Une loi pour vous espionner… | Le Net Expert Informatique

Une loi pour vous espionner…

Alors que les révélations sur les activités de la NSA en France se multiplient et que le terrorisme frappe à nouveau, le gouvernement vient de faire voter une loi sur le renseignement qui autorise de nouvelles techniques d'espionnage très intrusives. Enquête sur ces nouveaux dispositifs controversés.

«Inacceptables.» C'est en ces termes attendus que l'Elysée a qualifié les écoutes de l'agence américaine NSA sur la France, révélées à partir du 24 juin par l'organisation WikiLeaks et les journaux Mediapart et Libération. L'ensemble de la classe politique a réagi à l'unisson aux premières publications de documents concernant les interceptions par la NSA, entre 2006 et 2012, des conversations des trois présidents successifs Jacques Chirac, Nicolas Sarkozy et François Hollande, ainsi que des cas d'espionnage économique. «Ces pratiques portent atteinte à la confiance entre alliés», a fustigé le …
Lire la suite….

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

Source : http://www.lefigaro.fr/actualite-france/2015/07/03/01016-20150703ARTFIG00179-loi-renseignement-comment-vous-allez-etre-espionnes.php

Les techniques du renseignement français se dévoilent un peu plus | Le Net Expert Informatique

	Les techniques du renseignement français se dévoilent un peu plus

Le Nouvel Obs a publié dans ses colonnes une longue enquête faisant le point sur les écoutes et techniques mises en place par le renseignement français. Un rapide aperçu des capacités de la France en la matière.

Et le premier constat que l'on peut tirer, c'est que la France s'est évertuée à rattraper son retard sur les américains dès 2008. Comme le rapporte l'Obs, c'est en effet à cette date qu'a été lancée la première phase d'un plan initié par Nicolas Sarkozy afin de remettre en adéquation les méthodes et équipement des services de renseignement français, dont l'essentiel des ressources s'était concentré dans les années 80 et 90 sur l'interception des communications satellites.

Des satellites aux câbles

Plus intéressants que les communications satellites en effet, les câbles sous-marins sont devenus au cours de la première décennie des années 2000 l'axe privilégié de transit d'informations. Et comme le remarquaient certains observateurs, la France est particulièrement bien située à cet égard, disposant à la fois de nombreux câbles en direction de l'Afrique du Nord, ainsi qu'à travers le pacifique ou la méditerranée. Et dispose en plus de cela d'un acteur majeur du marché, Alcatel, qui selon l'Obs a participé à la mise en place de cette surveillance du réseau en formant les services du renseignement aux techniques de manipulation de la fibre.

Orange serait aussi venu prêter main-forte, l'opérateur gère en effet l'accès aux points d'arrivée de ces câbles sous-marins en France, qui en dénombre une douzaine. La technique utilisée n'a rien de révolutionnaire : il s'agit de l'extension numérique de la technique des « bretelles » : une ligne dédoublée, dont l'une des extrémités part directement vers un local de la DGSE.

L'Obs détaille le régime auquel ces écoutes étaient soumises : la commission nationale de Contrôles des Interceptions de Sécurité avait ainsi son mot à dire, et des règles étaient posées afin d'éviter les abus, notamment à l'égard des citoyens français. Mais face aux réalités et à l'ampleur du phénomène, la CNCIS se contentait de donner un avis par pays pour autoriser ou non les écoutes, simplifiant l'acheminement des données vers un datacenter dédié au traitement situé à Paris, boulevard Mortier. L'organe de contrôle, aujourd'hui remplacé par la CNCTR dans le cadre de la loi renseignement, pouvait aussi décider de limiter les écoutes à un thème précis.

Des écoutes encadrées ?

