Logiciel Espion Superfish installé par Lenovo : son site Internet piraté en représailles

Logiciel Espion Superfish installé par Lenovo : son site Internet piraté en représailles

Le site Internet de Lenovo a été piraté et son trafic redirigé vers un compte Twitter critiquant l'installation par le fabricant de l'adware Superfish. Lenovo enquête sur d'autres effets possibles de cette cyberattaque.

Après le scandale du logiciel publicitaire et à risque installé par défaut sur un grand nombre de ses ordinateurs portables, Lenovo a dû s'expliquer et présenter des excuses. Mais manifestement, le fabricant doit aussi faire face à des représailles du fait de Superfish.
Mercredi 25 février, le site Internet de Lenovo était inaccessible. Cette indisponibilité fait suite à une cyberattaque. Mais avant que l'entreprise ne déconnecte son site et n'informe les visiteurs d'une maintenance en cours, celui-ci affichait un diaporama diffusant des images tirées du service Imgur. Un clic sur les images redirigeait vers un compte Twitter Lizard Squad, critique à l'égard de Lenovo pour la diffusion de l'adware Superfish.

Attaque sur le gestionnaire de domaine
Lenovo a confirmé une faille de sécurité au Wall Street Journal. « Malheureusement, Lenovo a été victime d'une cyber attaque » reconnaît le fabricant de PC. « Un effet de cette attaque a été de rediriger le trafic depuis le site Web de Lenovo. Nous étudions activement d'autres aspects de cette attaque » précise-t-il encore.
Les attaquants avaient semble-t-il pris le contrôle du site du registrar du domaine utilisé par Lenovo et pu ainsi rediriger le trafic vers un compte gratuit ouvert sur CloudFlare. Contacté par Bloomberg, le spécialiste du CDN et des services DNS déclare avoir désactivé le compte depuis.
Sur Twitter, un compte se revendiquant de Lizard Squad prétend que les hackers du groupe sont à l'origine de cette attaque réussie. Toutefois, cette revendication ne suffit pas à en faire les auteurs véritables du piratage. En janvier, ces derniers assuraient ainsi être à l'origine de la panne de Facebook. Or, cette panne résultait d'une défaillance informatique et nullement d'une attaque.

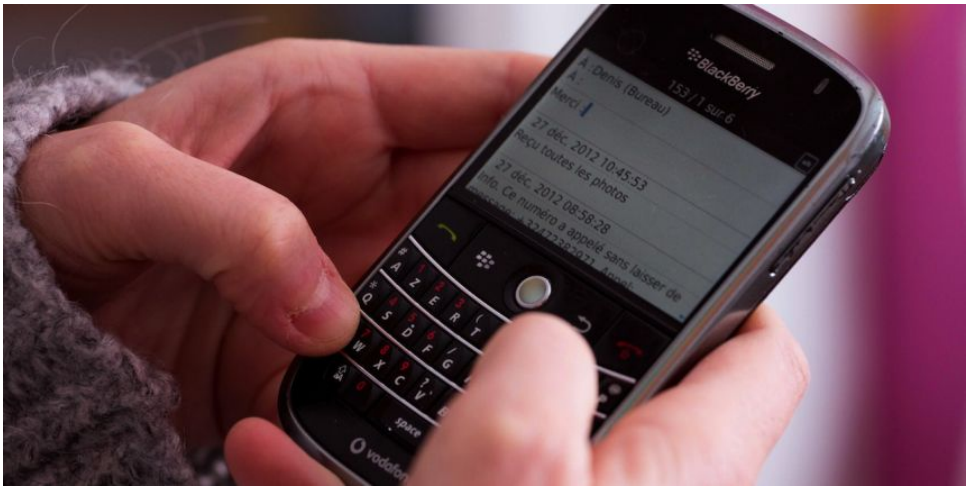
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/superfish-le-site-de-lenovo-pirate-en-represailles-39815368.htm

Big Boss is watching you: votre patron va adorer les objets connectés

	Big Boss is watching you: votre patron va adorer les objets connectés

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !



