes de compétence et d'entraide entre Etats, et de les obliger à conserver certaines données pour permettre le traçabilité de l'information. Elle énumère plusieurs infractions (accès illégal, interception illégale, atteinte à l'intégrité des données et des systèmes) pour lesquelles chaque pays doit avoir un volonté politique et une coopération efficace de leurs services de justice et de police. Cette coopération internationale pose le problème de la gouvernance d'internet sur le plan mondial. Certains s'interrogent sur la pertinence d'une réglementation, d'autres demandent qu'elle soit déclarée comme un bien commun, et placée sous le contrôle de l'ONU ou d'un organisme intergouvernemental autonome.

QU'EN EST-IL DE CETTE QUESTION DE LA CYBERCRIMINALITÉ POUR LE MAROC ?
D'après Microsoft, le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale. Le Maroc présente des failles touchant l'administration et les infrastructures qui constituent des menaces pour la sécurité nationale publique et économique. Preuve en est le piratage à partir du mois d'Octobre 2014 de documents confidentiels marocains relatifs à la diplomatie, au Sahara, et aux services de l'appareil de l'Etat. Le cybercriminel se fait appeler Chris Coleman, sévit sur un compte Twitter et n'a pas caché son objectif de nuire au Maroc. Une lecture officielle de ce cybercrime a été présentée le 11 Décembre 2014 devant la Chambre des Conseillers accusant les services spécialisés algériens d'avoir monté et accompagné cette opération. Dès lors, il faut que la cybercriminalité soit un chantier prioritaire pour le gouvernement, et passe du stade défensif à celui offensif. D'où la nécessité de créer une structure civile placée à un haut niveau, et qui aura par vocation la centralisation des informations et la coordination entre les services civils et militaires. Elle doit disposer également d'un centre de documentation chargé recueillir les statistiques spécifiques en vue de les analyser. Elle devra jouer un rôle opérationnel, signaler les contenus illicites sur internet, et apporter une assistance technique au profit du secteur public et privé. Elle sera également chargée de la formation et de la sensibilisation, et assurera les relations avec les Agences internationales chargées de lutter contre la cybercriminalité.

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

Source : http://www.aufait.ma/2014/12/23/chronique-de-jawad-kerdoudi-president-de-limri-la-cybercriminalite-migration-du-crime-reel-vers-le-virtuel_635947
par Jawad Kerdoudi, président de l'IMRI

La cybersécurité a-t-elle une obligation de résultat ?

La cybersécurité a-t-elle une obligation de résultat ?

Obligation de résultat ou obligation de moyens : qu'est-ce que cela implique en matière de cybersécurité ? Olivier Iteanu, avocat à la Cour (www.iteanu.com), nous livre son analyse et revient sur la sanction infligée à Orange par la Cnil.

Chacun conviendra qu'il est absurde de considérer que la sécurité en général, et plus particulièrement celle attachée aux systèmes d'information, soit soumise à une obligation de résultat. Aucune technologie, aucun système de défense n'est capable de garantir une fiabilité à 100 % contre toute attaque. L'éditeur d'une solution ou le prestataire qui prétendrait le contraire serait tout simplement un menteur. L'esprit humain est ainsi fait, et c'est tant mieux, qu'un jour ou l'autre, l'attaquant, venu de l'extérieur ou plus encore, de l'interne, trouve le moyen de contourner les meilleures protections techniques et organisationnelles mises en place.
Le pendant de l'obligation de résultat ou son contraire, est l'obligation de moyens. Dans le cas de l'obligation de moyens, si l'attaque a causé des dommages à des tiers, ceux-ci ne peuvent se retourner contre le maître du système attaqué pour obtenir réparation que si une négligence ou une faute prouvées peut être retenue contre lui. Dans le cas de l'obligation de résultat, le tiers n'aura qu'à démontrer l'existence de l'attaque et son dommage, pour engager la responsabilité du maître du système, sans même avoir à démontrer que ce dernier a commis une faute. Evidemment, on comprend ici que les conséquences de l'un ou de l'autre régime juridique sont radicalement différentes.
On est en droit de se demander si le système plein de bon sens de l'obligation de moyens en matière de cybersécurité, n'est pas remis en cause par une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014, qui a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés.
http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf

