État d’urgence : perquisition dans le cloud et Internet coupé ?

État d’urgence : perquisition dans le cloud et Internet coupé ?

Le projet de loi qui veut mettre à jour les règles en cas d'état d'urgence prévoit d'une part d'autoriser la saisie de fichiers informatiques stockés à distance pendant les perquisitions, d'autre part d'interdire aux assignés à résidence de communiquer avec certaines personnes, et peut-être même sur internet…

Le projet de loi relatif « à l'état d'urgence et renforçant l'efficacité de ses dispositions » a été mis en ligne sur le site de l'Assemblée nationale.
Débattu le jeudi 19 novembre, il a pour but de modifier la loi n° 55-385 du 3 avril 1955 sur l'état d'urgence en le rendant notamment plus adapté aux nouvelles technologies.
Le premier exemple de ce qu'on peut y lire est d'ailleurs parlant. « Il permet enfin l'accès aux données informatiques accessibles depuis le lieu perquisitionné, ainsi que la prise de copies », indique d'abord le texte avant de préciser plus loin que durant une perquisition il sera possible d'accéder aux données dans un système ou un équipement (ordinateur, smartphone, etc.) « dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial ».
Il semble donc que cela concerne les systèmes de stockage à distance lorsque les enquêteurs sont sur place.
Les forces de l'ordre pourront également copier « sur tout support (…) les données auxquelles il aura été possible d'accéder dans les conditions prévues par le présent article ».
Plus loin, le texte précise que « cette rédaction vise les données informatiques telles que celles qui sont présentes dans un ordinateur, celles qui sont accessibles depuis un ordinateur (« nuage »), celles qui sont contenues dans un téléphone… ».
L'article 2 proroge également la possibilité « d'ordonner des perquisitions de jour et de nuit », lit-on encore.

Assignation à résidence = plus d'internet ?
Ces mesures vont de pair avec une autre information contenue dans le document, mais qui est encore à l'heure actuelle peu précise. Il s'agit de prescrire à une personne assignée à résidence l'interdiction « de se trouver en relation, directement ou indirectement, avec certaines personnes nommément désignées dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité et l'ordre publics ».
L'utilisation des termes « directement ou indirectement » laisse planer un certain doute quant à ce que cela peut signifier concrètement. Elle pourrait se traduire par l'interdiction d'utiliser des appareils de communication comme les téléphones ou même Internet. Mais cette dernière disposition paraît délicate à mettre en œuvre dans la mesure où Internet est devenu un droit fondamental en France, et est entré dans les Droits de l'Homme reconnus pas l'ONU.
En revanche, l'état d'urgence permet quant à lui de déroger à certains Droits de l'Homme.

Réagissez à cet article
Source : http://www.linformaticien.com/actualites/id/38575/etat-d-urgence-perquisition-dans-le-cloud-et-internet-coupe.aspx

---

Les auteurs seront-ils passés

à travers les mailles du filet du renseignement ?

Les auteurs seront-ils passés à travers les mailles du filet du renseignement ?

Qu'un « loup solitaire » puisse ne pas être décelé, on peut le comprendre, mais qu'une telle opération, méticuleusement préparée, n'ait pas pu être contrée, peut poser question.

La kyrielle de services mise en place depuis une dizaine d'années nuit-elle à l'efficacité du repérage ?
DGSI (direction générale de la sécurité intérieure), SCRT (service central du renseignement territorial), sans compter direction du renseignement à Paris et autres, on compte 19 entités anti-terroristes en France, alors, qu'à titre de comparaison, le Royaume-Uni n'a que le fameux MI5. Comment croiser ou recroiser les informations ?
Le rapport du sénateur Dominati mettait récemment en lumière de possibles dysfonctionnements liés à cette profusion de services : « Une nouvelle évolution de l'organisation du renseignement intérieur semble inévitable à moyen terme, compte tenu de la fragilité de la situation actuelle », insistait Philippe Dominati.
Les attentats de janvier avaient poussé les autorités à accélérer le recrutement de plusieurs centaines d'agents, la loi sur le renseignement a été adoptée, mais il reste indubitablement des failles. Selon les derniers chiffres du ministère de l'Intérieur, 1700 djihadistes français seraient passés par le Moyen-Orient. Prêts à revenir ?