Il faudra désormais prendre garde à ce que vous écrivez depuis votre téléphone portable professionnel… Photo : Sipa

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !

La Cour de cassation a récemment rendu un arrêt qui donne aux SMS échangés sur les téléphones portables mis à disposition par les employeurs une présomption de « caractère professionnel ». Si vous voulez être certain que vos textos privés ne puissent être utilisés contre vous, il faudra désormais inscrire les mots « personnel » ou « perso » dans vos messages…

C'est une décision passée totalement inaperçue, mais qui concerne des centaines de milliers de salariés : tous ceux qui se sont vus mettre à disposition un téléphone portable par leur employeur. La Cour de cassation, dans un arrêt rendu le 10 février, que metronews s'est procuré, a validé le principe selon lequel les SMS envoyés ou reçus par cet appareil « sont présumés avoir un caractère professionnel ». Conséquence : « l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ».

Un processus pas « déloyal »

La plus haute juridiction de l'ordre judiciaire était invitée à statuer sur le litige opposant deux sociétés de courtage, GFI Securities Limited et Newedge. Cette dernière, reprochant à son concurrent d'avoir été déloyal en débauchant « un grand nombre » de ses salariés, avait utilisé comme preuve pour l'attaquer des SMS échangés entre ses anciens employés, qui évoquaient leur départ concerté de l'entreprise. En l'occurrence, Newedge négociant des produits financiers, tous les messages envoyés et reçus par ses salariés étaient automatiquement enregistrés sur un serveur informatique, conformément à la législation en vigueur.

Cette filiale de la Société Générale n'a donc eu qu'à effectuer une recherche à base de mots-clé pour retrouver et faire constater par huissier les SMS en question. Qui, pour la cour de Cassation comme pour la Cour d'appel de Paris dans un arrêt rendu il y a deux ans, constituent bien des preuves recevables : leur utilisation ne peut être considérée comme un « processus déloyal » ni « être assimilée à l'enregistrement d'une communication téléphonique privée effectuée à l'insu de l'auteur des propos ».

Pour les emails, c'était déjà le cas

Si dans cette affaire, les SMS avaient la particularité d'être stockés sur un serveur, la décision « est destinée à faire jurisprudence » pour tous les salariés à qui l'employeur a mis un téléphone portable à disposition, assure à metronews maître Jean-Philippe Duhamel, avocat au Conseil d'Etat et à la Cour de cassation. Avec cette décision souligne-t-il, la justice a manifesté « un souci de cohérence et de simplicité ». La Cour de cassation avait en effet déjà pris des arrêts similaires en ce qui concerne les fichiers détenus sur un ordinateur de travail ou les emails envoyés par un salarié depuis sa boîte pro. Depuis mai 2013 ainsi, l'employeur est dans son droit s'il ouvre en dehors de la présence de son employé un courrier électronique qui n'a pas été identifié comme personnel.

Comment éviter que vos textos privés ne puissent être utilisés contre vous ? La seule solution, explique Jean-Philippe Duhamel, est d'y intégrer « une mention les identifiant comme personnels, par exemple en les faisant commencer par les mots 'personnel' ou 'perso' ». Un peu contraignant pour des messages courts qui, contrairement aux emails, ne comportent le plus souvent pas de champ « objet ». Il existe toutefois une autre solution, plus radicale : réserver vos communications privées à votre téléphone personnel.

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

Source : http://www.metronews.fr/info/attention-votre-employeur-a-desormais-le-droit-de-fouiller-dans-les-sms-de-votre-telephone-pro/mobs!1pxxcsNP7VEA/
Par Gilles DANIEL

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

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Statut de l’hébergeur : nouvelles passes d’armes en prévision

Ce n'est pas la première fois qu'une reforme du statut des hébergeurs est évoquée et ça ne sera surement pas la dernière : le coup vient cette fois de la ministre de la Culture Fleur Pellerin qui appelle dans une interview du journal Les Echos à une réévaluation du statut juridique de l'hébergeur. « Ces statuts datent de la loi de confiance dans l'économie numérique, de 2004, qui transpose elle-même une directive européenne de 2000. Internet a évolué depuis ! ».

