Surveillance informatique par la NSA, C’est bien réel | Le Net Expert Informatique

Surveillance informatique par la NSA, C’est bien réel

Sur son blog, le cybercriminologue Jean-Paul Pinte a relayé un article du « Monde » racontant comment la NSA avait pu surveiller les organes de pouvoir de la France. « C'est bien réel, ce n'est pas de la science-fiction » assure-t-il.

Maître de conférences à l'université de Lille, spécialiste de la veille et de l'intelligence compétitive, il estime que la France devait savoir qu'elle était surveillée. Notamment « après l'expérience vécue par Angela Merkel en 2012 et 2013. Il ne peut donc y avoir de surprise, surtout vis-à-vis des États-Unis. Ceci dit, pour les pays qui subissent ce genre de surveillance, la principale chose qui les dérange c'est qu'ils ne peuvent pas faire la même chose. »
> Les moyens des États-Unis. Pour Jean-Paul Pinte la puissance acquise par les États-Unis dans le domaine du renseignement n'a pas d'égal. « Ils ont des logiciels comme Upstream qui vont capter les informations et analyser les contenus. Même involontairement, on peut être à la base d'une surveillance. Imaginez deux personnes qui communiquent par mail. L'une fait partie d'Alcatel ou EDF et si elle raconte qu'il y a du mouvement dans son entreprise, ce sera capté. » On a beaucoup parlé du programme Prisme, « cela prouve que les États-Unis pratiquent ce genre de surveillance depuis très longtemps ». Et les écoutes téléphoniques à la sauce américaine ont « plus de 50 ans ».
> L'espionnage dépasse les États. C'est pour cela que Jean-Paul Pinte ne croit absolument pas à la possibilité d'instaurer un code de bonne conduite. « Il faut être naïf pour penser s'en sortir comme ça. C'est une méconnaissance des entrailles du Web qui vont au-delà des États. Les États-Unis ont par ailleurs une certaine emprise sur Internet, ils peuvent fermer ou ouvrir des robinets et bloquer des pays, ils ont accès aux infrastructures, aux câbles et Prisme, Upstream… sont tellement puissants qu'ils sont presque devenus indolores. »
> Avoir toujours un coup d'avance. L'espionnage a toujours existé. « Aujourd'hui encore, des passagers montent dans l'Eurostar en première classe uniquement pour écouter les conversations de cadres ou de patrons du Cac40 et en faire des rapports. » Et le citoyen lambda n'est pas en reste. « Nous laissons énormément d'informations en chemin. C'est ce qu'on appelle aussi des métadonnées qui permettent de suivre nos pérégrinations, nos interactions sur les réseaux sociaux… » Pour l'espion, le tout est de ne pas se faire prendre. « Ce qui importe c'est que celui qu'on surveille ne soit pas conscient des écoutes. En cybercriminalité, c'est la même chose. C'est ce qui permet de se garantir d'avoir toujours un coup d'avance. »
Lire la suite….

Source : http://www.centre-presse.fr/article-397900-jean-paul-pinte-il-ne-peut-y-avoir-de-surprise-surtout-venant-des-etats-unis.html

---

Les outils techniques de la

lutte anti-drone évoluent| Le Net Expert Informatique

	**Les outils techniques de la lutte anti-drone évoluent**

Depuis octobre 2014, plusieurs dizaines de survols de sites sensibles par des drones ont été enregistrés. Des centrales nucléaires, des sites militaires ou encore le palais de l'Elysée ont été survolés par de petits engins difficiles à bloquer. Une mobilisation sans précédent a été lancée par le gouvernement et les entreprises. A l'occasion du Salon du Bourget, où des dizaines de drones civils et militaires sont présentées, 20 Minutes fait le point sur les outils techniques de la lutte anti-drones…

Vers une intégration de plusieurs dispositifs

Plusieurs systèmes regroupant des outils de détection, d'identification et d'interception sont en phase de développement. La société d'ingénierie JCPX Development a signé ce mercredi au Salon du Bourget un partenariat avec la direction des services de la navigation aérienne, Aveillant (groupe Altran), SkySoft et l'Ecole nationale de l'aviation civile (Enac) pour son système « Uwas – UAV Watch and Catch System ».