Source :
http://www.republicain-lorrain.fr/france-monde/2015/11/15/les-auteurs-seront-ils-passes-a-travers-les-mailles-du-filet-du-renseignement

---

La surveillance des communications

internationales validée | Le Net Expert Informatique

	La surveillance des communications internationales validée

Le Parlement a adopté un texte comblant un vide laissé par la loi renseignement. La surveillance des communications internationales impliquera moins de contrôles que celle des interceptions effectuées dans l'Hexagone.

Le débat est clos. Le Parlement a adopté définitivement jeudi 5 novembre par un dernier vote de l'Assemblée la proposition de loi destinée à légaliser la surveillance des communications internationales, qui resteront soumises à moins de contrôles que les interceptions effectuées en France.

Les députés ont voté le texte dans les mêmes termes que les sénateurs un peu plus tôt dans la journée.

Le législateur compétent

La proposition de loi a pour objet de pallier un vide juridique résultant de la censure par le Conseil constitutionnel d'une disposition de la loi renseignement. Celle-ci, qui légalise et encadre l'activité des services en France, était restée floue pour leurs activités à l'étranger, renvoyant cela à un décret en Conseil d'État.

Mais le Conseil constitutionnel a jugé que c'était au législateur d'agir dès lors que des libertés publiques étaient concernées.

Une autorisation du Premier ministre

Les auteurs du texte, les députés socialistes Patricia Adam et Philippe Nauche, respectivement présidente et vice-président de la commission de la Défense à l'Assemblée, ont proposé un cadre juridique spécifique en introduisant un nouveau chapitre dans le code de la sécurité intérieure.

Dès lors que « la défense et la promotion des intérêts fondamentaux de la Nation », qui comprennent notamment « les intérêts économiques, industriels et scientifiques majeurs » de la France, sont concernées, « la surveillance des communications qui sont émises ou reçues de l'étranger » est autorisée et le Premier ministre pourra « désigner les zones géographiques, les organisations ou les personnes objets de cette surveillance ».

Moins de contrôles

Ces interceptions à l'étranger seront nettement moins encadrées que celles effectuées en France. Le Premier ministre n'aura pas besoin de solliciter l'avis préalable de la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR).

Sur proposition du Sénat, la commission mixte paritaire a retiré au Premier ministre la faculté de déléguer à un collaborateur la désignation des réseaux de communications électroniques internationales sur lesquels l'interception est autorisée.

Source :
http://www.latribune.fr/economie/france/la-surveillance-des-communications-internationales-validee-par-le-parlement-520191.html

Le secret professionnel des avocats menacé par la Loi renseignement ? | Le Net Expert Informatique

Le Conseil de l'ordre des avocats de Paris va saisir la Cour européenne des droits de l'Homme (CEDH) contre la loi controversée sur le renseignement. | AFP	**Le secret professionnel des avocats menacé par la Loi renseignement ?**

Le Conseil de l'ordre des avocats de Paris va saisir la Cour européenne des droits de l'Homme (CEDH) contre la loi controversée sur le renseignement.

« Nous allons saisir la CEDH contre cette loi qui repose à nos yeux sur deux mensonges d'État », a expliqué vendredi le bâtonnier de Paris Pierre-Olivier Sur, confirmant une information du site Next INpact.

« Le premier mensonge, c'est que cette loi ne vise pas simplement à protéger la société contre le terrorisme, elle concerne toute la matière pénale. Le second, c'est qu'il n'y a pas dans le texte de véritable juge pour protéger les libertés publiques car le seul juge habilité à le faire, c'est le juge judiciaire. Et le législateur a choisi un juge administratif, très éloigné des questions de liberté », a-t-il fait valoir.

