Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Abidjan – Le ministre de la Poste et des Technologies de l'information et de la communication, Bruno Nabagné Koné, appelle au développement d' »une culture nationale » autour de la question de la sécurisation des réseaux et services numériques qui, estime-t-il, est essentielle pour lutter efficacement contre la cybercriminalité en Côte d'Ivoire.

Pour le ministre Nabagné Koné qui procédait lundi à l'ouverture d'un séminaire sur la cyber-sécurité organisé par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI) autour du thème principal « Développement d'une stratégie nationale en matière de cyber sécurité », il s'agit notamment d'élever la question au rang de celles relevant de la sécurité nationale.
Le séminaire qui s'étendra sur deux jours se veut, selon le DG de l'ARTCI, Bilé Diéméléou, une lucarne d'échanges et de partage d'expériences afin de présenter les actions entreprises par sa structure dans l'accomplissement de sa mission visant à développer la cyber-sécurité.
La rencontre sera également l'occasion d'établir les bases du développement d'un partenariat public/privé fort en matière de cyber-sécurité avec la centaine de structures conviées, a-t-il ajouté.
Le ministre Nabagné Koné déplorait, à l'occasion, le fait que le traitement de la question de la sécurisation des réseaux et services numériques, « considérée comme la 5ème roue du carrosse dont on peut se passer », n'a pas toujours suivi le niveau d'évolution enregistré ces dernières années en Côte d'Ivoire en matière de TIC et même dans le monde.
C'est pourquoi, il appelle à une culture nationale en la matière et qui, selon lui, permettra de faire du souci de la sécurisation du cyber espace ivoirien une question de sécurité nationale.
Le ministre des TIC rappelait auparavant le danger que laisse planer la cybercriminalité sur le développement global de la Côte d'Ivoire, un phénomène qui, a-t-il reprécisé, va au-delà de la perception commune l'assimilant abusivement aux petites escroqueries commises au moyen des outils de moderne de communication.
La cybercriminalité est plutôt le fait pour une personne de s'introduire de façon malveillante dans des systèmes d'information, a-t-il fait comprendre, relevant que c'est cet aspect des choses qui rend le phénomène si préoccupant.
« Que des personnes entrent dans nos systèmes, c'est de cela que nous avons peur et c'est face à cela que nous devons prendre des mesures », a fait remarquer M. Nabagné Koné.
Il a notamment relevé le fait que le phénomène, s'il n'est pas efficacement combattu, pourrait consacrer un recul de l'usage des TICS qui partirait d'une méfiance légitime des populations vis-à-vis des solutions offertes.
« Sans confiance, la réaction des utilisateurs sera le rejet et c'est notre société qui recule », a laissé entendre le ministre.
« Les personnes malveillantes dans le cyberespace ou en ligne sont nombreuses, organisées et leurs motivations sont très diverses: politiques, criminelles, terroristes ou activistes. La cyber-sécurité doit faire partie intégrante du progrès technologique », a-t-il, pour ce faire, appelé.

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

Source : http://news.abidjan.net/h/526302.html

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

Le système de suivi numérique des passagers aériens prêt en fin d’année

Seul, le Royaume-Uni a déjà commencé à alimenter une base PNR. (Crédit D.R.)

Le système de suivi numérique des passagers aériens prêt en fin d’année

Malgré les incertitudes sur le respect de la vie privée et les doutes sur son utilité, le projet de suivi des passagers qui entrent ou sortent de l'Union européenne à travers une série de bases de données nationales devrait devenir réalité d'ici la fin de l'année. Au Parlement européen, seuls les Verts s'y opposent encore.