Ce dispositif comprend un radar pour détecter les engins volants, des caméras pour vérifier leur identité et les localiser, mais aussi des drones pour recueillir des données, voire les neutraliser grâce « à une claque magnétique », explique le président de JCPX Jean-Christophe Drai.

Ce système succède à deux projets primés en mars par l'Agence nationale de la recherche pour le compte du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN). Le premier, « Boreades », est développé par CS Systèmes d'information et deux PME. Il regroupe un système enregistrant la signature thermique du drone, le recueil de son image grâce à un réseau de caméras au sol, un leurre des repères GPS du drone, et une neutralisation de la télécommande de l'opérateur.

Des projets primés par l'Agence nationale de recherche

Le deuxième projet, « Angelas », est piloté par l'Onera, le centre français de recherche aérospatiale, dans le cadre d'un consortium réunissant trois industriels et quatre laboratoires publics de recherche. Ce dispositif recouvre la détection et l'identification des drones grâce à des caméras et des lasers, des équipements radars et acoustiques. Il peut utiliser le brouillage électronique.

Un brouillage des données de navigation (ondes radios, liaisons wi-fi, guidages par GPS) qui peut poser problème : « Le brouillage n'est pas directionnel. Dans la zone concernée, tout le monde le subit. Le GPS des voitures ne fonctionnera plus, les téléphones seront hors d'usage », relève Jean-Christophe Drai. La technique est difficilement utilisable en milieu urbain, où la chute d'un drone peut être dangereuse.

Le drone anti-drone

Une autre solution anti-drone est développée depuis plusieurs mois par l'entreprise française Malou Tech. Son drone « Intercepteur » fonce vers sa proie avant de la prendre dans ses filets. Mais selon une vidéo de présentation, un as du télépilotage semble pouvoir facilement échapper à ce drone anti-drone.

Le laser « tueur » de drone

Plusieurs pays, dont les Etats-Unis, la Chine et l'Allemagne ont développé des lasers anti-drones. LaChine paraît aujourd'hui en pointe dans ce domaine, avec un laser pouvant détruire, dans un rayon de deux kilomètres, des drones de petite taille. Cependant, ce système a ses limites : Difficilement utilisables par mauvais temps, les lasers ne sont pas adaptés au milieu urbain.

Source : http://www.20minutes.fr/societe/1634983-20150618-survol-zones-sensibles-outils-techniques-lutte-anti-drone-evoluent
Par Anne-Laëtitia Béraud

La lutte de la Cybercriminalité passe par la coopération et la formation des enquêteurs (Octopus 2015) | Le Net Expert Informatique

	Cybercriminalité: la lutte passe par la coopération et la formation des enquêteurs (Octopus 2015)

Une coopération internationale renforcée en matière de cybercriminalité et des enquêteurs mieux formés permettraient aux Etats de mieux lutter contre ce fléau, ont conclu vendredi des experts réunis à Strasbourg au Conseil de l'Europe.

Experts internationaux, juges, policiers, responsables gouvernementaux: réunis depuis mercredi à Strasbourg (est de la France), 300 participants à la conférence sur la cybercriminalité Octopus 2015 ont avancé plusieurs pistes de travail.
Parmi les domaines d'actions jugés prioritaires, une coopération internationale plus efficace, des outils et des capacités de lutte renforcés permettraient aux Etats d'être mieux armés pour poursuivre et faire condamner les auteurs d'infractions dans le cyberespace, a affirmé Gabriella Battaini-Dragoni, vice-présidente du Conseil de l'Europe, qui présentait les conclusions des participants à la conférence.
Le Conseil de l'Europe a annoncé qu'il allait « démultiplier » ses efforts pour aider les Etats qui le souhaitent à organiser un programme de formation pour juges et procureurs internationaux, a indiqué Mme Battaini-Dragoni.
L'organisation paneuropéenne, qui compte 47 Etats-membres, veut notamment aider les enquêteurs à se servir du « cloud-data », ces traces informatiques qui permettent d'identifier et de poursuivre les criminels.
Elle proposera dans un premier temps un « Guide des preuves électroniques », sous forme de glossaire informatique.
L'idée est aussi de permettre aux enquêteurs de « parler la même langue », selon Alexander Seger, chef de la division de la lutte contre la cybercriminalité au Conseil de l'Europe.
Selon M. Seger, les « territorialités » et les frontières continuent en effet de faire obstacle en matière de coopération entre enquêteurs, qui peuvent avoir besoin de trouver des éléments de preuve hébergés sur des serveurs informatiques à l'étranger.
Selon le Conseil de l'Europe, depuis 2001, 66 pays dont la France ont signé, ratifié la Convention de Budapest sur la cybercriminalité, ou ont été invités à y adhérer.
Plus de 120 pays au total coopérent avec le Conseil de l'Europe pour renforcer leur législation et leur capacité de lutte contre la cybercriminalité.