« Ce secret professionnel a une valeur sacrée »

Pour le représentant des avocats parisiens, la loi sur le renseignement porte également atteinte « au secret professionnel des avocats ».

« Ce secret professionnel a une valeur sacrée. Il ne place pas l'avocat au-dessus des lois mais on doit prendre en compte la spécificité de son travail, ne pas aller chercher, en fracturant le secret, des renseignements sur des actes qu'il aurait pu commettre et qui, par capillarité, risque de nuire à la défense de son client. Il faut donc que les premiers actes d'investigation soient particulièrement contrôlés, notamment par le président du TGI », a-t-il fait valoir.

Cette saisine intervient quelques jours après celle de l'Association de la presse judiciaire (APJ) qui estimait, elle, que la loi sur le renseignement menaçait la liberté de la presse et le secret des sources.

Ecoutes, caméras, logiciel-espion…

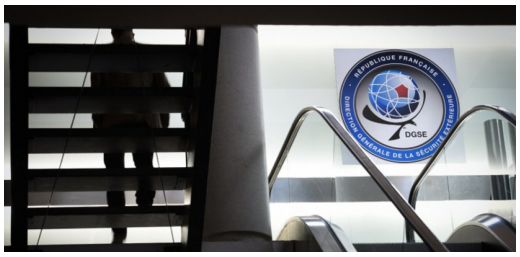
De la prévention d'attentats à l'espionnage économique, le texte définit un large éventail des missions des services de renseignement ainsi que le régime d'autorisation et de contrôle de techniques d'espionnage (écoutes, pose de caméra ou de logiciel-espion, installation chez les opérateurs de télécommunications de dispositifs pour collecter les données de connexion, etc.).

Fin juin, le Parlement a adopté définitivement la loi à une large majorité gauche-droite, mais avec des voix dissidentes dans presque chaque groupe.

Face à la controverse, François Hollande a saisi le Conseil constitutionnel. Ce dernier a validé la loi en juillet estimant notamment que « le législateur (avait) prévu des garanties suffisantes pour qu'il ne résulte pas » du texte contesté « une atteinte disproportionnée au droit au respect de la vie privée, au droit de la défense et au droit à un procès équitable, y compris pour les avocats et les journalistes ».

Source :
http://www.ouest-france.fr/loi-renseignement-le-secret-professionnel-des-avocats-menace-3752413

En exclusivité, la nouvelle loi sur les écoutes de la DGSE – L'Obs | Le Net Expert Informatique



En exclusivité, la nouvelle loi sur les écoutes de la DGSE

La commission de la Défense de l'Assemblée Nationale rendra publique, jeudi 10 septembre, une proposition de loi très sensible dont « L'Obs » a pu se procurer le texte. Celui-ci définit les modalités d'autorisation et de contrôle des écoutes internationales de la DGSE et de ce fait les légalise pour la première fois.

Cette proposition de loi (dite « relative aux mesures de surveillance des communications électroniques internationales ») fait suite au rejet, le 23 juillet, par le Conseil Constitutionnel des dispositions sur le même sujet inscrites dans la loi sur le renseignement.

L'article avait été retoqué par les Sages au motif notamment qu'il renvoyait à un décret secret (dont « l'Obs » avait révélé l'existence). La représentation nationale n'avait donc pas une idée assez précise du fonctionnement de ces grandes oreilles ni de leur contrôle. Cette nouvelle proposition de loi répond, semble-t-il, à l'exigence de (relative) transparence formulée par le Conseil Constitutionnel.