Depuis les récentes attaques terroristes à Paris et Copenhague au cours desquelles 19 personnes ont été tuées, la volonté de créer des bases de données nationales ayant accès aux données des dossiers passagers (ou PNR pour Passenger Name Record) s'est encore accentuée.
Les pays de l'Union européenne ont fait valoir que le stockage de données pour suivre les déplacements des personnes, permettrait de mieux appliquer la loi en matière de prévention, de détection, d'investigation et de poursuite des infractions terroristes et de la criminalité transnationale.
Selon les termes du projet, les compagnies aériennes devront envoyer les données PNR qu'elles recueillent lors des procédures de réservation et d'enregistrement d'un vol par un passager, y compris son itinéraire de voyage, les informations sur le billet et ses détails de contact, à une autorité du pays concerné. Cette autorité sera chargée d'analyser les données et de partager ses résultats avec d'autres autorités compétentes, en Europe et dans d'autres pays. Si certains pays comme le Royaume-Uni disposent déjà d'une base de données PNR, ce n'est pas le cas pour d'autres. Et il n'existe actuellement aucun système pour partager cette information. Jeudi dernier, lors d'une réunion informelle sur le terrorisme, les chefs d'État et de gouvernement européens ont convenu de poursuivre les discussions pour doter l'UE d'un tel système. « Nous avons défini de nouvelles priorités en matière de lutte contre le terrorisme. En premier lieu, nous devons trouver un accord sur l'échange des informations sur les passagers dans l'Union européenne. Et nous en avons besoin rapidement », a déclaré dans un communiqué le président du Conseil européen, Donald Tusk. Les chefs d'État ont demandé aux législateurs de l'UE d'adopter d'urgence une directive PNR européenne forte et efficace avec de solides garanties pour la protection des données.

Le Parlement européen prêt à finaliser le projet PNR
Dans le cas présent, la protection des données est une question clef. En 2013, un précédent projet d'échange de données sur les passagers entre pays de l'UE avait été rejeté par le Parlement européen, au motif que ces dispositions pouvaient empiéter sur les droits fondamentaux. Mais depuis les derniers attentats, la Commission européenne a modifié le projet pour convaincre le Parlement d'aller de l'avant, promettant une meilleure protection de la vie privée. Et cela semble avoir porté ses fruits. Mercredi dernier, avant la réunion du Conseil, le Parlement avait adopté une résolution par laquelle il s'engageait à travailler « à la finalisation d'une directive PNR de l'UE d'ici la fin de l'année ». Le Parlement veut s'assurer que la collecte et le partage des données seront conformes à un cadre cohérent en terme de protection des données et qu'il comportera des obligations de protection des données personnelles juridiquement contraignantes au sein de l'UE.

Les opposants au projet d'accès aux données des dossiers passagers avaient contesté sa légalité, car dans son objectif, les questions posées sont similaires à celle d'une directive européenne invalidée par la Cour de justice européenne (CJUE). En effet, la Cour de justice avait invalidé une directive sur la conservation des données, ou Data Retention Directive, qui demandait aux opérateurs de télécommunication de conserver les informations sur la destination et la durée des communications, au motif qu'elle portait atteinte à des droits fondamentaux à la vie privée. L'utilité d'un système PNR a également été remise en question par les opposants, lesquels affirment qu'un tel système n'aurait pas empêché les attentats de Paris. « En plaidant pour une directive européenne PNR, le Parlement veut pousser l'UE vers une plus grande centralisation des données et plus de rétention de données, sans motif établi, et en ignorant la jurisprudence de la CJUE », a déclaré mercredi dernier dans un blog Alexander Sander, le directeur général du groupe de défense des droits digitaux allemand Digitale Gesellschaft.