Source : http://www.notretemps.com/internet/cybercriminalite-la-lutte-passe-par-la,i88427

La vidéosurveillance de la ville auditée par un Infirmier | Le Net Expert Informatique

	La vidéosurveillance de la ville auditée par un Infirmier

Interdictions de stade : le PSG à nouveau épinglé par la CNIL | Le Net Expert Informatique

	Interdictions de stade : le PSG à nouveau épinglé par la CNIL

Le Paris-Saint-Germain (PSG) est à nouveau épinglé dans le traitement de certains de ses supporteurs. La Commission nationale de l'informatique et des libertés (CNIL) a publié, mercredi 10 juin, un communiqué officiel pour signifier une nouvelle mise en demeure à l'encontre du club de football de la capitale. Il s'agit de la deuxième procédure de ce type en deux ans.

La Commission, chargée de sanctionner les manquements à la loi informatique et libertés, reproche aux dirigeants du club francilien de ne pas s'être « borné à gérer la liste des interdits de stade à l'intérieur du cadre légal, mais d'avoir décidé d'exclure les personnes faisant l'objet de ces mesures, après l'expiration de celles-ci, pendant une durée au moins équivalente ».

Pas de sanctions pour l'instant

La CNIL pointe notamment l'interdiction de stades de certains supporteurs parisiens, ainsi que la conservation de données personnelles au-delà du délai de l'interdiction. Or, seuls le préfet ou le juge peuvent prendre, ou étendre, des mesures d'interdiction de stade.

Dans son communiqué, la CNIL rappelle que cette mise en demeure n'est pas synonyme de sanction. « Aucune suite ne sera donnée à cette procédure si la société [le PSG] se conforme à la loi dans le délai imparti d'un mois », peut-on lire. Dans le cas contraire, l'organisme de défense des libertés individuelles et publiques pourrait nommer un rapporteur qui sera chargé de proposer une sanction à l'égard du champion de France en titre.

En janvier 2014, la CNIL avait autorisé le club dirigé par Nasser Al-Khelaïfi à créer un fichier afin de lister les supporteurs exclus du stade par les autorités selon des motifs bien précis comme « l'existence d'un impayé, le non-respect des règles de billetterie, l'activité commerciale dans l'enceinte sportive en violation des conditions générales de ventes, etc. », précise le communiqué.

.

Source : http://www.lemonde.fr/ligue-1/article/2015/06/10/interdictions-de-stade-le-psg-a-nouveau-epingle-par-la-cnil_4651214_1616940.html
Par Kozi Pastakia

Surveillance des salariés et logiciel de détection

d’infractions pédopornographique | Le Net Expert Informatique

Surveillance des salariés et logiciel de détection d’infractions pédopornographique

Dans un arrêt du 11 mai 2015, le Conseil d’État confirme une délibération de la Cnil refusant à une entreprise la mise en place sur les postes informatiques d’un logiciel de recherche des infractions à caractère pédopornographique.

Si l’employeur peut exercer une surveillance sur les connexions internet des salariés sur leur poste de travail, de là à pouvoir mettre en œuvre un logiciel ayant pour objet de collecter des données relatives à la consultation par les salariés de sites à caractère pédopornographique, il y a un pas que n’a pas franchi la Cnil ni le Conseil d’État.
En effet, le Conseil d’État a été saisi par une entreprise d’une demande d’annulation de la décision de la Cnil lui refusant l’autorisation de mettre en place un tel logiciel.
La Haut juridiction n’a pas annulé la décision de la Cnil en considérant que la loi informatique et libertés ne permet à une entreprise privée de mettre en œuvre un traitement de données personnelles visant des infractions pénales ou qui peuvent en établir l’existence.