La proposition de loi apporte les clarifications suivantes :

La France préservée

Il est redit qu'il s'agit des communications « émises ou reçues de l'étranger » et que la DGSE ne peut cibler la France. Plus précisément, le texte stipule que si, du fait du trajet aléatoire des signaux électroniques, le service de renseignement intercepte des communications échangées entre personnes ou équipement « utilisant des numéros d'abonnement ou des identifiants rattachables au territoire national, y compris lorsque ces communications transitent par des équipements non rattachables à ce territoire, ces interceptions sont instantanément détruites. »

Le Premier ministre au centre du dispositif

Cet article est le plus important pour la DGSE. Il stipule que la décision générale d'écouter tel ou tel « système de communication » revient au Premier ministre qui en assume donc la responsabilité. Autrement dit, c'est le chef du gouvernement qui désormais autorise l'interception des flux provenant des satellites de communication et des câbles sous-marins.

Cette disposition oblige également la DGSE à obtenir l'autorisation des Premiers ministres futurs si elle veut écouter de nouveaux moyens de communication. Le but est notamment d'éviter que ne se reproduise l'épisode de 2008. A l'époque, la loi ne permettait pas à la DGSE d'écouter les câbles sous-marins. Pour passer outre, elle avait obtenu à l'insu de la représentation nationale la signature du décret secret évoqué dans la précédente mouture de la loi.

Le big data légalisé

Le Premier ministre « autorise l'exploitation non individualisée des données de connexion interceptées ». Il s'agit de la reconnaissance publique que la DGSE intercepte des flux et pas seulement des communications individuelles et qu'elle analyse les « big data » ainsi récoltées. Le texte ajoute que « ces autorisations [délivrées pour un an] déterminent la ou les finalités poursuivies ainsi que les types de traitements automatisés pouvant être mis en œuvre. »

Les pays cibles des grandes oreilles

Le paragraphe le plus novateur stipule que le Premier ministre autorise l'écoute de « zones géographiques [donc des pays ou des régions] », d' »organisations », de « personnes » ou de « groupes de personnes ». C'est la première fois qu'un texte officiel confirme que la France écoute elle aussi le monde, que la DGSE agit comme la NSA (avec, certes, moins de moyens). On remarquera que le législateur n'interdit pas l'écoute de dirigeants étrangers, ennemis ou amis…

Contrôle théorique

La Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) « dispose d'un accès permanent, complet et direct aux renseignements collectés, aux transcriptions et extractions réalisées […] et peut contrôler à sa demande les dispositifs techniques ». Sur le papier, les écoutes de la DGSE sont donc bien contrôlées. Tout dépendra des moyens dont la future CNCTR va disposer.

Destruction possible

La CNCTR peut recommander au Premier ministre la destruction d'écoutes non conformes. Si celui-ci refuse, elle peut saisir le Conseil d'Etat pour trancher. Une disposition originale.

Recours individuel

Comme pour les écoutes intérieures, « toute personne souhaitant vérifier qu'aucune mesure de surveillance [par la DGSE] n'est irrégulièrement mise en œuvre à son égard » peut saisir la CNCTR. Celle-ci notifie à la personne en question qu'il a procédé aux vérifications nécessaires « sans confirmer ou infirmer la mise en œuvre de mesures de surveillance ».

Délais de conservation

La loi définit des délais de conservation des interceptions qui s'étalent entre un an pour les communications à huit pour les renseignements chiffrés en passant par six pour les données de connexion.

Le texte du projet de loi :
proposition loi surveillance publié par NouvelObs.com

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://tempsreel.nouvelobs.com/monde/20150909.OBS5547/exclusif-la-nouvelle-loi-sur-les-ecoutes-de-la-dgse.html
Par Vincent Jauvert

Écoutes : la mise en place de la PNIJ avance doucement | Le Net Expert Informatique

Écoutes : la mise en place de la PNIJ avance doucement

Interpelé par un député qui se plaignait de la lenteur des procédures de réquisition effectuées auprès des opérateurs de téléphonie mobile, le ministre de l'Intérieur vient de donner quelques nouvelles de la Plateforme nationale des interceptions judiciaires (PNIJ), qui n'en finit pas d'accumuler du retard.