L'objectif affiché par Fleur Pellerin est ici de permettre une meilleure lutte contre la contrefaçon en ligne d'œuvre de l'esprit. Si la ministre exclut la possibilité de rendre ces « plateformes » entièrement responsables du délit, elle appelle à la mise en place d'un statut « hybride » afin de garantir une meilleure défense du droit d'auteur et une plus grande réactivité face à ces contenus illégaux.
Des propositions qui s'inspirent librement des recommandations émises par le conseil d'état comme le souligne Nextinpact, qui avait dans son rapport annuel 2014 consacré au numérique évoqué la mise en place d'un principe de « loyauté des plateformes » qui se traduirait par une série d'obligations et de contraintes venant limiter la marge de manœuvre des éditeurs vis-à-vis des contenus qu'ils diffusent via leurs services.

L'Afdel craint les effets de rebonds
La reforme du statut des hébergeurs est un thème qui revient régulièrement dans les projets législatifs et autres rapports du gouvernement. Mais celui-ci ne manque pas de faire réagir l'Afdel, qui a publié par voie de communiqué une longue tribune mettant en garde le gouvernement à l'égard de ces mesures. Si l'Association des éditeurs de logiciels ne parait pas opposée sur le principe à de nouvelles mesures visant à protéger plus efficacement les œuvres de l'esprit, elle s'inquiète des éventuels ricochets que pourrait provoquer une reforme du statut de l'hébergeur.
L'association souligne ainsi que « le statut juridique de l'hébergeur ne fait pas la différence entre différents types d'hébergeurs (B2C, B2B…) » Un point à clarifier pour l'Afdel, qui s'inquiète d'un impact possible de ce nouveau statut sur les entreprises proposant des services en mode Saas ou « qui stockent des données à la demande du destinataire du service ».
Le gouvernement reste pour l'instant évasif sur les prochaines mesures concrètes visant à matérialiser cette volonté affichée. Mais la grande loi sur le numérique promise par Axelle Lemaire pour 2015 est encore dans les cartons et sera peut être l'occasion pour le gouvernement de détailler leurs intentions.

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

Source : http://www.zdnet.fr/actualites/statut-de-l-hebergeur-nouvelles-passes-d-armes-en-prevision-39814102.htm
Par Louis Adam

Sommes-nous invisibles sur les réseaux sociaux anonymes

? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons » sur France 4

Sommes-nous invisibles sur les réseaux sociaux anonymes ? Denis JACOPINI répond à une journaliste de l'émission « On n'est plus des pigeons » sur France 4

Denis JACOPINI interviewé par une journaliste de l'émission « On n'est plus des pigeons » a répondu à la question « Sommes-nous invisibles sur les réseaux sociaux anonymes ? »Secret, Whisper ou Yik Yak… Ces nouveaux réseaux sociaux promettent l'anonymat à leurs utilisateurs. Sauf que rien n'est invisible sur le net.Rumeurs, mots doux, coup de gueule… Publier tout ce qui vous passe par la tête sans dévoiler sa véritable identité, c'est la promesse des réseaux sociaux anonymes comme Whisper.sh, chuchotement en français, Secret.ly, Rumr ou encore Yik Yak, une sorte de Twitter. Conçues essentiellement pour les smartphones, ces plates-formes gratuites incitent leurs membres à se lâcher sans compromettre leur e-réputation. Elles disent garantir des discussions avec des amis ou de parfaits inconnus sans qu'on puisse, dans certains cas, retrouver l'identité de l'émetteur, ou bien, les messages envoyés.