Les Verts font toujours bande à part
Au sein du Parlement, seul le parti des Verts s'oppose encore à un système PNR au niveau européen. Plutôt que d'investir 500 millions d'euros dans la surveillance des passagers aériens, les Verts demandent que cet argent soit dépensé pour le travail de terrain et la coopération entre la police et les autorités de sécurité. Mais sa représentation sera insuffisante pour faire pencher la balance. Dans le même temps, les chefs d'État de l'UE ont estimé que la loi devait renforcer le partage d'informations et la coopération opérationnelle, et que la coopération des services de sécurité entre les pays membres devait également être accentuée. Par ailleurs, ils ont convenu que les autorités devaient intensifier leur action de traçage des flux financiers et geler les actifs utilisés pour financer le terrorisme. La détection et la suppression des contenus Internet faisant l'apologie du terrorisme, en coopération avec des entreprises Internet, est également une priorité pour les États membres. En avril, date à laquelle la Commission présentera ses plans sur la sécurité, le projet devrait franchir une nouvelle étape. C'est au mois de juin que le Conseil devrait exposer en détail comment seront mises en oeuvre les mesures proposées.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-ue-le-systeme-de-suivi-des-passagers-aeriens-pret-en-fin-d-annee-60253.html
Par Jean Elyan

Piratage Anthem : voici venu le temps du phishing

	Piratage Anthem : voici venu le temps du phishing

Victime d'une importante cyber-attaque, l'assureur américain Anthem invite ses clients à ignorer les e-mails qui leur seraient envoyés en son nom.

Victime d'une attaque informatique qui a potentiellement exposé les données personnelles de 80 millions d'individus, Anthem est passé en mode gestion de crise.
La compagnie américaine d'assurances santé mène actuellement l'enquête avec les autorités sur place. Elle a également sollicité la firme Mandiant (filiale de FireEye) pour pratiquer un audit de son système d'information et adopter les solutions de protection ad hoc.
Depuis le lancement de l'alerte mercredi dernier, de nouveaux éléments ont été révélés… sans qu'Anthem en soit systématiquement à l'origine. On a ainsi appris, d'une source dite « proche du dossier » par la presse américaine, que les données subtilisées par les pirates n'étaient pas chiffrées.
Sur la liste figurent, selon les déclarations officielles de l'assureur, des noms, des dates de naissance, des numéros de téléphone et de Sécurité sociale, des adresses postales et électroniques, ainsi que des éléments relatifs à l'activité salariée de clients, comme leur niveau de revenus.
Il n'existe toujours pas de preuves que des informations bancaires et médicales aient été dérobées. Mais celles-ci pourraient l'être d'une façon détournée ; en l'occurrence, par des campagnes de hameçonnage (phishing). Les clients d'Anthem commencent effectivement à recevoir des e-mails d'apparence légitime qui les invitent à cliquer sur un lien pour bénéficier d'un suivi de leurs encours de crédit.
Problème : si l'entreprise a bel et bien annoncé son intention de fournir gratuitement ce service à toutes les victimes collatérales de la cyber-attaque, elle n'a pas encore adressé de communication officielle. Bilan : les e-mails reçus ces derniers jours ne sont qu'un scam visant à récupérer de précieuses données auprès des utilisateurs insuffisamment vigilants.
Voilà Anthem contraint d'user de pédagogie. La société cotée en Bourse – sur le NYSE – a ouvert une rubrique dédiée dans la foire aux questions du site AnthemFacts, créé pour centraliser les dernières nouvelles relatives à la cyber-attaque. Elle enjoint ses clients à ne cliquer sur aucun lien, à ne pas ouvrir les éventuelles pièces jointes, à ne renseigner aucune information sur le site Web qui s'ouvrirait éventuellement et à ne pas répondre au mail.
Pour l'heure, il reste difficile de déterminer s'il s'agit d'une campagne de phishing ciblée ou si ces envois de mails sont l'œuvre de pirates qui ont visé large en espérant toucher des souscripteurs aux assurances santé d'Anthem. Ce qui laisse supposer que les données volées sont bel et bien activement exploitées, ce sont plutôt ces appels téléphoniques invitant les clients à fournir leur numéro de carte bancaire et/ou de Sécurité sociale.
Le bilan pourrait être lourd : près de 40 millions de clients revendiqués à fin 2014… et autant d'anciens souscripteurs. Une affaire d'une telle envergure que le Département des services financiers de New York envisage aujourd'hui un audit global de toutes les compagnies d'assurance. L'agence fédérale compte intégrer ces contrôles « réguliers et ciblés » dans sa feuille de route. Elle projette aussi de durcir les obligations auxquelles les institutions sont soumises en matière de sécurité informatique.