Initialement prévue pour fin 2013, la PNIJ n'est toujours pas opérationnelle. Cet énorme centre, placé dans les locaux du géant Thales, était pourtant censé faciliter le travail des enquêteurs – même si ce n'est pas l'avis de ses détracteurs. Autorisée par un décret publié en octobre au Journal officiel, cette plateforme doit en effet permettre de centraliser les nombreuses interceptions de correspondances ordonnées par la justice, de même que les réquisitions de données de connexion (quel abonné derrière telle adresse IP ou numéro de téléphone, etc).
Aujourd'hui, pour identifier un client d'Orange ou SFR, les réquisitions « sont transmises par les moyens de communication classiques – principalement le fax – et traitées par les employés des services des obligations légales des différentes sociétés », reconnaît ainsi le ministre de l'Intérieur au travers d'une réponse à une question écrite du député Jean-Luc Bleunven. Si le Code de procédure pénale permet théoriquement aux opérateurs de répondre à ces réquisitions par voie électronique, le locataire de la Place Beauvau explique qu'en pratique, ce n'est pas encore totalement le cas, en raison des retards de la PNIJ.

Une expérimentation menée depuis février en vue des identifications d'abonnés
Bernard Cazeneuve indique toutefois que des « protocoles » permettant de « mettre en place un système de réponse automatisé aux demandes de l'autorité judiciaire » a été signé « récemment » avec les quatre principaux opérateurs de téléphonie : Orange, SFR, Bouygues et Free. « L'expérimentation de la PNIJ sur ce point est en cours depuis le 9 février 2015 dans certains services d'enquête » poursuit le ministre de l'Intérieur. Selon lui, « les résultats sont extrêmement probants : les réponses aux réquisitions dont les opérateurs ont automatisé le traitement sont obtenues par les services d'enquête en quelques minutes contre plusieurs jours ou semaines auparavant ».
Restera maintenant à voir quand cette expérimentation limitée à quelques « services d'enquête » sera généralisée… Point sur lequel ne s'avance pas le premier flic de France.

Source : http://www.nextinpact.com/news/96181-ecoutes-mise-en-place-pnij-avance-doucement.htm
Par Xavier Berne

Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés) | Le Net Expert Informatique

Après les yeux, les oreilles Crédits : alphaspirit/iStock/Thinkstock	Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés)

Journal officiel, un arrêté vient encadrer, sous l'œil de l'ANSSI, la définition des mouchards que les juges peuvent désormais utiliser pour faire espionner non seulement les données saisies au clavier ou affichées sur l'écran, mais également celles « reçues et émises par des périphériques audiovisuels ».

En 2011, la loi d'orientation et de programmation pour la sécurité intérieure (LOPPSI) avait permis à la police, sur autorisation d'un juge, la mise en place de mouchard, même à distance. L'enjeu ? Enregistrer les frappes au clavier (keylogger) ou les images affichées sur un écran afin d'espérer glaner quelques preuves, dans le cadre d'enquête pour des infractions sérieuses (criminalité organisée, terrorisme).
Seulement, il y avait un trou dans la raquette. En visant les données affichées « sur un écran » ou celles introduites « par saisie de caractères », le texte initial excluait mécaniquement la captation de parole. Une lacune très contrariante pour qui veut épier une conversation sur Skype par exemple.

La loi contre le terrorisme et Skype
La loi contre le terrorisme de novembre 2014 a comblé la faille. Depuis, non seulement les données saisies au clavier peuvent être espionnées judiciairement, mais également celles « reçues et émises par des périphériques audiovisuels ». La rustine se trouve à l'article 706-102-1 du Code de procédure pénale.
Toutefois encore, une dernière étape manquait pour parfaire ce système. Un autre article, le 226-3 du Code pénal, soumet ces armes de surveillance intrusive à un arrêté du Premier ministre, épaulé par le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son objet ? Dresser la liste de ces outils sensibles dont est autorisée la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente. Sans ce feu vert, ces mêmes opérations, susceptibles de générer des atteintes à la vie privée ou au secret des correspondances, sont en effet sanctionnées de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Cet arrêté du 4 juillet 2012 « fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal » n'avait pas non plus été mis à jour depuis la loi contre le terrorisme. Cet oubli empêchait donc la commercialisation sous contrôle de mouchards de nouvelle génération.
Ce nouveau manque a été corrigé aujourd'hui au Journal officiel. Le Premier ministre a en effet complété le texte de 2012 en y remplaçant l'expression « ou telles qu'il les y introduit par saisie de caractères » par les mots « telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». Sous l'œil de l'ANSSI, certains espiogiciels capables de surveiller Skype (et assimilés) peuvent donc maintenant être introduits en France et utilisés par les services autorisés.