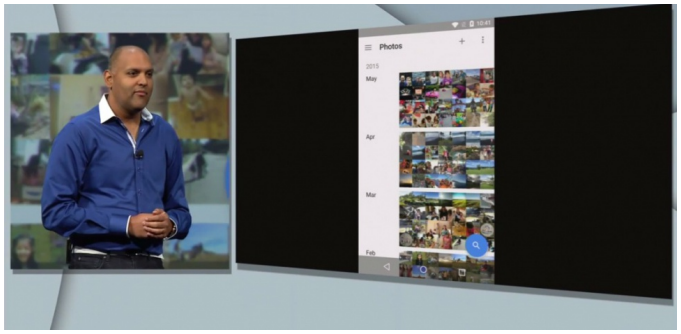
CE 11 mai 2015, n° 375669
Lire la suite….

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

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

S o u r c e : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126327/Surveillance-des-salaries-et-logiciel-de-detection-dinfractions-pedopornographique.aspx
Par Dominique Jullien

Et maintenant Google veut vos photos. Toutes vos photos… | Le Net Expert Informatique



Ani Sabharwal, responsable de l’application Photos chez Google, lors de sa présentation au Google I/O le 29 mai 2015. Google

Et maintenant Google veut vos photos. Toutes vos photos…

Après les courriers électroniques, Google veut héberger toutes les photos des internautes. Et bien sûr, analyser leur contenu.

A peine quelques jours avant Apple, c’est Google qui a organisé sa grand-messe annuelle à l’attention des développeurs. L’occasion de se faire une idée des prochains développements sur lesquels mise le géant américain. Parmi eux, une application qui a de bonnes chances de faire mouche auprès du grand public : Google Photos. A première vue, rien de révolutionnaire, car il s’agit d’une application de stockage et de partage de ses photos. Mais avec le petit détail dont Google s’est fait une spécialité : le stockage illimité et gratuit. Et la taille du stockage, c’est ce qui avait assuré par le passé le succès de Gmail face aux messageries déjà implantées.

Un stockage gratuit et illimité

Pour la première fois, le grand public a donc une solution gratuite de sauvegarde de l’ensemble de ses photos et même de ses vidéos. Avec une limitation technique qui ne devrait pas poser de problème aux non-professionnels : la qualité des photos est limitée à 16 mégapixels et celle des vidéos à 1080p (limitation dont on peut se défaire pour 10 dollars par mois et par teraoctet de données). L’interface est soignée, très épurée, dans la droite ligne des produits maison. On peut classer les photos, les retoucher, faire des montages. Google a aussi mis à disposition de chacun ses algorithmes de fouille d’image. Ainsi, toutes les photos sont analysées et l’application y reconnaît toute seule les visages ou des éléments comme par exemple de la nourriture. On peut théoriquement ainsi retrouver des photos en tapant des mots-clés dans le moteur de recherche sans jamais avoir « taggé » ses photos. Démonstration sur scène avec une recherche instantanée des photos après avoir dicté « tempête de neige à Toronto ». La recherche combine sans doute les éléments de neige sur l’image avec la géolocalisation de la ville.

La mort de Google+

Cette nouvelle application marque le premier signe du repositionnement de Google sur les réseaux sociaux. En effet, elle découle du début de démantèlement de Google+, qui n’a jamais su s’imposer face à Facebook. En séparant la partie photos de son réseau social, Google va essayer de reprendre du terrain sur les images. D’autant que l’application n’existe pas que sur le web ou les appareils Android : elle est aussi disponible sur iOS (le système d’exploitation d’Apple), ce qui en fait un grand concurrent du stockage des photos sur le cloud d’Apple, qui lui est facturé au prix fort : de 0,99 € par mois pour 20 Go à 19,99 € pour 1 To. Avec ce nouveau service, Google semble bien armé pour réussir ce qu’il a fait avec Gmail : garder l’internaute dans son propre univers en hébergeant ses données personnelles, afin de pouvoir par la suite se rémunérer avec la publicité. En sachant en plus cette fois tout ce qu’il y a dans ses photos et où et quand elles ont été prises.