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

Source : http://www.itespresso.fr/piratage-anthem-temps-phishing-88038.html
Pat Clément BOHIC

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Des pirates se sont infiltrés dans les systèmes d'information d'une centaine de banques en 2013, ont dérobé au moins 300 millions de dollars, et agissent encore aujourd'hui, apprend Kaspersky.

C'est l'une des cyberattaques les plus sophistiquées jamais identifiées par Kaspersky. L'éditeur de solutions antivirus russe a dévoilé auprès du New York Times, lundi, les résultats d'une enquête menée depuis 2013 en partenariat avec Interpol et Europol. Conclusions : de 300 millions à 1 milliard de dollars ont été dérobés à une centaine de banques dans trente pays. Active depuis près de deux ans, la cyberattaque a toujours cours.

Pour ces raisons, l'éditeur reste volontairement imprécis sur les informations divulguées, ne fournissant pas, par exemple, le nom des établissements concernés. Les institutions sont basées principalement en Russie, au Japon, aux Etats-Unis et en Suisse. D'après le quotidien américain, JP Morgan Chase figure parmi les cibles.
Ce cybergang basé en Russie, Chine et Ukraine, « a franchi un nouveau cap » dans la méthode employée, souligne Kaspersky, en dérobant des fonds aux banques sans avoir à passer par les clients. L'attaque aurait débuté avec des infections classiques par hameçonnage, quand des employés de banque téléchargeaient malgré eux sur leur poste le malware nommé « Carbanak » – c'est également le nom de ce groupe de pirates.

Observer et imiter les transferts d'argent

Une fois bien installés sur les ordinateurs chargés des transferts de fonds ou de la compatibilité, il peuvent observer discrètement et patiemment les routines des employés et les processus des banques. Les pirates remontent ensuite sur les machines des responsables des transferts et des comptes, où ils installent un outil d'administration à distance (RAT) afin d'en prendre le contrôle et « d'imiter les activités normales ».
Ainsi, les assaillants peuvent créer de faux comptes pour y transférer de l'argent, a priori sans éveiller de soupçons. Si le hameçonnage n'a rien d'exceptionnel en soi, c'est l'aspect méthodique et la patience des pirates que Kaspersky pointe du doigt dans son rapport. De quoi leur avoir évité de s'être fait pincer à ce jour.
Ce qui a déclenché l'enquête remonte à la fin 2013 lorsqu'un distributeur s'est mis à émettre des billets en plein Kiev, en Ukraine. Alertée, la banque concernée a alors missionné Kaspersky. Lequel découvrira assez tôt que cette avarie allait en fait devenir, comparé à l'ampleur de la cyberattaque, le dernier souci de la banque.

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

S o u r c e :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-754433-kaspersky-cyber-attaque-banques.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_17/02/2015&partner=-&svc_position=86524329@&svc_misc=-&crmID=639453874_86524329@&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-754433-kaspersky-cyber-attaque-banques.html

Vous allez pouvoir décider du sort de votre Facebook après

votre mort

Vous allez pouvoir décider du sort de votre Facebook après votre mort

Le réseau social va vous permettre de nommer un légataire pour qu'il puisse gérer votre page après votre décès. Il aura accès à presque tout sauf aux messages privés.

Facebook pense à tout, même à votre vie après la mort. Le plus gros réseau social du monde a déployé jeudi une mise à jour qui permet de désigner un « légataire », permettant de prendre le contrôle du profil du défunt et même de publier des messages en son nom.
« Facebook est un endroit pour partager et se rapprocher de sa famille et de ses amis. Et, pour plusieurs d'entre nous, il s'agit d'un endroit pour se souvenir et rendre à hommage à ceux qui nous ont quittés », a annoncé le réseau social sur son blog (en anglais).