De la surveillance judiciaire à la surveillance administrative
Rappelons au passage que le projet de loi Renseignement permet elle aussi la captation des données informatiques dans un cadre cette fois strictement administratif. Donc sans juge. La même loi s'est servie de l'article 226-3 du Code pénal pour également étendre l'aspiration des métadonnées.
Pour la poursuite de finalités jugées très floues, les services du renseignement pourront en effet utiliser l'ensemble des appareils mentionnés à cet article, afin de moissonner « les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ». Cet arsenal (IMSI catcher, mais pas seulement) pourra par exemple être utilisé pour connaître « directement » les données générées par un smartphone, situé à proximité d'un point déterminé.

Source :
http://www.nextinpact.com/news/95893-au-journal-officiel-encadrement-mouchards-skype-et-assimiles.htm
Par Marc Rees

Inquiétude sur les données de connexion | Le Net Expert Informatique

Inquiétude sur les données de connexion

C'est, pour le Conseil constitutionnel, un petit tour de chauffe avant sa décision, vendredi 24 juillet, sur la loi renseignement, un mois après avoir été saisi par le président de la République et 106 parlementaires. Le Conseil examinait en effet, mardi 21 juillet, une question prioritaire de constitutionnalité (QPC), transmise par le Conseil d'Etat, sur la délicate surveillance des données Internet.

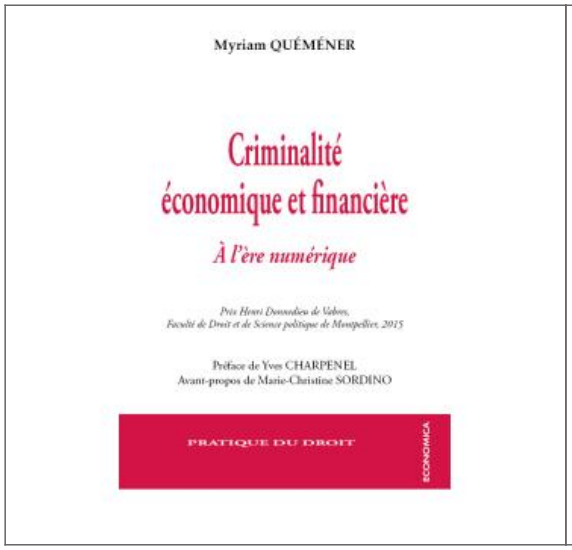
Trois associations (French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs) attaquaient un article décisif, repris par la loi renseignement, de la loi de programmation militaire de décembre 2013 sur « l'accès administratif [policier] aux données de connexion » qu'elles jugent contraire « aux droits au respect de la vie privée, à un procès équitable et à la liberté de communication ».
Les associations s'inquiètent d'une mesure, introduite dans le code de la sécurité intérieure, qui autorise « le recueil, auprès des opérateurs de communications électroniques, (…) des informations et documents traités ou conservés par leurs réseaux ».

Que sont exactement ces « informations et documents » ? Les données de connexion ? Le contenu des correspondances ?
La loi ne le dit pas et a donc, pour les associations, délégué au pouvoir réglementaire – à l'administration – le soin de faire pour le mieux. Ça ne se fait pas. Le Conseil constitutionnel supporte mal de voir « reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination…
Lire la suite….

