Non, la politique de confidentialité de Facebook n’est pas un progrès

	**Non, la politique de confidentialité de Facebook n’est pas un progrès**

Avec ses nouvelles règles, entrées en vigueur en janvier 2015, Facebook promettait transparence et contrôle pour les utilisateurs. D'après un rapport commandé par la Cnil belge, ce contrôle s'avère en vérité très restreint.

« Vous avez le contrôle ». C'est le message qu'a tenu à faire passer Facebook auprès de ses utilisateurs en introduisant une nouvelle version de sa politique de confidentialité et de ses conditions d'utilisation.
Mais ce contrôle s'avère en vérité à géométrie variable, et même parfois tout bonnement inexistant, en particulier lorsqu'il s'agit pour l'utilisateur de limiter la collecte de ses données à des fins publicitaires. D'après le rapport rendu à l'autorité belge de protection des données personnelles par des chercheurs universitaires, il ne fait pas de doute que Facebook viole le droit européen.

D'anciennes « pratiques rendues plus explicites » et étendues
Cette situation préexistait toutefois à l'entrée en vigueur en janvier 2015 des nouvelles conditions d'utilisation du réseau social. « Pour être clair : les changements introduits en 2015 n'étaient pas tous drastiques. La plupart des 'nouveaux' termes et règles de Facebook sont simplement d'anciennes pratiques rendues plus explicites » souligne le rapport en préambule.
Pas pire qu'avant alors ? Pas si vite. Les juristes estiment en effet que la firme a aussi profité de ce changement pour étendre ses traitements de données. En substance, Facebook combine une grande variété de sources et de types de données, et de plus en plus y compris hors de ses seuls services.
Et si Facebook se montre plus gourmand en données, il a en revanche fait (ou presque) du sur-place sur l'information des utilisateurs et les moyens dont ils disposent pour contrôler ou s'opposer à ces traitements.
« Les usages des données sont encore seulement communiqués de manière générale et abstraite. La majeure partie de la politique d'utilisation des données consiste en des hypothèses et des termes vagues plutôt qu'en des déclarations claires quant à l'utilisation réelle des données » analyse le rapport.
« En outre, les choix qu'offre Facebook à ses utilisateurs sont limités. Pour nombre des utilisations de données, le choix pour les utilisateurs relève simplement du 'à prendre ou à laisser'. S'ils n'acceptent pas, ils ne peuvent plus utiliser Facebook […] » est-il encore précisé.

Choix limités et faux sentiment de contrôle
En vérité, les seules options de contrôle dont les internautes disposent sur le service portent sur l'accès à leurs contenus par les autres utilisateurs. Les auteurs de l'étude relèvent d'ailleurs que les règles par défaut de partage restent problématiques.
Et ainsi cette granularité dans le contrôle de la confidentialité s'estompe dès qu'il s'agit pour Facebook et des partenaires de collecter et exploiter des données. Les utilisateurs ne peuvent alors exercer « un contrôle significatif » sur l'exploitation de leurs données personnelles. Cette situation se traduit chez l'utilisateur par « un faux sentiment de contrôle » tranche le rapport.
D'ailleurs, la définition de l'opt-out appliquée par Facebook à la publicité sociale et comportementale ne respecte pas la législation en matière de recueil effectif du consentement. Dans certains cas, comme le partage des données de localisation, les juristes précisent que les utilisateurs n'ont tout simplement aucun droit d'opposition.
Si cette analyse juridique a été commanditée par la Cnil belge, ce n'est pas un hasard. Celle-ci participe en effet, aux côté des autorités allemande et néerlandaise, à un groupe de travail de l'Article 29 sur la conformité de la politique de confidentialité de Facebook avec le droit européen.
A noter que des représentants de Facebook ont rencontré le ministre belge en charge de la confidentialité afin de discuter des conclusions de ce rapport. La firme assure d'ailleurs respecter les lois du pays en matière de protection des données. Une ligne de défense qui était celle de Google en 2012 après l'entrée en vigueur d'une nouvelle politique de confidentialité.