La conférence est à revoir en intégralité ici :

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.sciencesetavenir.fr/high-tech/20150529.OBS9810/et-maintenant-google-veut-vos-photos-toutes-vos-photos.html?cm_mmc=EMV-_-SEA-_-20150531_NLSEAACTU-_-et-maintenant-google-veut-vos-photos-toutes-vos-photos##xtor=EPR-6-ActuSciences17h-20150531

La NSA écoute nos disques durs ?

La NSA écoute nos disques durs ?

Kaspersky Lab a découvert une plate-forme de cyber-espionnage dont l'une des composantes, très certainement exploitée par la NSA, permet de surveiller des disques durs.

Iran, Russie, Pakistan, Afghanistan, Chine, Mali, Syrie, Yémen, Algérie… Les gouvernements, organes militaires, sociétés télécoms, banques, médias, chercheurs et activistes d'une trentaine de pays auraient été exposés à des logiciels espions cachés dans des disques durs.
Les équipes de Kaspersky Lab en sont arrivées à cette conclusion après plusieurs années d'enquête sur ce qu'elles considèrent aujourd'hui comme le dispositif de surveillance électronique « le plus complexe et le plus sophistiqué » découvert à date*.
Encore activement exploitée, cette plate-forme serait opérationnelle depuis au moins 2001, voire 1996, si on se fie à la date d'enregistrement de certains serveurs utilisés pour contrôler les malware.
Elle hébergerait notamment un ver très proche de Stuxnet. Ce virus complexe et polymorphe dont la conception est attribuée à l'Agence américaine de sécurité nationale (NSA) avec la collaboration de l'unité 8200 de l'armée israélienne (cyberdéfense) avait mis à mal un site d'enrichissement d'uranium implanté en Iran, endommageant un millier de centrifugeuses.
Mais c'est bien le module de piratage des disques durs qui retient l'attention de Kaspersky. Dans son rapport publié lundi (document PDF sur http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf, 44 pages), l'éditeur russe note que la quasi-totalité des produits du marché sont affectés : Seagate, Western Digital, Toshiba, IBM, Micron, Samsung…
Il est d'autant plus difficile de détecter l'infection qu'elle se loge dans le firmware des disques durs. Ce qui lui permet aussi de s'activer presque instantanément au démarrage (la seule étape qui précède dans la séquence d'amorçage est l'initialisation du BIOS) et d'ouvrir discrètement des portes dérobées permettant de récupérer des données à foison.
Pour Kaspersky Lab, réussir à implanter un logiciel malveillant dans le firmware d'un disque dur est une prouesse. A moins que les pirates aient eu accès au code dudit firmware. Du côté de Western Digital, on assure ne pas avoir communiqué ce genre de données. Chez Seagate, on estime avoir intégré des couches de sécurité pour éviter les modifications non sollicitées du micrologiciel, ainsi que son étude par reverse engineering.

A qui la faute ?
Le problème remonte peut-être à 2009. Dans le cadre d'une vague de cyber-attaques contre des sociétés high-tech américaines, les pirates avaient eu accès à du code source qualifié de « très précieux » car hébergé sur les serveurs de multinationales et d'organes gouvernementaux.

Dans ce butin figuraient probablement des copies du firmware des différentes marques de disques durs. Et pour cause : lorsqu'elles acquièrent un équipement informatique, les agences classées « sensibles » peuvent demander, pour le compte du gouvernement américain, un audit de sécurité des produits pour s'assurer de l'intégrité du code source… lequel est certainement sauvegardé au passage.

Kaspersky Lab n'affirme pas que la NSA est à l'origine de ce « mouchard à disques durs ». Ses chercheurs disposent toutefois de nombreux indices, comme ce mot-clé GROK trouvé dans le code d'un enregistreur de frappe et déjà présent dans un outil d'espionnage dévoilé en 2013 par Edward Snowden.