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

Source : http://www.lemonde.fr/societe/article/2015/07/22/inquietude-sur-les-donnees-de-connexion_4693599_3224.html
Par Franck Johannès

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

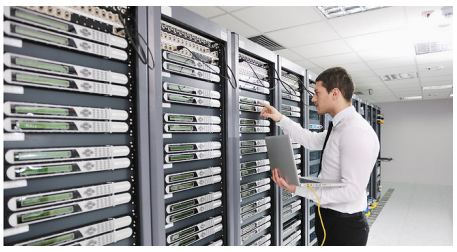
Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

Des datacenters Helvétiques très discrets | Le Net Expert Informatique



Des datacenters Helvétiques très discrets

Pas d'opération clean data à l'horizon grâce à l'ipséité du droit suisse, mais plutôt un data shopping auquel se livrent les entreprises du monde entier. Avec une réglementation aussi exigeante que celle l'Union européenne, mais sans la surveillance tous azimuts des citoyens, la Suisse attire les sociétés désireuses de protéger leurs données dans un havre de sécurité et de secret.

Une protection des données à caractère personnel équivalente à celle de l'Union européenne

Le droit suisse de la protection des données personnelles repose sur la loi fédérale 235.1 de 1992 par l'Assemblée fédérale de la Confédération suisse (ou LPD). Les similitudes avec le droit européen sont nombreuses tant dans son champ d'application (définition des données à caractère personnel et statut particulier des données sensibles telles que les données de santé), que dans ses principes : licéité de la collecte des données et de leur traitement, bonne foi, proportionnalité, finalité, exactitude, sécurité et droits d'accès (art.4 à 25 LPD).

Ceci résulte des accords de Schengen et de Dublin, en vertu desquels la Suisse doit reprendre le droit pertinent de l'UE, y compris en matière de protection des données personnelles. Le droit suisse de la protection des données personnelles est d'ailleurs reconnu adéquat au sens de la directive 95/46/CE par la Commission européenne depuis 15 ans (décision n°2000/5/8/CE). Les garanties sont donc bien plus solides que celles offertes par le droit américain qui ne bénéficie que d'un accord de Safe Harbor (les entreprises américaines qui veulent recevoir des données de l'UE doivent y adhérer).

La Suisse préserve le secret digital

La valeur ajoutée de la Confédération réside dans le fait qu'elle se refuse à exercer tout contrôle administratif sur les données stockées tel qu'il existe aux US avec le Patriot Act et en France avec la Loi de Programmation Militaire qui permet de requérir l'accès à des informations de connexion ou à la localisation des équipements terminaux utilisés ou encore avec le Projet de loi français relatif au renseignement déposé à l'Assemblée nationale le 19 mars 2015. De tels mécanismes poussent les entreprises à faire héberger leurs données hors des territoires américain et français.

La Confédération helvétique, bien au contraire, n'autorise la levée du secret que sur ordre judiciaire et garantit ainsi le respect du principe démocratique. Le juge suisse utilise d'ailleurs la jurisprudence européenne en matière de protection des données personnelles pour justifier ses propres considérants (affaire Logistep, 2010). La Suisse maintient ainsi un niveau de protection des données à caractère personnel équivalent au droit de l'UE tout en respectant les libertés individuelles.

Enfin, une nouvelle génération de datacenter écologiques a récemment été récompensée par le Prix du développement durable afin de promouvoir auprès des clients, partenaires, fournisseurs et des collaborateurs une gouvernance intégrant l'éthique et des valeurs de responsabilité sociale (engagements autour de thématiques telles que l'énergie, la mobilité, la politique d'achat et la gestion des déchets). Or, les entreprises doivent réaliser un audit énergétique de leurs activités avant le 5 décembre 2015. Une raison de plus d'exiler ses données vers la Confédération.

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-134577-lexil-des-datacenters-vers-la-confederation-helvetique-1135913.php
Par Nathalie Devillier / Docteur en Droit – Grenoble Ecole de Management