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

Source : http://www.zdnet.fr/actualites/non-la-politique-de-confidentialite-de-facebook-n-est-pas-un-progres-39815200.htm
Par Christophe Auffray
c

Près d’un tiers des Européens donnent de fausses informations pour protéger leurs données personnelles

Près d’un tiers des Européens donnent de fausses informations pour protéger leurs données personnelles

Une majorité d’européens (57%) s’avoue inquiet quant à la sécurité de leurs informations personnelles, selon le rapport 2015 sur la protection des données privées publié par l’éditeur de solutions antivirus Symantec.

81% des adultes interrogés estiment que leurs données ont de la valeur (équivalentes à moins de 1.000 euros pour 57% d’entre eux), ce qui explique que 66% déclarent qu’ils aimeraient pouvoir mieux les protéger, mais ne savent pas nécessairement comment faire. À l’inverse, ils sont 14% à ne voir aucun inconvénient à ce que les entreprises partagent leurs données avec des tiers.
Ce sont les données bancaires dans lesquelles les sondés ont le plus confiance en la sécurité en ligne (66%), devant celles médicales (60%), loin devant toutes celles relatives aux achats en ligne (15%). En conséquence, ils évitent dans la mesure du possible de poster des informations trop personnelles afin de se protéger (57%) et n’hésitent même plus à communiquer de fausses données pour parer à toute éventualité (31%).
À noter que, dans tous les cas, les données concernant le panel français ne diffèrent guère des résultats globaux européens, puisqu’ils sont par exemple 56% à s’inquiéter pour la sécurité de leurs données personnelles partagées sur Internet. Ils sont en revanche plus nombreux que la moyenne (66%, contre 57% au niveau européen) à refuser de poster systématiquement certaines informations trop personnelles en ligne.
Cette étude a été conduite en ligne par Edelman Berland pour Symantec en décembre 2014, auprès de 7.041 répondants répartis dans sept pays européens (Allemagne, Danemark, Espagne, France, Italie, Pays-Bas et Royaume-Uni) selon la méthode des quotas.

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

Source : http://www.leparisien.fr/high-tech/pres-d-un-tiers-des-europeens-donnent-de-fausses-informations-pour-proteger-leurs-donnees-personnelles-24-02-2015-4555475.php

---

TrueCrypt n’est pas mort,

l’audit bouge encore

TrueCrypt n’est pas mort, l’audit bouge encore

Les développeurs chargés d’auditer la sécurité de TrueCrypt ont donné quelques nouvelles de leur avancement. Le développement du logiciel de chiffrement avait été interrompu brusquement durant l’été 2014, soulevant de nombreuses inquiétudes quant à la fiabilité du programme.

L’affaire TrueCrypt fait partie des mystères de la cybersécurité: en mai, le site web distribuant le logiciel annonçait la fin du développement, ajoutant que TrueCrypt n’était « plus sûr » et que les utilisateurs qui décidaient de s’appuyer dessus s’exposaient « à des failles de sécurité non comblées.»
Une nouvelle version du logiciel était distribuée par la même occasion, fortement déconseillée par la plupart des experts en cybersécurité. Un coup dur : TrueCrypt était l’un des projets considérés comme les plus solide en matière de protection des données et, aux dernières nouvelles, donnait encore du fil à retordre aux analystes de la NSA selon des documents datés de 2012.

Doutes et remises en question
Un audit de TrueCrypt avait néanmoins été initié en 2013, en s’appuyant sur un crowdfunding réalisé auprès de la communauté afin de financer un examen en profondeur du code source du logiciel. Si celui-ci avait été lancé bien avant l’arrêt brutal du développement, ses résultats sont aujourd’hui très attendus par les utilisateurs de TrueCrypt. Mais depuis juin 2014, aucune nouvelle n’avait émané du projet, suscitant les interrogations de la communauté.
Sentant monter l’inquiétude, Matthew Green, le chercheur à l’origine du projet d’audit a posté une mise à jour faisant le point sur l’avancement des travaux du groupe. Et c’est bien la moindre des choses : le financement de cet audit a été réalisé sur une opération de crowdfunding, qui avait rassemblé 70.000 dollars au mois de décembre 2013. Compte tenu de la somme récoltée auprès de donateurs et de l’actualité inquiétante du développement de Truecrypt, l’initiative menée par Matthew Green et Kenn White est surveillée de très près.
L’annonce de l’arrêt du développement a d’ailleurs suscité de nombreuses interrogations au sein du groupe chargé de l’audit du code : « L’annonce de l’abandon du projet par l’équipe de Truecrypt nous a poussé à reconsidérer notre approche. Etait-ce vraiment la bonne manière d’utiliser nos ressources ? Ne devrions-nous pas nous pencher au contraire sur les forks de Truecrypt qui émergeaient alors ? »
Matthew Green explique que le projet d’audit a donc connu une longue période de remise en question, mais que le projet est aujourd’hui à nouveau sur les rails, au travers d’un partenariat avec la société NCC Group North America, qui reprend en charge la poursuite de l’audit. Celui-ci entre dans sa seconde phase, après la publication d’une première partie qui avait noté quelques vulnérabilités mais aucune backdoor sérieuse au sein du code de la dernière version de TrueCrypt jugée fiable, la version 7.1a du logiciel.