Aucun accès aux messages privés
Auparavant, Facebook créait une page commémorative lorsqu'elle était informée du décès d'un membre, mais celle-ci ne pouvait être gérée par une tierce personne. Mais « après avoir parlé avec des gens qui ont vécu la perte d'un proche, nous avons réalisé que nous pouvions en faire davantage pour les personnes endeuillées et pour ceux qui veulent garder le contrôle sur leur compte après leur mort ».
Pour les utilisateurs qui le désirent, le « légataire » pourra publier un message afin d'annoncer un service funéraire ou partager un message spécial. La personne qui gère le compte pourra aussi mettre le profil à jour et changer la photo de couverture, ainsi que répondre aux demandes d'amitié de membres de la famille et d'amis qui n'étaient pas encore connectés.

Problème de stockages de données personnelles
En désignant un légataire, le membre pourra aussi donner la permission de télécharger les photos, ainsi que l'information du profil partagés sur Facebook. Cependant, « le légataire ne pourra se connecter directement au compte du défunt ou voir ses messages privés. »
L'annonce survient au moment où l'inquiétude croît quant au sort des « avoirs numériques » après la mort. Des experts légaux indiquent que la propriété des données stockées dans le « cloud » (dans les serveurs de Facebook), les courriels et les archives en ligne de musique et de livres demeurent sujets à interprétation. Par ailleurs, des utilisateurs remontent régulièrement à quel point les pages de proches décédés peuvent être une source de tristesse quand elles restent en ligne après leur mort.

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

S o u r c e :
http://lexpansion.lexpress.fr/high-tech/facebook-pense-a-votre-vie-apres-la-mort_1651127.html?PMSRC_CAMPAIGN=20150217130355_08_nl_lexpansion_high_tech_11437&xtor=EPR-3125-%5B20150217130355_08_nl_lexpansion_high_tech_11437_000YKDN5D-20150217-%5B_____Vous_allez_pouvoir_decider_du_sort_de_votre_Facebook_apres_votre_mort_____002TCI1%5D-20150217120800#LBdEJLMBMIkXokbR.99

L’Odre des Médecins souhaite un remboursement des objets connectés

L’Odre des Médecins souhaite un remboursement des objets connectés

À l'occasion d'un débat et de la publication d'un livre blanc, le Conseil National de l'Ordre des Médecins préconise d'encadrer les objets connectés liés à la santé par une réglementation européenne.

"Bonjour, il me faudrait une boîte de pastilles pour la gorge et un bracelet connecté s'il vous plaît". Et si bientôt, entendre cette phrase dans une pharmacie devenait banal ? Les objets connectés liés à la santé sont de plus en plus nombreux : mesure du rythme cardiaque, des phases du sommeil, sans compter les applications associées où l'on rentre des données relatives à nos habitudes alimentaires ou autres. Partant de ce constat, le CNOM (Conseil National de l'Ordre des Médecins) a débattu sur la question, avant de publier un livre blanc détaillant six recommandations.

Parmi elles, on note le souhait d'encadrer les objets connectés par une réglementation européenne : "Afin que la mise sur le marché des outils de m-santé [santé mobile, ndlr] comporte des garanties, le CNOM estime qu'ils devraient faire l'objet d'une déclaration de conformité à un certain nombre de standards. Cette déclaration devrait comporter 3 volets : la confidentialité et la protection des données recueillies, la sécurité informatique, logicielle et matérielle, la sûreté sanitaire".
Il paraît en effet logique que, tout comme ce qu'il se dit lors d'une consultation médicale, les données sanitaires recueillies par des objets connectés et/où des applications restent confidentielles.

Le CNOM estime aussi que ces outils devraient faire l'objet d'une évaluation scientifique systématique, par des experts indépendants. Si l'on devait arriver à la conclusion que l'objet connecté/l'application est bénéfique pour la santé individuelle/collective, "il serait cohérent d'envisager qu'ils soient pris en charge par la collectivité". Autrement dit : l'achat d'un objet connecté ou d'une application pourrait faire l'objet d'un remboursement au même titre que certains médicaments.