L'hebdomadaire rapporte que les écoutes se focalisaient sur certains pays, tels que les États-Unis ou le Moyen-Orient, et en délaissaient d'autres, comme le Japon. Le magazine souligne également le fait que ces écoutes n'ont pas été simplement employées dans le cadre de la lutte antiterroriste, mais aussi pour la promotion économique du pays. Une révélation qui peut faire sourire, alors que Wikileaks a révélé en début de semaine les indiscrétions de la NSA sur ces questions. On se demande même si ces révélations ne tombent pas à pic…

L'Obs donne les contours d'un vaste plan engagé par le renseignement français : en l'espace de 5 ans, à compter de 2008, 700 millions d'euros ont été débloqués dans le cadre ce plan et 600 embauches parmi les services. Et d'expliquer que François Hollande, lors de son arrivée au pouvoir en 2012, n'a pas remis en question cet effort et travaille au contraire à approfondir les premiers accords noués sous Sarkozy avec le GCHQ britannique, avec qui la France a établi en 2010 un traité militaire comprenant un discret volet sur l'échange d'informations dans le domaine du renseignement.

Une structure d'ampleur, que la loi renseignement, actuellement examinée par le Conseil constitutionnel, ne vient absolument pas remettre en cause.

Source : http://www.zdnet.fr/actualites/les-techniques-du-renseignement-francais-se-devoilent-un-peu-plus-39821892.htm
Par Louis Adam

Comment la France écoute (aussi) le monde | Le Net Expert Informatique

Comment la France écoute (aussi) le monde

Révélations sur un vaste plan de la DGSE pour intercepter les communications internationales passant par les câbles sous-marins : lancé en secret par Nicolas Sarkozy, il vient d'être légalisé par François Hollande en toute discrétion.

Il n'y a pas que la NSA. La France aussi écoute le monde. Après une enquête de plusieurs semaines, « l'Obs » révèle que :
– Début 2008, Nicolas Sarkozy a autorisé la DGSE à espionner les communications internationales transitant par les câbles sous-marins qui relient l'Europe au reste du monde. Un plan de 700 millions d'euros sur cinq ans (2008-2013) a été lancé par le service secret pour installer des stations d'interceptions à l'arrivée des câbles en France (notamment à Marseille, Penmarch et Saint-Valéry-en-Caux).
– Au moins cinq câbles majeurs ont été mis sur écoute pendant cette période avec l'aide de l'opérateur Orange et du groupe Alcatel-Lucent dont le TAT14 vers les Etats-Unis ; le I-Me We vers l'Inde ; le Sea-Me-We 4 vers l'Asie du Sud-est ; et le ACE vers l'Afrique de l'Ouest.
– La DGSE a passé un grand accord de coopération avec le GCHQ britannique. C'est une annexe secrète au traité de défense dit de Lancaster House, signé le 2 novembre 2010 par Nicolas Sarkozy et David Cameron.
– François Hollande a autorisé la DGSE à étendre ces opérations à d'autres câbles dans un nouveau plan quinquennal (2014-2019). L'article L-854-1 de la toute nouvelle loi sur le renseignement vise à les légaliser en catimini.
C'est un plan classé « très secret », exposé ici pour la première fois. Un projet de la Direction générale de la sécurité extérieure (DGSE) autorisé par Nicolas Sarkozy il y a sept ans et poursuivi sous François Hollande, qui explique leur surprenante modération après la révélation de leur mise sur écoute par la NSA. Une vaste entreprise française d'espionnage que la loi sur le renseignement, adoptée le 24 juin, vient de légaliser en catimini.
Cette histoire de l'ombre, « L'Obs » a pu la reconstituer grâce aux témoignages anonymes de plusieurs responsables actuels et passés. Il y est question de stations clandestines installées par la DGSE sur les côtes françaises pour « écouter » les câbles sous-marins, de la complicité de grandes entreprises hexagonales, des accords secrets entre le service français et ses homologues anglo-saxons et de l'indigence du contrôle parlementaire…

La France à la traîne
L'affaire commence début janvier 2008, dans le bureau du chef de l'Etat, à l'Elysée. Nicolas Sarkozy a réuni le Premier ministre, François Fillon, le patron de la DGSE, Pierre Brochand, et quelques collaborateurs. Au menu : l'avenir des services spéciaux français. Leur problème ? Ils sont devenus (presque) sourds. Ils ont de plus en plus de mal à écouter les communications mondiales…
Lire la suite….