Que dit la loi ?
Pour mémoire, la Loi du 6 janvier 1978 en son article 34 prévoit que « Le responsable du traitement est tenu de prendre toutes précautions utiles (…) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » Le défaut de prendre « toutes précautions utiles » est sanctionné des peines maximales de 5 ans de prison et de 300 000 € d'amende par l'article 226-17 du Code pénal. Et comme la matière informatique et libertés prévoit une double peine aux contrevenants à la Loi, la Cnil peut également prendre une sanction dite administrative à l'encontre du responsable du traitement défaillant. Les sanctions de la Cnil peuvent être pécuniaires, jusqu'à 300 000 € en cas de récidive et portent surtout atteinte à l'image du condamné, car ces sanctions sont publiques, donnent lieu à publication, et sont régulièrement reprises par la presse et les médias.

Orange attaqué… et condamné
Une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014 a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés. Dans l'affaire jugée, Orange était alertée en mars 2014 par un client et découvrait que le serveur d'un prestataire de l'opérateur « chargé de réaliser certaines campagnes de marketing direct » par courriel avait été piraté. Plus de 1,3 millions de clients d'Orange étaient impactés par cette attaque. L'enquête révélait qu'Orange avait confié à un premier prestataire la mission de réaliser des campagnes de emailing auprès de ces clients. Ce prestataire avait lui-même sous-traité la prestation à un prestataire secondaire. C'est ce dernier qui était piraté.

Le lien de désinscription, qui se trouvait au bas du courriel de prospection, menait par une modification de l'URL aux 700 fichiers de prospects et de clients d'Orange, permettant à l'indélicat à les aspirer. Le 25 avril 2014, Orange notifiait la faille de sécurité à la Cnil comme elle y est contrainte depuis le Paquet Télécom d'août 2011 et un Règlement 611/2013 de la Commission européenne du 24 juin 2013. Le 5 mai 2014, la presse s'emparait de l'affaire. Une semaine plus tard, la Cnil diligentait sur deux jours un contrôle dans les locaux d'Orange qui révélait les circonstances dans lesquelles les 700 fichiers de clients et prospects avaient été aspirés. Orange déposait une plainte pénale. Mais Orange était également convoquée devant la formation contentieuse dite restreinte de la Cnil, qui lui infligeait un avertissement public le 9 août 2014 pour manquement à l'obligation de sécurité.

Orange se trouvait donc à la fois victime et responsable. Ce qui nous interpelle dans cette décision, ce sont les motifs retenus par la Cnil pour sanctionner Orange. Le premier grief est que selon l'autorité française, Orange « n'a pas fait réaliser d'audit de sécurité sur la version de l'application technique spécifiquement développée par son prestataire secondaire. » Face à la généralité de l'obligation imposée par la Cnil, on cherche désespérément la base légale à ce grief. Mais à supposer celui-ci fondé, on peut penser que le prestataire secondaire a, quant à lui et en sa qualité de professionnel, procédé à cet audit. Tenir Orange, le client dans cette relation, responsable au motif qu'elle n'a pas procédé à cet audit devrait glacer le sang de tous les clients utilisateurs. Le second motif nous paraît, quant à lui, lunaire. La Cnil reproche à Orange d'avoir « communiqué de manière non sécurisé les mises à jour de ses clients » à ses prestataires. L'enquête avait certes révélé qu'Orange avait transmis les 700 fichiers de ses clients et prospects par simple courriel, mais la même enquête a établi que ce n'est pas durant cette communication que les fichiers ont été captés. Cette communication ne serait donc pas en cause. Enfin, la Cnil reproche à Orange « qu'aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire secondaire »,c'est-à-dire au sous-traitant du sous-traitant d'Orange, c'est-à-dire la société avec laquelle elle n'a pas de contrat … C'est compte tenu de ces « défaillances » que la Cnil entre en voie de condamnation à l'encontre d'Orange.