Quand on sait que 3 millions d'objets connectés se sont vendus en France en 2013 (étude GFK) et que 11 % des détenteurs déclarent les utiliser dans le contexte de la santé / du bien-être, on comprend la nécessité d'établir une réglementation. Dans les faits, celle-ci risque d'être difficile à mettre en œuvre, surtout au niveau de la confidentialité des données recueillies : pour la grande majorité des applications, le modèle économique repose justement sur la vente des données à diverses entreprises. Il s'agirait alors pour les développeurs d'applis estampillées "santé" de repenser totalement leur stratégie financière.

Et avant même d'envisager une réglementation, le livre blanc du CNOM rappelle qu'il est encore difficile d'évaluer le véritable impact (positif ou négatif) des objets connectés/applications liés à la santé. Selon l'OMS, sur 114 pays interrogés en 2011, seuls 12 % se sont penchés sur cette question.

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

Source : http://www.android-mt.com/news/lodre-medecins-souhaite-remboursement-objets-connectes-35850

Cybercrime : la fraude à un milliard de dollars

Cybercrime : la fraude à un milliard de dollars

La fraude est inédite par son ampleur : une centaine d'établissements financiers et de banques ont été victimes d'une cyberattaque encore jamais vue.(c) Shutterstock/EconomieMatin

La société de sécurité informatique Kaspersky Labs a mis au jour le pot aux roses, qui touche une trentaine de pays parmi lesquels la Russie, les États-Unis, l'Allemagne, la Chine, l'Ukraine ou encore le Canada. En tout et pour tout, c'est un milliard de dollars qui s'est évaporée des comptes de ces banques !

Interpol, sur le coup, reçoit l'aide des fins limiers de Kaspersky pour débusquer les pirates qui ont mis la main sur ce pactole. Il s'agirait, d'après les premiers renseignements, d'un groupe de hackers provenant de l'est de l'Europe (Russie et Ukraine), ainsi que de Chine.

Les méthodes employés, rapporte Interpol, marquent un tournant pour ce type d'infraction. Le processus mis en œuvre par les pirates relèvent d'une grande sophistication, qui leur permet de subtiliser l'argent « directement dans les banques », mais « sans avoir à viser ceux qui, au final, vont utiliser cet argent ».

Des méthodes redoutables donc, et transparentes, qui exploitent de nouvelles failles de sécurité et autres brèches dans les systèmes utilisés par les établissements bancaires. Et l'attaque se poursuit à l'heure actuelle.

Lire la suite….

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

Source : http://www.journaldeleconomie.fr/Cybercrime-la-fraude-a-un-milliard-de-dollars_a1994.html

« Cloud computing » et marchés publics : garantir la confidentialité

« Cloud computing » et marchés publics : garantir la confidentialité

L'« informatique en nuage » ou « cloud computing » permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe, et aux services publics de gagner en efficacité. Son utilisation pose cependant des questions sur la sécurité et sur la gestion des données transmises et stockées dans le cloud, qui est l'origine des normes mises en place depuis trois ans, fort utiles aux acheteurs publics.

Une analyse juridique de Nicolas Nahmias et Emmanuelle Bénoit, avocats à la cour, cabinet AdDen avocats

Le « cloud computing » ou « informatique en nuage » désigne le stockage de données (telles que des fichiers de texte, des images et des vidéos) et de logiciels, auxquels les utilisateurs accèdent par internet en utilisant l'appareil de leur choix.

Selon la Commission nationale de l'informatique et des libertés (Cnil), il s'agit de la forme la plus évoluée d'externalisation, dans laquelle le client ou l'utilisateur dispose d'un service en ligne dont l'administration et la gestion opérationnelle sont effectuées par un sous-traitant (entendu comme celui qui traite les informations personnelles pour le compte du responsable de traitement, selon ses instructions). Ce type de services permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe (il suffit de disposer d'un ordinateur, d'une tablette ou d'un smartphone connecté à internet) et aux services publics de gagner en efficacité.