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

Source : http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html?cm_mmc=EMV-_-NO-_-20150701_NLNOACTU08H-_-exclusif-comment-la-france-ecoute-aussi-le-monde#xtor=EPR-1-Actu8h-20150701

Défendre la loi renseignement et s’indigner de la surveillance de la NSA, c’est possible | Le Net Expert Informatique

Défendre la loi renseignement et s’indigner de la surveillance de la NSA, c’est possible

Des hommes et femmes politiques qui avaient voté la loi renseignement se sont émus après les révélations de Wikileaks de la surveillance opérée par l'agence américaine NSA. Sans peur de la contradiction.

Trois présidents sur écoute. Libération et Médiapart ont publié ce 23 juin des documents de Wikileaks qui indiquent que la NSA a réussi à écouter au moins trois présidents, Jacques Chirac, Nicolas Sarkozy et François Hollande, au moins entre 2002 et 2012.
Ces révélations sont arrivés la veille de l'adoption définitive par le Parlement du projet de loi sur le renseignement, qui, comme le rappelle Le Lab, «légalise des pratiques contestables des services [de renseignement], selon ses détracteurs».

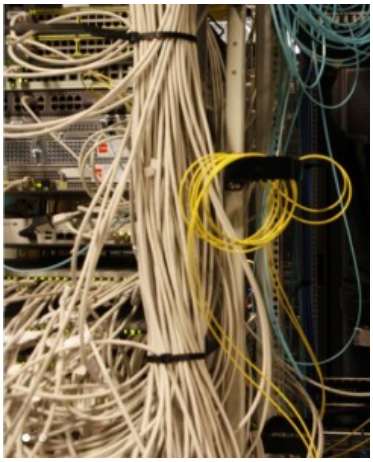
Certains n'ont donc pas manqué de souligner l'ironie de la situation:
Les mesures de surveillances internationales #PJLRenseignement permettront de faire ce que le PS dénonce http://t.co/x8ITr9YBxq #FranceLeaks
Pour @fhollande @manuelvalls @BCazeneuve, être écoutés, ce n'est pas grave, ils n'ont rien à cacher… #Franceleaks #PJLRenseignement
Et le ministère de l'Intérieur lui-même a bien vu le problème, regrettant la date de parution des révélations de Wikileaks, susceptibles selon lui de «créer un amalgame» avec le projet de loi renseignement.

Source : https://fr.news.yahoo.com/d%C3%A9fendre-loi-renseignement-sindigner-surveillance-nsa-cest-possible-170902346.html

---

Le business des écoutes et

des données personnelles | POLICEtcetera | Le Net Expert Informatique



Le business des écoutes et des données personnelles

Au moment où les États-Unis sont en train – timidement – de faire machine arrière sur le Patriot Act, la France se dote d'une véritable armada de machines électroniques pour surveiller ses propres ressortissants – et à l'occasion, les étrangers de passage dans notre beau pays. Dans cette guerre secrète contre le crime et le terrorisme, qui s'est amplifiée ces dernières années, pas de chars, pas d'avions, pas d'armes, mais un chiffre d'affaires en pleine érection. On peut se demander à qui profite le crime et combien cela va nous coûter… Dans quelle poche va-t-on prendre les sous ? Au détriment de quels services publics ?…