Doit-on féliciter ces applications en matière de protection de la confidentialité de ses utilisateurs ?
Mouais. Avant tout, à donner la possibilité de tout dire sous couvert d'anonymat, ces réseaux se livrent aux dérives de racisme, d'harcèlement et de diffamation. Au niveau technique, quelques incohérences. En octobre dernier, le quotidien britannique The Guardian, sur le point à l'époque de conclure un partenariat média avec Whisper, a eu accès aux coulisses de l'éditeur. Le journal a accusé l'application de collecter des données personnelles et de géolocalisation de ses utilisateurs. D'après The Guardian, Whisper gardait un œil sur les publications et les localisations de ses utilisateurs pour sa collaboration avec les médias. Le but : recouper le contenu des messages pour vérifier si une information était avérée.

Un réseau social qui ne laisse pas de traces, impossible ?
Pour Denis Jacopini, expert judiciaire en informatique, Whisper, comme les autres réseaux sociaux anonymes « se revendiquent dans leur communication comme une forme de réseau social anonyme. Sauf que la souscription n'est pas anonyme. Tous les éléments pour identifier une personne sont là au moment de l'inscription via son smartphone. »
Même si ce type d'applications ne donne pas directement accès à l'identité d'une personne, l'adresse IP du terminal utilisé pour la connexion Internet permet de récolter les informations du téléphone.
Pourtant, la garantie de l'impossibilité de « tracer » les utilisateurs a été mise en avant notamment par le réseau Whisper. Sur Twitter, son éditeur Neetzan Zimmerman garantissait mi-octobre 2014 qu'il est techniquement impossible de déterminer la localisation des utilisateurs qui n'activaient pas leur localisation GPS. Pour l'expert en informatique Denis Jacopini, « désactiver la localisation GPS est inutile » pour éviter tout traçage. En effet, l'adresse IP du téléphone permet de remonter au fournisseur d'accès à Internet puis de déterminer la localisation de l'utilisateur.
Des informations que les fournisseurs peuvent communiquer aux autorités sur demande. D'autant que le droit applicable en matière de protection des données est celui du pays du propriétaire des plates-formes, souvent américaines. « L'anonymat n'est pas garanti vis-à-vis des autorités, c'est bien pour les copains », conclut Denis Jacopini. Et encore. Alors, pour vider son sac en public sans problème, parlez-en à une proche. Tout s'arrange avec l'écoute et la parole.
Marie Dagman

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

Source : http://www.france4.fr/emissions/on-n-est-plus-des-pigeons/enquete/sommes-nous-invisibles-sur-les-reseaux-sociaux-anonymes_294315
Par Marie Dagman

Le fichage des passagers heurte les libertés individuelles

	Le fichage des passagers heurte les libertés individuelles – Politis

Ce procédé de récupération de données personnelles par le biais des compagnies aériennes était, jusqu'à présent, rejeté par le Parlement européen, pour incompatibilité avec la Charte européenne des droits fondamentaux.

Dimanche 11 janvier, réunion de crise à Paris. Bernard Cazeneuve a réuni ses homologues européens pour évoquer les attentats qui ont frappé la capitale quelques jours auparavant. Le but : prendre des mesures pour renforcer la lutte contre le terrorisme. Très vite, le Passenger Name Record (PNR) se retrouve sur les lèvres des politiques et s'affirme comme étant une des réponses à apporter pour renforcer la lutte anti-terroriste.

L'idée est reprise officiellement mardi à la tribune de l'Assemblée nationale par Manuel Valls. Le Premier ministre, s'engage à la mettre en place en France rapidement et y « appelle, de manière solennelle, (…) le Parlement européen à prendre enfin, toute la mesure de ces enjeux et à adopter ce dispositif, comme nous le demandons depuis deux ans ». Ainsi, la France réclame que le Parlement européen « débloque » le PNR afin qu'il puisse entrer en vigueur sur tout le territoire européen.
Qu'est-ce que le PNR ? Il s'agit en fait des données personnelles concernant un passager d'une compagnie aérienne. Ces données regroupent, d'après le texte officiel, les dates du voyage, l'itinéraire, les informations figurant sur le billet, les coordonnées du passager, le nom de l'agent de voyage auprès duquel le vol a été réservé, le moyen de paiement utilisé, le numéro du siège et des données relatives aux bagages.