Cette décision nous amène à deux commentaires sous formes de conclusions.
D'une part, il y a un auteur à cette infraction, « quelque part dans le monde » qui a accédé illicitement aux serveurs et a procédé à l'aspiration des fichiers. Les adresses IP relevées par les serveurs du prestataire attaqué ont désigné des pays lointains. Dans ce genre d'affaires, l'enquête judiciaire est souvent en panne. L'enquête bute en effet sur des difficultés de coopérations policières et judiciaires en termes de délais, de paperasserie et de coûts quasi insurmontables, sans compter que certains pays ne coopèrent tout simplement pas. Dans ce contexte, le seul condamné de l'histoire a toutes les chances d'être la victime, Orange. Il y a tout de même ici quelque chose de choquant sur le fond. En outre, c'est Orange qui a notifié elle-même la faille à la Cnil par application de la Loi certes. Si chaque notification donne lieu à condamnation de son auteur, ceux-ci risquent désormais de réfléchir à deux fois avant de se lancer dans ce qui apparaît comme « la gueule du loup ».

D'autre part, les griefs retenus à l'encontre d'Orange nous paraissent d'une interprétation des plus sévères des précautions utiles de l'article 34 de la Loi de 1978 et surtout très généraux, laissant dans le désarroi et l'insécurité juridique tous utilisateurs des systèmes d'information et de leurs services. Enfin, faire tenir Orange responsable des agissements du sous-traitant de son sous-traitant paraît déraisonnable.

En conclusion, on a le sentiment ici que le cri des victimes et des médias a couvert tout raisonnement juridique. Il fallait un responsable. L'auteur de l'infraction introuvable, c'est sur la victime qu'on se rabat. C'est un mode de fonctionnement regrettable sur le plan des principes et qui ne devrait pas se généraliser.

A défaut, oui, la cybersécurité deviendrait synonyme d'obligation de résultat.

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

Source : http://www.solutions-logiciels.com/actualites.php?titre=La-cybersecurite-a-t-elle-une-obligation-de-resultat-&actu=15232
par Juliette Paoli

Plaidoyer pour une législation spécifique à la cybercriminalité

Plaidoyer pour une législation spécifique à la cybercriminalité

Ordre des avocats au barreau de Tizi Ouzou : Les intervenants ont relevé l'insuffisance des moyens de lutte contre ce phénomène. Ils plaident pour une législation plus significative.

La Cellule de lutte contre le cyber-crime relevant de la Sureté de wilaya de Tizi Ouzou a enregistré 23 infractions en cybercriminalité en 2014, contre 12 en 2013. Ce phénomène est nouveau en Algérie. Les moyens de lutte en termes de législation et des structures existantes s'avèrent «insuffisants», indique-t-on. C'est ce qui ressort d'une journée d'étude sur «la cybercriminalité», organisée par l'Ordre des avocats au barreau de Tizi Ouzou, samedi dernier, au Centre des œuvres sociales. Présenté comme la forme de crime du 21e siècle, ce phénomène s'opère à l'aide des outils des technologies de l'information et de la communication (TIC). Il reste de l'avis des intervenants à cette rencontre «un véritable défi», car les auteurs des infractions susceptibles d'être menées ne sont pas facilement identifiables avec la procédure judiciaire classique actuelle.