Les multiples révélations du lanceur d'alertes pèsent sur l'activité des sociétés high-tech américaines : les ventes de solutions – aussi bien matérielles que logicielles – chutent. A tel point que Peter Swire, membre du groupe de réflexion «Renseignement et Nouvelles technologies» monté par Barack Obama, reconnaît qu'il est «plus que jamais indispensable, pour les Etats-Unis, de mesurer l'impact que chaque décision d'exploiter une faille de sécurité pourrait avoir sur les relations commerciales […] et diplomatiques».

* Malgré sa puissance, il semble que la plate-forme ne soit exploitée que contre un nombre restreint de «cibles d'intérêt» localisées hors des Etats-Unis.

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

Source : http://www.itespresso.fr/cyber-espionnage-nsa-ecoute-disques-durs-88684.html
Par Clément Bohic

La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ? | Le Net Expert Informatique

	La loi sur le renseignement mettra-t-elle en place une « surveillance de masse » ?

Depuis le début de l'examen, à l'Assemblée nationale puis au Sénat, du projet de loi sur le renseignement, une disposition du texte concentre les critiques et les débats. Il s'agit d'une partie de son article 2, qui permettra aux services de renseignement d'installer des appareils analysant le trafic Internet pour détecter des comportements suspects de terrorisme. Le terme de « boîte noire », d'abord avancé par le gouvernement, est devenu leur nom officieux.

Les détracteurs de la loi y voient, par son caractère systématique et indistinct, l'introduction dans la loi française de la surveillance de masse. Ses partisans refusent le terme. Au Sénat, mardi 2 juin, ils ne sont pas parvenus à trancher ce débat, qui est loin d'être seulement sémantique.

Que dit le projet de loi ?

Le projet de loi sur le renseignement prévoit, en l'état, dans le seul cadre de la lutte contre le terrorisme, la mise en place de « traitements automatisés » sur les réseaux des fournisseurs d'accès à Internet français. Cela signifie que des matériels seront physiquement installés chez les opérateurs, dans lesquels des logiciels – les fameux algorithmes – vont inspecter les flux de données des internautes à la recherche de signaux que les services estiment être avant-coureurs d'un acte terroriste.

Pour les opposants, cela ne fait pas de doute. Si des algorithmes inspectent, automatiquement, l'intégralité des flux qui transitent chez les fournisseurs d'accès à Internet (FAI) à la recherche de comportement suspects, il s'agit d'une mesure de surveillance de masse ; et ce, même s'ils ne sont destinés qu'au repérage de quelques personnes. C'est le cas du sénateur Claude Malhuret (Allier, Les Républicains), joint par Le Monde :

« Ceux qui disent qu'il ne s'agit pas de surveillance de masse disent, à la phrase suivante, qu'il s'agit de chercher une aiguille dans une botte de foin. Mais la botte de foin, c'est l'Internet français ! Les boîtes noires installées chez les FAI analyseront l'intégralité du trafic Internet français. C'est comme les radars sur les principales autoroutes : au bout de quelque temps, tous les Français seront passés devant. Elles cherchent des critères précis, mais en surveillant tout le monde ! »

Difficile en effet de qualifier autrement que « de masse » ce dispositif de surveillance, qui, au minimum, inspectera de très grandes quantités de données pour n'y repérer que quelques activités suspectes.

Ce qualificatif est pourtant violemment récusé par les défenseurs du texte. Le premier ministre, Manuel Valls, a assuré au Sénat mardi 2 juin que le projet de loi « n'exerçait pas de surveillance de masse des Français ». « Le texte n'autorise que de la surveillance ciblée, pas de surveillance de masse » a renchéri son collègue de la défense, Jean-Yves Le Drian.

Pas « d'atteinte à la vie privée »

Le sénateur socialiste du Loiret Jean-Pierre Sueur est du même avis :

« Il ne faut pas faire dire à la loi ce qu'elle ne dit pas. Certains disent que nous pompons les données comme le Patriot Act. C'est faux, c'est quelque chose contre lequel on a toujours été opposés. »

Lorsqu'on lui fait remarquer que pour repérer les suspects dans le flot des connexions, il faudra bien passer en revue toutes les connexions des internautes français, le sénateur dément : « Il ne s'agit pas de tout l'Internet français, mais seulement ceux qui se connectent aux sites terroristes. Notre objectif n'est pas de porter atteinte à la vie privée. » Un exemple d'utilisation des « boîtes noires » qui n'est cependant pas le seul avancé par les promoteurs du dispositif.