La récupération de ces données constitue un manquement certain à la protection de la vie privée et des données personnelles. La conservation des données, leurs potentielles transmission à d'autres organes que les départements de sécurité et enfin, l'incompatibilité globale du PNR avec la Charte européenne des droits fondamentaux ont amenés le Parlement européen à rejeter la plupart des textes de type PNR.

Car le débat n'est pas nouveau. A Strasbourg, plusieurs projets de PNR ont déjà été présentés depuis une dizaine d'année. En 2004, c'était avec les États-Unis qu'il était question de créer une base de données sur les passagers.
Le texte avait était rejeté par la Cour de justice de l'Union européenne, non parce qu'il constituait une violation de la législation européenne, mais pour vice de forme. Un projet de loi similaire est à nouveau présenté au Parlement en 2011. A ce moment, et contrairement à 2004, un avis positif du Parlement est impératif pour que ce texte soit voté. A la surprise générale, il est adopté. C'est la commission des libertés civiques qui rejette finalement la directive PNR en 2013. L'année suivante, en novembre 2014, le Parlement demande que le PNR avec le Canada soit examiné par la Cour de justice européenne.
Les PNR étaient donc rejetés…jusqu'à la semaine dernière, où devant les drames qui touchèrent la capitale française, les autorités réactivent le projet. Pourtant, d'après le G29, un groupe de travail représentants les autorités indépendantes de protection des données nationales, les USA, un pays qui pratique le PNR, « n'ont jamais prouvé de façon concluante que la quantité considérable de données passagers collectée est véritablement nécessaire à la lutte contre le terrorisme et la grande criminalité ». En effet, selon Claudine Guerrier, enseignante-chercheuse en droit à l'institut des Mines Télécom, le PNR n'aurait réussi à faire intercepter que deux terroristes en dix ans.
Alors si le PNR est d'une efficacité relative, et si, comme le dit le contrôleur européen des données, Peter Hustinx, le PNR est contraire aux droits fondamentaux de l'UE, pourquoi les politiques insistent-ils aussi lourdement pour que le Parlement européen l'adopte ?
« Il faut qu'ils disent à l'opinion public qu'ils sont efficace », explique la députée européenne Front de gauche Marie-Christine Vergiat. « La question n'est pas d'être pour ou contre le terrorisme, la question est de ne pas se servir de ce prétexte pour mettre en place une surveillance généralisée. Ne pas agir au mépris des libertés publiques. »
Claudine Guerrier partage l'analyse : « C'est une mesure de facilité. Elle ne pose pas de problèmes de mise en place sur le plan juridique. Elle est quasiment prête, il n'y a qu'à prendre pour base les textes des précédents PNR qui n'ont pas aboutis. »
Mais si le Parlement européen tient bon depuis une dizaine d'années, cette fois, Marie-Christine Vergiat craint que « sous la pression de l'actualité et des Etats membres, certains eurodéputés ne changent d'avis à l'Assemblée ». Le PNR sera à l'ordre du jour du Conseil européen consacré en février à la lutte contre le terrorisme. Quoi qu'il arrive, Manuel Valls a de son côté annoncé que « la plate-forme de contrôle française sera opérationnelle dès septembre 2015 ».
Par Marie Roy

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

Source : http://www.politis.fr/PNR-Le-fichage-des-passagers,29704.html

---

Comme les États-Unis en 2001, ira-t-on vers un « Patriot

Act » ?

Comme les États-Unis en 2001, ira-t-on vers un « Patriot Act » ?

Les communications téléphoniques et sur Internet sont des vecteurs parfois utilisés par les terroristes. Après l'attentat de la semaine dernière, la France pose la question du renforcement de la surveillance.