Pour ce faire, il faudra «constituer des organes de lutte contre la cybercriminalité. L'Algérie est en retard par rapport à cette question. Il n y a que la gendarmerie et la sûreté nationales qui sont chargées de contrer ce phénomène», soutient Chellat Smaïn, bâtonnier à Tizi Ouzou, en parlant des «aspects juridiques de la cybercriminalité». Et de préconiser : «Il serait intéressant aux législateurs de créer une commission à laquelle on donnera la latitude d'agir, et tous les éléments à même de prévenir ce genre de crimes et d'assister la sureté judiciaire dans l'échange et la coordination des informations», ajoutera l'orateur en donnant l'exemple de structures existantes aux USA (Interpol) et en Europe (Europol). Il n'est pas toujours facile de surveiller, d'identifier où de réunir des preuves nécessaires incriminant le mis en cause, compte tenu, explique le bâtonnier, de l'ampleur du réseau informatique, de l'absence de traces, de la rapidité d'exécution du délit …etc.
S'agissant des attaques, l'atteinte à la vie privée semble la plus répandue. En effet, depuis l'avènement des TIC, les moyens d'attaque informatique sont développés et ont amplifié le phénomène pour devenir transnational. «Où que tu sois, tu peux faire l'objet d'une atteinte à ta vie privée au niveau de n'importe quel point du globe», explique quant à lui, Naït Ali Amrane, avocat et enseignant à la Faculté de droit de Tizi Ouzou, dans sa communication sur : «L'atteinte à la vie privée dans le cadre de la cybercriminalité», en citant des intrusions pour vol des informations personnelles à partir de divers supports de stockage de données.
Aussi, explique-t-il, des informations d'un compte rendu médical ou d'une carte d'assurance sociale peuvent être soustraites illégalement à une personne. Abordant à son tour la question de la lutte contre le phénomène, l'orateur a indiqué qu'à défaut de moyens suffisants, «les adolescents et les enfants doivent être sensibilisés pour prévenir contre ces attaques, car nous ne sommes pas encore prêts pour contrer ce genre de délits», a-t-il ajouté. Cet avis n'est pas partagé par les représentants de la gendarmerie et de la sûreté nationales, puisque dans leurs communications, ils ont abordé l'expérience des services de sécurité dans la lutte contre le cyber crime.

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

Source : http://www.elwatan.com/regions/kabylie/tiziouzou/plaidoyer-pour-une-legislation-specifique-a-la-cybercriminalite-22-12-2014-282428_144.php

---

Accord des CNIL européennes: la protection des données personnelles devient « un droit fondamental »

Accord des CNIL européennes: la protection des données personnelles devient « un droit fondamental » | FrenchWeb.fr

«La protection des données à caractère personnel est un droit fondamental» : C'est ainsi que débute la «Déclaration commune des autorités européennes de protection des données» officialisée lundi 8 décembre par les CNIL européennes. Le texte, adopté depuis le 25 novembre 2014, est une forme de réponse à la défiance des citoyens face à la captation et à l'exploitation de leurs données personnelles. Un sujet de société qui a connu un fort regain d'intérêt depuis les révélations d'Edward Snowden.

«Les données à caractère personnel constituent la particule élémentaire de [du] monde numérique» soulignent les autorités européennes. «Le fonctionnement de l'environnement numérique repose sur des infrastructures informationnelles complexes que des acteurs privés ont développées pour leurs besoins propres. Ceux-ci amassent des quantités gigantesques de données personnelles que certains d'entre eux stockent, traitent et partagent souvent sans laisser à l'individu un niveau de contrôle suffisant et sans être soumis à une supervision effective. Par ailleurs, comme les révélations d'Edward Snowden l'ont récemment dévoilé, des autorités publiques et des services de renseignement ont exigé d'avoir un accès massif à ces infrastructures de données pour d'autres finalités, notamment celle de sécurité nationale.
C'est ainsi que les CNIL justifient cette Déclaration commune: «Le caractère massif et routinier de cet accès a choqué le monde entier. Désormais, le défi consiste à remédier à la crise de confiance que ces révélations ont générée envers les gouvernements (nationaux et étrangers) et les services de renseignement et de surveillance. Il s'agit également de régler la question sous-jacente du contrôle de l'accès à ces quantités gigantesques de données personnelles. Comment construire un cadre qui permette à la fois aux entreprises privées et aux organisations d'innover, d'offrir des produits et services qui répondent aux demandes des consommateurs et aux besoins publics, aux services de surveillance et de renseignement de remplir leurs missions dans le cadre de la loi, et de ne pas sombrer pour autant dans une société de surveillance».
Voici les 15 points clés de la Déclaration:

La protection des données à caractère personnel est un droit fondamental
Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux

La technologie est un moyen qui doit demeurer au service de l'homme.
La confiance du public dans les produits et services de l'économie numérique dépend en grande partie du respect des règles de protection des données par l'industrie.

La prise de conscience et les droits des personnes doivent être renforcés. [Surveillance à des fins de sécurité]
La surveillance secrète, massive et indiscriminée de personnes en Europe, (…) n'est pas conforme aux Traités et législation européens.

L'accès à des données à caractère personnel aux fins de sécurité n'est pas acceptable dans une société démocratique dès lors qu'il est massif et sans condition.
Le traitement de données personnelles dans le cadre d'activités de surveillance ne peut avoir lieu que dans le cadre de garanties appropriées définies par la loi.

L'autorité publique d'un Etat non membre de l'Union ne peut par principeaccéder directement à des données personnelles couvertes par les règles européennes
Aucune des dispositions figurant dans les instruments européens visant à encadrer les transferts internationaux de données entre parties privées ne peut servir de base légale à des transferts de données vers les autorités de pays tiers pour des finalités de surveillance massive et indiscriminée

Le stockage des données sur le territoire de l'Union est un moyen effectif de faciliter l'exercice de [leur] contrôle.
Les règles de protection des données de l'Union (…) doivent être considérées comme des principes internationaux impératifs en droit international public et privé.

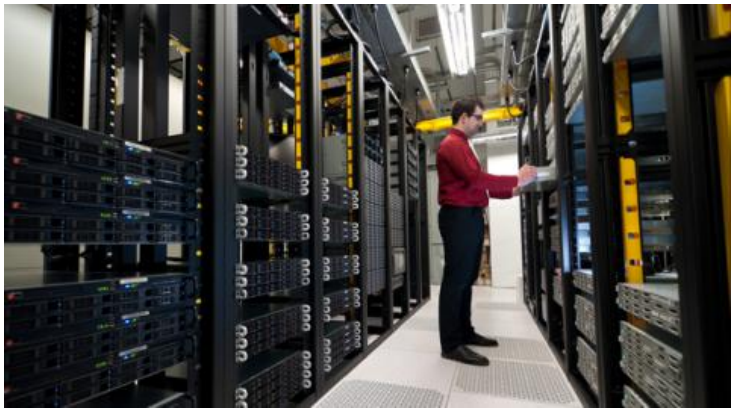
Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015.
Le niveau européen de protection des données ne peut être érodé, en tout ou partie, par des accords bilatéraux ou internationaux, y compris des accords commerciaux sur les biens et services à conclure avec des pays tiers.

L'équilibre à établir entre protection des données, innovation et surveillance n'implique ni de reconstruire les frontières internes de l'Union ni de fermer les portes de l'Europe
Cette Déclaration devrait s'appliquer aux Etats ainsi qu'aux entreprises. Mais n'a pour l'instant aucune application directe au niveau du droit.

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

Source : http://frenchweb.fr/accord-des-cnil-europeennes-la-protection-des-donnees-personnelles-devient-un-droit-fondamental/176535

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.