La loi ne précise pas les modalités exactes du déploiement de ces « traitements automatisés ». Elle ne limite d'ailleurs pas leur activité à la détection des visiteurs de sites terroristes (dont le blocage est par ailleurs prévu par la loi sur le terrorisme adoptée à la fin de 2014) mais, plus largement, des « connexions susceptibles de révéler une menace terroriste ».

De multiples amendements de suppression des algorithmes

La délicate question des algorithmes dans la loi sur le renseignement a été abordée mercredi soir au Sénat. Des députés issus de tous les groupes politiques, de la gauche à la droite, ont déposé des amendements de suppression du dispositif de « boîtes noires ».

La commission des lois du Sénat a apporté quelques modestes retouches : la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'organisme administratif de contrôle que crée la loi, pourra désormais se prononcer sur les « paramètres » des algorithmes, et non plus sur leurs « critères ». La commission a aussi précisé que l'autorisation du premier ministre, dont la validité sera ramenée de quatre à deux mois, devra préciser les paramètres des algorithmes. L'accès de la CNCTR aux algorithmes ne sera, enfin, pas seulement « permanent », mais également « direct ».

Source : http://www.lemonde.fr/pixels/article/2015/06/03/la-loi-sur-le-renseignement-mettra-t-elle-en-place-une-surveillance-de-masse_4646733_4408996.html
Par Martin Untersinger

Les atteintes aux libertés de la Loi Renseignement | Le Net Expert Informatique

Les atteintes aux libertés de la Loi Renseignement

Hier, le Sénat a commencé l'examen du projet de loi sur le renseignement par l'inévitable discussion générale. Chacun des groupes et sénateurs a pu ainsi donner « sa » religion sur ce texte, contesté par bon nombre d'organisations de la société civile, tout comme la CNIL ou le défenseur des droits. Compte rendu.

D'entrée, Manuel Valls a jugé le texte comme indispensable afin d'apporter la précision et l'encadrement nécessaire aux activités des services du renseignement, dans un contexte d'évolution technologique : « Il faut pouvoir suivre les terroristes sur leurs réseaux, car ils utilisent tous les outils du numérique pour leurs actions de propagande et d'embrigadement, ainsi que pour échanger. C'est pourquoi nous autorisons le recours aux algorithmes : afin de détecter des terroristes jusqu'alors inconnus et des individus connus qui recourent à des techniques de dissimulation. Moins d'un djihadiste sur deux avait été détecté avant son départ en Syrie ; nous devons pouvoir faire mieux. »

Quand Philippe Bas s'attaque aux « inoculations toxiques »

Des propos à comparer à ceux de Philippe Bas (UMP), rapporteur du texte : « **Le texte confronte les intérêts fondamentaux de la Nation et la sauvegarde de la vie humaine aux exigences aussi fortes que sont le respect de la vie privée et la garantie des libertés fondamentales. Il donne un cadre légal aux services de renseignement** » s'est-il félicité, en pleine phase avec le gouvernement. S'en prenant aux détracteurs, il jure cependant que ce projet « ne renforce pas les moyens des services de renseignement, ce n'est pas son objet. Il n'a rien à voir avec la caricature qui en a été faite. Les critiques qui lui sont faites, cependant, sont autant d'anticorps pour que l'État de droit résiste à des inoculations toxiques pour les libertés ».
Une erreur d'analyse patente puisque le projet de loi vise bien à décupler les moyens des services du renseignement, au motif ou prétexte de leur encadrement.