Nous sommes tellement habitués à ces projets qui capotent, comme Ecomouv ; ou d'autres qui aboutissent, mais dont la facture a été multipliée par 2, 3, 4…
Tiens, par exemple, parlons de la plateforme nationale d'interceptions judiciaires (PNIJ). En 2007, il était question d'une enveloppe de 17 millions d'euros. En 2010, elle était de 42 millions, et en 2014, de 47. En cette année 2015, alors que les premiers essais ont commencé dans certains services de police et de gendarmerie sur le ressort des cours d'appel de Paris, Versailles et Rouen, on se rapprocherait des 55 millions. C'est du moins ce que dit Le Canard enchaîné daté du 20 mai 2015, ajoutant malicieusement, que, pour l'instant, seuls les clients d'Orange peuvent être mis sous écoute.
En fait, l'addition sera beaucoup plus lourde, car, parallèlement, les fournisseurs d'accès à Internet ont dû effectuer des travaux et notamment déployer des fibres optiques jusqu'à Élancourt, dans les Yvelines, sur le site de Thales qui accueille la PNIJ. Il faut également revoir les réseaux des services de police, de gendarmerie, des douanes… Lors du jeu de questions à l'Assemblée Nationale, le député Alain Tourret a avancé un surplus de 50 millions. Il n'a obtenu ni confirmation ni infirmation de ce chiffre, la garde des Sceaux se contentant de dire qu'il était prévu que le ministère de l'Intérieur participe au pot commun.
Et l'addition n'est pas close, car il pourrait se révéler nécessaire de renforcer la sécurité de la PNIJ. On se souvient des propos tenus lors du débat sur la loi sur le renseignement : la centralisation des données dans un même lieu géographique « pourrait constituer une source de vulnérabilité importante ». La centralisation nationale des réquisitions judiciaires constitue donc une faiblesse dans la sécurité, ce que policiers et magistrats n'ont cessé de clamer depuis que l'idée est dans l'air. D'autant que cette plateforme, contrairement à ce que son nom peut laisser penser, n'est pas seulement destinée à intercepter les communications téléphoniques : c'est un système complet de traitement automatisé de données à caractère personnel. Une machine qui va brasser et enregistrer les données personnelles de toutes les personnes impliquées ou suspectées dans une affaire judiciaire.
Une caverne d'Ali Baba sur laquelle les services de renseignement, français ou étrangers, vont forcément loucher. À ce sujet, on peut d'ailleurs s'interroger sur la portée exacte de l'amendement de dernière minute (un de plus) présenté par le gouvernement à la loi sur le renseignement : les services habilités pourront avoir accès aux traitements automatisés de données à caractère personnel, y compris celles des procédures judiciaires en cours. Il s'agit pour ces services, nous dit-on, de pouvoir consulter le TAJ, c'est-à-dire le fichier d'antécédents judiciaires (qui a remplacé le STIC de la police et le JUDEX de la gendarmerie). Mais alors, pourquoi ce pluriel dans l'article L.234 : « pourront avoir accès aux traitements automatisés… » Cela vise-t-il également le fichier Cassiopée du ministère de la Justice et la PNIJ ?
Je vais finir parano !
Lire la suite….

Source : http://moreas.blog.lemonde.fr/2015/06/21/le-business-des-ecoutes-et-des-donnees-personnelles
par G.Moréas

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

Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai | Le Net Expert Informatique

Loi «Renseignement» : Ce que vous avez vu dans les séries TV pourrait bien se passer en vrai

Quand la réalité rejoint la fiction. Le projet de loi renseignement, qui va être défendu par le gouvernement dans l'hémicycle du Sénat à partir de ce mardi, va « légaliser » certaines pratiques déjà utilisées par les services de renseignement. Les données récupérées avec ces nouveaux outils vont pouvoir être versées au dossier judiciaire des suspects.

Loi «Renseignement»: Les séries TV savent ce… *par 20Minutes*

Si elle fait l'objet d'un large consensus parmi la majorité des parlementaires, cette loi est contestée par les sénateurs communistes qui ont déposé une série d'amendements de suppression et ont dénoncé un risque de « surveillance de masse ». La plupart des techniques sur le point d'être légalisées sont déjà utilisées. Et diffusées dans les séries TV. Florilège…

Poser un mouchard sous une voiture
Dans Breaking Bad (Episode 9, Saison 5), Walt accuse Hank qui travaille pour la DEA, la brigade des stupéfiants américaine, d'avoir posé un tracker GPS sous sa voiture. Le projet de loi prévoit l'emploi de balises « permettant de localiser en temps réel un véhicule ou un objet ».