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

Source : http://www.zdnet.fr/actualites/chiffrement-truecrypt-n-est-pas-mort-l-audit-bouge-encore-39815118.htm
Par Louis Adam

Lenovo accusé d’infecter ses propres PC. Le protocole sécurisé SSL aurait été atteint

	Lenovo accusé d’infecter ses propres PC. Le protocole sécurisé SSL aurait été atteint

Très mauvaise publicité pour le premier fabricant mondial. Lenovo a été contraint d'admettre qu'il a installé secrètement un logiciel de publicité sur ses ordinateurs, lors de leur fabrication. Problème : ce logiciel aurait un effet pervers en mettant en péril la sécurité du protocole de sécurisation SSL. Face au tollé, Lenovo fait une courbe rentrante.

Lenovo, ce n'est pas n'importe qui. Il s'agit ni plus ni moins du premier fabricant mondial de PC. 60 millions de PC vendus l'an passé tout de même… Le groupe chinois est connu pour avoir racheté il y a quelques années la division PC d'IBM, ce qui lui a permis de faire son entrée dans la cour des grands. Ensuite, il a particulièrement bien tiré son épingle du jeu grâce à du matériel de qualité. Mais là, son image en prend un coup …

Toujours plus gourmand ?
Le logiciel installé secrètement par Lenovo, appelé Superfish, aurait pour but de créer un canal d'affichage de publicités ciblées lors des recherches effectuées sur certains moteurs de recherche. On appelle cela un « Adware ».

Le but ? Probablement faire de la concurrence à des systèmes bien connus comme Adwords, et créer une source de revenus complémentaires pour le fabricant qui pourrait ainsi entrer dans le marché très rentable de la publicité en ligne. Un péché de gourmandise ?
Le groupe ne nie pas mais minimise. Selon lui, il s'agirait d'améliorer « l'expérience utilisateur » selon l'expression consacrée, en permettant d'afficher du contenu publicitaire qui lui convient vraiment. Du marketing ciblé en un mot.

Contre publicité
Jusque-là, les enjeux sont éthiques (les publicitaires diront que les enjeux touchent l'image de l'entreprise), outre bien entendu un problème potentiel au niveau de la protection des données personnelles de l'utilisateur. Il y a tout de même des règles à respecter dans le cas de l'utilisation de données à caractère personnel à des fins de marketing. Il y a aussi des développements potentiels en droit des contrats si l'on considère que le PC livré ne correspond pas à ce qui a été vendu puisqu'un module supplémentaire, secret et indiscret est livré avec.
Il s'agit toutefois d'une contre-publicité remarquable, car plusieurs commentateurs rappellent que Lenovo a déjà été accusé plusieurs fois d'infecter ses PC lors de leur fabrication en modifiant les microprocesseurs afin de créer une porte d'entrée dérobée. Derrière cela, il y aurait le gouvernement chinois et de sombres opérations d'espionnage et/ou de cyber-guerre. Difficile de savoir si ces accusations ont quelque fondement ou s'il s'agit d'un fantasme lié à l'origine chinoise du fabricant, mais la rumeur est solide. Tel le monstre du Loch Ness, la rumeur est réapparue plus forte que jamais ces jours-ci, suite à l'affaire Superfish.