Renseignement, Google, même combat

Yves Detraigne (UDI-UC) s'en est tout autant pris aux opposants à ce texte qui condamnent l'usage des algorithmes, « dont l'utilisation quotidienne, à des fins mercantiles, par les géants du web tels que Google, ne provoque pas les mêmes réactions ». Comme si Google pouvait vous envoyer en prison… Jean-Jacques Hyest (UMP) a pris pour cible la presse et les discours anxiogènes amplifiés lors d'une précédente loi sécuritaire: « On annonçait une catastrophe pour les libertés publiques, c'était « l'horreur » – alors que l'article 13 est plus protecteur des libertés publiques que le droit qui prévalait jusque-là. » Tellement protecteur que cet article (devenu l'article 20), qui autorise l'aspiration de données de connexion par le renseignement, est actuellement en voie de QPC au Conseil d'État. La Quadrature du Net, FDN et FFDN ayant victorieusement fait valoir aux yeux du rapporteur que certains droits et libertés fondamentaux étaient un peu trop menacés par ces mécanismes, qui servent de socles juridiques à la loi Renseignement.

Il y aura des faux positifs et des atteintes aux libertés

Pierre Charon (UMP) admet sans sourciller que des « faux positifs » seront possibles avec les boites noires (algorithme détectant les premières traces de menace terroriste). Mais pas grave : « Cela confirme que nos services ont aussi besoin de moyens humains » et que « les citoyens doivent avoir des voies de recours ». Analyse similaire chez Jean-Pierre Sueur (PS) qui explique que les atteintes aux libertés sont nécessaires : « Vous savez qu'il existe des sites dangereux parce qu'ils encouragent à l'oeuvre de mort. Je crois l'atteinte aux libertés nécessaire pour combattre le terrorisme, pourvu qu'elle soit limitée par le droit ». La question du terrorisme cependant n'est qu'un petit versant de ce texte qui autorise l'espionnage pour d'autres fins, notamment celle de la défense ou la promotion des intérêts français.

Le germe d'une collecte massive débouchant sur une surveillance généralisée

La sénatrice Michelle Demessine (CRC) sera pour sa part plus critique : « ce texte porte en lui le germe d'une collecte massive et indifférenciée de données qui débouche inévitablement sur une surveillance généralisée de la société. ». Claude Malhuret (UMP) embraye, plus réservé encore : « On nous dit que ne seraient concernées que les métadonnées. Cela relève de l'escroquerie intellectuelle. M. X, marié, se connecte tous les quinze jours à un site de rencontres extra-conjugales ; M. Y, dans la même situation, visite toutes les semaines un site de rencontres homosexuelles. Les métadonnées contiennent toute l'information intéressante. Point besoin de connaître aussi le contenu ».

Le sénateur s'est d'ailleurs appuyé sur les (pseudos) reculades aux États-Unis en matière de renseignement pour justement torpiller le pas de danse français. « Nous ne sommes plus loin des horreurs décrites par Orwell après la révélation par Edward Snowden des pratiques de la NSA » ajoute Catherine Morain-Desailly (UDI-UC). « Ce texte est bien un Patriot Act à la française, pris en hâte après les attentats de janvier. Les algorithmes sont source d'erreur, on le sait. Pourquoi les légaliser quand le Congrès américain le refuse désormais ? Supprimons le contrôle par les boites noires qui fragilisent la sécurité des données des entreprises et des institutions à cause des failles que les cybercriminels savent exploiter. Instituons un contrôle de la CNIL, le seul rempart contre l'arbitraire, l'hypersurveillance et l'hypervigilance ».

C'est quoi le programme ?

Les sénateurs débattront véritablement des articles et des amendements à partir de 14 h 30 aujourd'hui jusqu'au 9 juin. Ensuite « leur » texte sera arbitré avec celui des députés en Commission mixte paritaire. Si le gouvernement le souhaite, c'est l'Assemblée nationale qui pourra avoir le dernier mot, du moins si la disharmonie perdure. Après cela, le projet de loi devrait être contrôlé par le Conseil constitutionnel, avant sa publication au Journal officiel. Une promesse de François Hollande, alors que plus de 60 députés se sont déjà réunis pour doubler cette saisine par une action parlementaire en ce sens. Ajoutons que le Conseil constitutionnel pourrait dans le même temps examiner le recours précité, initié par la Quadrature du Net, la FDN et FFDN, si du moins le Conseil d'État suit l'avis du rapporteur général en ce sens (notre compte rendu et l'interview de Me Spinosi)

Source : http://www.nextinpact.com/news/95299-loi-renseignement-faux-positifs-atteintes-aux-libertes-pas-grave.htm
Par Marc Rees