Le recours au cloud pose néanmoins d'assez nombreuses questions auxquelles les personnes publiques doivent impérativement être attentives : la sécurité des données transmises et stockées dans le cloud est-elle assurée ? Le choix du modèle économique de certains prestataires est-il compatible avec le fait que les personnes publiques gèrent des données sensibles, personnelles et d'intérêt général ? Ces problématiques et d'autres sont à l'origine d'une nouvelle norme qui peut s'avérer fort utile aux acheteurs publics.

I. La normalisation du cloud computing

Le cadre réglementaire.

La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données constitue aujourd'hui le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Elle met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne (UE) (1). En France, c'est la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui constitue le fondement de la protection des données personnelles. Elle a notamment été modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui a transposé la directive de 1995.

Il existe également plusieurs normes internationales en matière de sécurité de l'information, et notamment la norme certifiante ISO/CEI 27001 Management de la sécurité de l'information et la norme ISO/CEI 27002 Technologies de l'information/Techniques de sécurité/Code de bonne pratique pour le management de la sécurité de l'information.

Lire la suite….

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

Source : http://www.courrierdesmaires.fr/46179/cloud-computing-et-marches-publics-garantir-la-confidentialite/

Les CNIL en Europe et le G29 : comment ça marche ?

	Les CNIL en Europe et le G29 : comment ça marche ?

L'utilisation de l'Internet pose de nombreux problèmes en termes d'utilisation des données personnelles des usagers du réseau. Pour tenter de gérer au mieux ces notions et éviter les débordements, plusieurs CNIL ont été créées en Europe. Un autre groupe, appelé « G29 », travaille également sur ces sujets. Qu'en est-il exactement, comment ces organismes fonctionnent-ils, quel est leur champ d'action et tout ceci fonctionne-t-il de façon efficace in fine ?…

La France a été un des tous premiers pays à établir une loi homogène et globale de protection des données personnelles et de la vie privée. La fameuse loi « informatique et libertés » a ainsi vu le jour en 1978 dans le prolongement de nombreux travaux et de quelques scandales. Comme souvent en France, une nouvelle loi s'accompagne d'une agence ou d'une commission composée de nombreux représentants, parlementaires et fonctionnaires. Quand l'Europe a accepté de légiférer à son tour sur la question de la protection des données personnelles en 1995, à la demande des pays latins et germains, la création d'équivalents de la CNIL dans chaque pays devenait une évidence. C'est ainsi que sont nées les autorités de protection des données personnelles en Europe.

Les CNIL dans chaque pays

La souveraineté d'un pays se traduit principalement par l'édiction de politiques et de lois propres à un territoire donné. Pourtant, dans le cadre juridique de l'Union européenne, les pays doivent « transposer » des directives qui sont des lignes directrices. Ainsi, dans le cadre de la directive de 1995, tous les pays de l'UE avaient l'obligation de créer des « CNIL » locales.
Dans ce cadre, les pays ont adopté des législations parfois différentes mais ressemblantes : l'Espagne a créé une autorité particulièrement présente et respectée, imposant une interprétation restrictive et très protectrice des données personnelles, pendant que certains pays de l'Est instauraient des autorités souples et peu dotées. Certains, comme le Luxembourg, demandaient l'assistance de la France pour former son personnel, de telle manière qu'aujourd'hui, la CNPD luxembourgeoise ressemble au petit frère de la CNIL. Enfin, un pays fédéral comme l'Allemagne connait un système où les länder ont un pouvoir certain au regard de la loi allemande.
Lire la suite….

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

Source : http://recherche-referencement.abondance.com/2015/02/les-cnil-en-europe-et-le-g29-comment-ca.html