Un risque grave pour la sécurité
L'affaire Superfish se corse car des chercheurs ont révélé un effet pervers majeur du logiciel superfish : il mettrait en péril le protocole de sécurisation SSL.

Le protocole SSL – abréviation de Secure Socket Layer – est une application des outils cryptographiques, largement utilisée pour les paiements électroniques en ligne, bien qu'il n'a pas été créé spécifiquement pour cela. Le système – intégré par défaut à presque tous les logiciels de navigation – crée un canal de communication sécurisé entre le serveur du vendeur et l'ordinateur du client, assurant entre eux la transmission cryptée des informations communiquées (par exemple : le numéro facial de la carte de crédit, la date d'expiration et le nom du titulaire).

Le protocole SSL présente principalement les avantages suivants :
• coût réduit : le protocole est intégré dans les logiciels récents de navigation sur l'internet (MS Internet Explorer, Netscape, Opera, etc.) et ne requiert donc pas d'équipement particulier ;
• simplicité d'utilisation : l'intégration au logiciel de navigation dispense l'acheteur de toute démarche particulière. La présence d'un logo représentant un cadenas fermé sur l'écran du logiciel confirme le recours à une transmission cryptée ;
• authentification du vendeur : le protocole SSL assure avant tout l'authentification du vendeur ce qui permet, dans une certaine mesure, de décourager les escrocs qui se font généralement vite repérer par les sociétés émettrices de cartes de crédit ;
• cryptage : l'utilisation de la cryptographie asymétrique permet de sécuriser les transmissions sur le réseau.

Toute médaille ayant son revers, ces avantages et la simplicité d'utilisation constituent également les principales faiblesses du système :
• il n'y a aucune vérification de l'identité du client ;
• le numéro apparent de la carte est transmis au vendeur, ce qui laisse subsister le risque d'une utilisation frauduleuse par ce dernier, ni ne résout le danger d'une intrusion dans le serveur du vendeur par un tiers désireux de faire main basse sur les informations bancaires des clients ;
• l'efficacité de la protection en cours de transmission dépend essentiellement de la clef de cryptage retenue.
• L'importance de SSL est considérable. S'il fallait l'exprimer en quelques mots, on pourrait dire qu'à l'heure actuelle, ce protocole protège quasiment toutes les transactions sur l'internet. Qu'il s'agisse d'acheter des billets de trains, de réserver un spectacle, de télécharger de la musique payante, de commander un livre … SSL est derrière l'immense majorité des opérations. Presque tous les sites qui opèrent le paiement par la transmission du numéro facial de carte de crédit, utilisent SSL. Ce protocole n'est pourtant pas le seul, mais il est le plus utilisé.

En raison de sa conception (recours à des certificats auto signés, en utilisant de surcroît la même clef privée sur tous les ordinateurs équipés de ce logiciel), le logiciel Superfish peut déchiffrer des connexions supposées sécurisées afin d'insérer des contenus publicitaires sans que l'utilisateur ne soit averti d'une telle intrusion, et briser ainsi la sécurité du protocole (plus d'infos en faisant une recherche sur votre moteur préféré avec les mots-clef « superfish ssl »).

Lenovo fait une courbe rentrante
Face au tollé général, le fabricant chinois a été contrainte de reconnaître les faits en les minimisant, et d'assurer que depuis ce mois de janvier, les nouvelles machines ne sont plus équipées de ce logiciel. (voir le communiqué http://news.lenovo.com/article_display.cfm?article_id=1929)

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

Source : http://www.droit-technologie.org/actuality-1698/lenovo-accuse-d-infecter-ses-propres-pc-le-protocole-de-securise-ssl.html
Par Etienne Wery, Avocat aux barreaux de Bruxelles et Paris (cabinet Ulys)

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

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?PM&RC_CAMPAIGN=20150217130355_08_nl_lexpansion_high_tech_11437&xtor=EPR-3125-%5B20150217130355_08_nl_lexpansion_high_tech_11437_000YKD%5D-20150217-%5B_____Vous_allez_pouvoir_decider_du_sort_de_votre_Facebook_apres_votre_mort_____002TCI1%5D-20150217120800#LBdEJLMBMIVXokbR.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

« 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