Mettre un appartement sous vidéosurveillance

Dans la deuxième saison de Scandal, l'appartement de l'avocate Olivia Pope est placé sous vidéo-surveillance par Jake Ballard, le fidèle ami du président. Elle s'en rend compte dans le 18e épisode. Des caméras partout, ainsi que des micros quasiment indétectables sont utilisés. Le projet de loi permettra aux services de renseignement d'appliquer ce type d'écoutes. Les policiers passeront cependant à travers le filtre de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Les plus sceptiques regrettent le pouvoir amoindri de cet organe de contrôle.

Géolocaliser un téléphone portable

Dès le premier épisode de la saison 1 du Bureau des Légendes, Cyclone, un des clandestins du BDL, est arrêté à Alger alors qu'il est ivre au volant d'une voiture. Le Bureau des Légendes va s'inquiéter : Cyclone étant musulman pratiquant, il n'aurait pas dû être saoul. Sisteron décide alors de géolocaliser son téléphone portable. Le signal du mobile indique qu'il se trouve bien au commissariat.

Intercepter les métadonnées d'un téléphone
Dans la série américaine Those who kill, Catherine Jensen, experte en tueurs en série, fait appel à un détective de la brigade des stupéfiants pour mettre sur écoute un suspect. Ce dernier, à l'épisode 9 détaille comment les policiers parviennent à récupérer les données enregistrées sur un téléphone portable, en se faisant passer pour une antenne relais après avoir copié la carte sim. Dans la « vraie vie », les policiers utilisent des Imsi-Catchers qui peuvent intercepter dans un rayon donné toutes les données qui transitent via un téléphone. Cette technologie, rendue possible par la loi renseignement, fait pourtant polémique.

Capter un écran d'ordinateur en direct grâce à un logiciel espion
Les experts de CSI : Cyber (saison 1, épisode 1), mettent au point ce qu'ils appellent un RAT (Remote Administration Tool), un outil d'administration à distance. En clair, un programme permettant la prise de contrôle total, à distance, d'un ordinateur depuis un autre ordinateur. Ils y ont introduit un logiciel espion qui permet, en fonction de mots-clés utilisés dans un mail, d'activer une alarme. Ils peuvent aussi capter en direct le mot-clé qui est tapé. Les défenseurs de la liberté numérique dénoncent à travers la loi Renseignement la surveillance massive des ordinateurs des internautes.

Source : http://www.20minutes.fr/societe/1621371-20150602-video-loi-renseignement-vu-series-tv-ca-pourra-passer-vrai
Par William Molinié

Renseignement : le Sénat apporte sa touche au texte | Le Net Expert Informatique

	Renseignement : le Sénat apporte sa touche au texte

Après un vote solennel à l'Assemblée, la commission des lois du Sénat s'est penchée sur le texte du projet de loi Renseignement. Les sénateurs se sont attachés à renforcer les contrôles et limiter certains points du texte.

Si à l'Assemblée, le texte de loi Renseignement était passé comme une lettre à la poste malgré les efforts de rares opposants, il semble que le Sénat ait choisi une approche plus prudente à l'égard de ce projet de loi qui suscite de nombreuses controverses, malgré un apparent consensus dans la majorité et l'opposition.

La commission des lois du Sénat a ainsi adopté pas moins de 145 amendements lors de l'examen du texte, qui avait lieu mercredi et jeudi. Ceux-ci concernent différents aspects du texte et visent, pour la plupart, à renforcer les contrôles et les garanties, sans pour autant changer en profondeur la portée du texte.