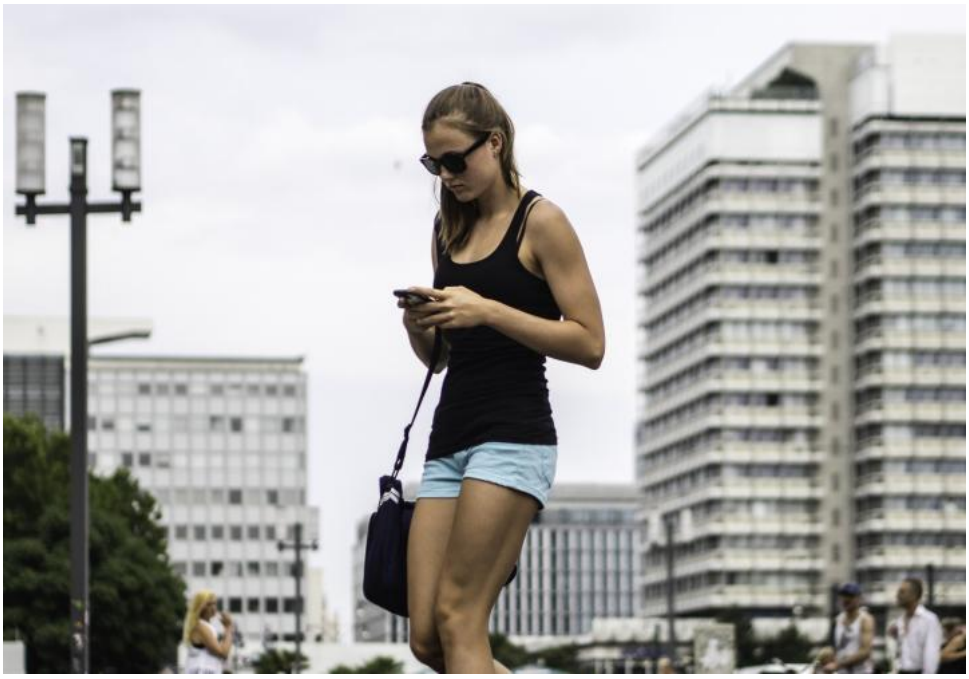
*Le rapport d'étude intitulé "Données : actifs protégés ou bombe à retardement ?" se fonde sur des entretiens menés en octobre 2014 auprès de 2 276 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne.

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

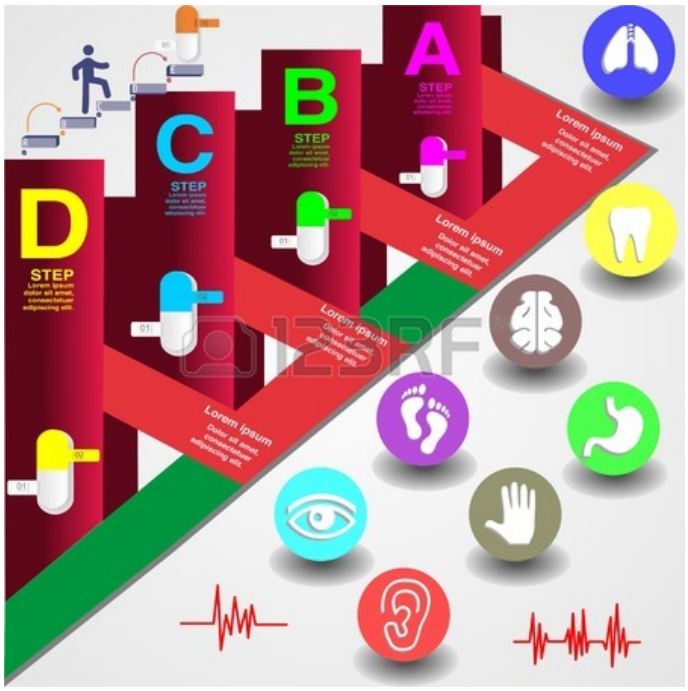
Une nouvelle étude de la Cnil publiée ce lundi souligne que deux tiers des applications pour smartphones collectent des informations personnelles auxquelles elles ne devraient pas avoir accès et sans que les utilisateurs en aient conscience. L'étude démontre que nos téléphones sont devenus de vrais petits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