Sous l'émotion des attentats du 11 septembre 2001 aux États-Unis, l'administration Bush avait adopté, sept semaines plus tard, une loi d'exception. Elle renforçait les pouvoirs du FBI, de la CIA et de la fameuse NSA, afin de lutter plus efficacement contre le terrorisme. Prévue, initialement, pour une durée de quatre ans, elle fut reconduite plusieurs fois. En 2015, le « Patriot Act » existe encore, et pourrait faire un émule en France.
Après l'attentat du 7 janvier contre Charlie Hebdo et les assassinats qui ont suivi, la classe politique française commence à formuler des propositions en ce sens. L'une des personnalités les plus unanimes sur le sujet est sans doute Valérie Pécresse, ministre UMP de l'Enseignement supérieur de 2007 à 2011. Sur Twitter, elle écrit ce lundi : « Il faudra bien entendu un Patriot Act à la française. Il faut une réponse ferme et globale ».

« Des mesures à prendre sur le Net »
En matière de renseignement, la surveillance des communications joue un rôle central. Alors que le suivi des frères Kouachi, suspectés d'avoir perpétré la tuerie à Charlie Hebdo, aurait connu un arrêt durant l'année 2014, le Premier ministre, Manuel Valls, considère qu'il y a une « faille » et appelle à « travailler à de nouveaux dispositifs pour être encore plus efficace ». Il suppose que des mesures seront prises pour combattre la diffusion de messages de « haine » sur Internet. « Il y a des mesures à prendre en plus sur le Net, car cela a un effet de contamination, de mimétisme », ajoute le ministre des Affaires étrangères, Laurent Fabius.

Des prises de position rejointes par l'opposition
L'ancien chef de l'Etat, Nicolas Sarkozy, s'exprimant au sujet d'Internet, a demandé à « surveiller ce qu'il s'y passe ». « Ce n'est pas parce que c'est virtuel que l'on peut s'exonérer des règles que l'on a mis plusieurs siècles à établir », a-t-il poursuivi. Si les débats ont commencé cette semaine au niveau politique, ces pistes sécuritaires ont suscité des réactions sur les réseaux sociaux.

Un Patriot Act « serait un comble »
« Après 4 millions de Français dans la rue aux cris de « liberté ! », on parle de PATRIOT Act à la française », dénonce par exemple « Maitre Eolas » sur Twitter. « Se réjouir de l'émergence d'un « Patriot Act à la française », c'est avaliser une altération programmée de la démocratie », estime pour sa part l'entrepreneur Gilles Babinet. Le blogueur Olivier Laurelli de rappeler que le Patriot Act tel que conçu aux Etats-Unis ne se limite pas à la surveillance des communications et qu'« on va pouvoir avoir un Guantanamo à la française ».
Interrogé par Petit Web, Benoit Thieulin, le président du Conseil national du numérique, estime que « ce serait un comble, après s'être opposé à la guerre en Irak et les révélations d'Edward Snowden » et souligne qu'Amedy Coulibaly, un des tueurs présumés, « ne disposait plus de smartphone depuis quelques temps déjà, afin d'éviter d'être tracé ». Mais au-delà de l'écoute des télécommunications, se pose enfin la question des prises de parole publiques sur les réseaux sociaux, telles que celle du polémiste Dieudonné ce lundi.
Sur sa page Facebook, il a affirmé se sentir « Charlie Coulibaly », détournant le slogan « Je suis Charlie » et l'associant au nom du tueur présumé. « Il ne faut pas confondre la liberté d'opinion avec l'antisémitisme, le racisme, le négationnisme », a aussitôt répliqué Manuel Valls à Dieudonné, au sujet duquel une enquête a été ouverte pour apologie d'actes de terrorisme. Bref, le débat sur le rôle d'Internet est loin d'être terminé.

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

Source : http://pro.clubic.com/legislation-loi-internet/actualite-749325-patriot-act-france.html
Par Thomas Pontiroli