Ainsi, les amendements viennent remanier l'article concernant les fameuses boîtes noires, censées être déployées chez les opérateurs afin de procéder à une surveillance automatisée et anonyme du trafic, anonymat qui sera levé sur autorisation du Premier ministre afin d'identifier des individus suspectés de préparer des actes terroristes.

Le délai « d'autorisation des techniques particulières portant sur les données de connexion a été abaissé à deux mois » renouvelables sur autorisation du Premier ministre, contre quatre mois dans la précédente version.

Le Sénat balise le texte

Le Sénat s'est également attaché à limiter l'ampleur de la collecte mise en place grâce à cette technique, en la limitant aux seules métadonnées ainsi qu'en supprimant l'application de la procédure d'urgence. Le gouvernement jugeait le recours à cette procédure « indispensable » mais le Sénat ne semble pas convaincu et recommande donc de s'en tenir au circuit normal, qui comprend l'autorisation par le Premier ministre et un avis de la CNCTR avant le déploiement de ces mesures.

Le Sénat a également renforcé les options de contrôle de la CNCTR : les sénateurs ont clarifié les règles de nomination et de fonctionnement de cette nouvelle commission de contrôle, facilité la possibilité de saisir le Conseil d'État ainsi que les recours à la disposition de la commission lorsque celle-ci découvre la mise en œuvre d'une technique de renseignement qui lui aurait été dissimulé.

Une version remaniée du texte donc, qui apporte de nouvelles garanties à l'égard des mesures détaillées dans ce texte de loi. Le projet doit encore recevoir l'approbation du Senat en séance plénière, à partir du 4 juin. Après cette date, la commission mixte paritaire sera chargée de trouver un texte conciliant les deux versions. Puis interviendra la saisine du Conseil Constitutionnel avant la promulgation du texte par le président de la République.

Source : http://www.zdnet.fr/actualites/renseignement-le-senat-apporte-sa-touche-au-texte-39819704.htm
Par Louis Adam

Skynet, un programme de la NSA. Pour Terminator ? | Le Net Expert Informatique

Skynet, un programme de la NSA. Pour terminator ?

La NSA fabriquerait-elle des Terminators ? Que l'on se rassure : même si l'agence de renseignement possède bien un programme nommé Skynet, il n'a rien à voir avec celui de la célèbre franchise de films.

La NSA possède un programme dénommé Skynet, une dénomination bien évidemment inspirée de celle de l'intelligence artificielle destructrice des films Terminator. Néanmoins, pas de panique : il s'agit d'un protocole d'espionnage destiné à analyser des métadonnées issues de conversations téléphoniques impliquant des personnes soupçonnées d'être des terroristes.
Révélée par le site The Intercept, l'information interpelle en raison du nom du programme, mais ce n'est finalement pas l'élément le plus intéressant mis en avant par l'article. On apprend dans ce dernier qu'un journaliste d'Al Jazeera, Ahmad Muaffaq Zaidan, s'est retrouvé sur la liste des suspects mis sur écoute après avoir réalisé une série d'articles et d'interviews consacrée à Al Qaeda. Les informations, issues de documents révélés par Edward Snowden, mettent donc en avant certains ratés dans ce programme qui utilise comme souvent des algorithmes pour recouper ses informations. Pas toujours efficace. . .

La fiche du journaliste, faussement soupçonné de terrorisme.Le petit frère de MonsterMind

Le Skynet version NSA ne ressemble peut-être pas à celui de Terminator, mais le site Wired ne manque pas de rappeler l'existence d'un autre programme, dévoilé quant à lui en août 2014, et qui lui ressemble davantage : il s'agit de MonsterMind (http://www.clubic.com/antivirus-securite-informatique/prism/actualite-721299-monstermind-antivirus-nsa-riposter-automatiquement.html), un logiciel conçu pour riposter automatiquement face à une cyber-attaque, sans intervention humaine.

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 !

Source : http://www.clubic.com/internet/actualite-766436-nsa-possede-programme-nomme-skynet-terminator-fourni.html?estat_svc=s%3D223023201608%26crmID%3D639453874_974809190