Big Data ou Big Brother ? la raison du numérique sur France Inter | Le Net Expert Informatique

	Big Data ou Big Brother ? la raison du numérique sur France Inter

Emission « Un jour dans le monde » sur France Inter du mardi 5 mai 2015

Data, smartphones, GoogleGlass, Data marketing, SmartCities, QuantifiedSelf… autant d'expressions nébuleuses que de chiffres, que de données(data).

Maintenant qu'il est sortit de sa caverne, l'Homme veut contrôler, veut savoir. Et tout savoir. A coup de lunettes magiques, de montres multifonctions, d'abribus connectés, de capteurs géolocalisés, l'ère du numérique comme on l'appelle, met à notre disposition, mais surtout nous impose, des moyens de prises sur notre vie, sur la réalité. Et ceci en temps réel.

La vie algorithmique : critique de la raison numérique © l'Echappée – 2015

Dans la smartCity (la ville intelligente), il ne semblera bientôt plus possible d'attendre en vain son autobus, ou d'être surprit par une panne de batterie. Les nouveaux abribus mettent à la disposition du citoyen des moyens de se recharger tout en envoyant un mail grâce à un wifi desservi dans l'ensemble de la ville. Par exemple.
Plus de surprise, donc plus de problème ? Ces nouveaux usages visent en effet à mettre en place une vie meilleure, plus smart (intelligente), où il est possible de tout maîtriser. Une vie « augmentée » comme on dit, enrichie. Mais enrichie pour qui ? Et pour quoi ? Ne sera t-il bientôt plus autorisé de lâcher prise, de s'oublier, un temps ?
Des pulsations du coeur, au nombre de calories ingérées, en passant par la proportion d'amis en commun avec nos voisins, notre vie est chiffrée, répertoriée, traitée, analysée…

Big Brother is watching you © – 2015

Eric Sadin est l'invité d'Un jour dans le monde. Son dernier livre, La vie algorithmique (Editions l'échappée) revient sur ces nouvelles technologies qui nous donnent l'impression de contrôler le réel. Pour nous rendre service. Mais Eric Sadin soulève une question cruciale, alors que la loi sur le renseignement doit être votée aujourd'hui à l'assemblée, ne sommes-nous pas en train de confondre l'ère du Big Data, avec l'ère de Big Brother ?

Emission du mardi 5 mai 2015 sur France Inter

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

Source : http://www.franceinter.fr/emission-un-jour-dans-le-monde-big-data-ou-big-brother-la-raison-du-numerique

Point de vue : d’un hébergeur / FAI sur la loi renseignement | Le Net Expert Informatique

	Point de vue : d’un hébergeur / FAI sur la loi renseignement

Mardi 5 mai, les députés ont voté l'adoption de la loi renseignement par 438 voix pour et 86 contre. En attendant la suite du processus législatif, Octave Klaba, fondateur et Chairman d'OVH, revient en détail sur les conséquences réelles de cette loi, pour les hébergeurs, les FAI et leurs clients.

OVH a menacé de s'exiler hors de France, si la loi renseignement était adoptée. La loi vient d'être votée par l'Assemblée nationale. Qu'allez-vous faire maintenant ?
Je souhaite d'abord m'exprimer sur la loi elle-même. Cette loi n'est pas bonne pour notre pays. Pourquoi ?
Parce qu'elle va changer nos comportements, notre manière de vivre au quotidien, notamment lorsqu'on utilise les téléphones et l'Internet. Nous allons avoir le sentiment d'être sur écoute constamment et cela va créer une psychose dans la population. Manuel Valls le Premier ministre disait « Nous sommes en guerre », et effectivement avec la loi renseignement, le stress vient d'être transmis à l'ensemble du pays. En bref, si le gouvernement voulait que la population se sente menacée, c'est réussi. Très rapidement et automatiquement, nous allons intégrer les mécanismes de l'autocensure.
Je pense qu'au contraire, le rôle du gouvernement est de gérer le pays et ses problématiques sans que cela ait un impact sur la population, sans provoquer un changement de nos comportements, sans modifier les habitudes, sans modifier nos libertés acquises ou notre manière de vivre au quotidien. Le gouvernement a décidé de nous lier tous à cet état d'urgence terroriste. C'est un fait. C'est un choix. Personne ne peut plus dire « moi dans mon village je me moque du terrorisme ».
63 % des Français pensent pourtant que cette loi n'est pas dérangeante parce qu'être écouté n'est pas grave quand on n'a rien à se reprocher. Quelles réflexions cela vous inspire-t-il ?
Nous vivons en démocratie. Le plus grand nombre décide pour le pays, les lois sont votées de manière démocratique par des personnes qui ont été élues et auxquelles nous avons décidé de donner le pouvoir. C'est dans ce type de système que nous avons choisi de vivre, il faut le respecter. Ceux qui ne sont pas contents, ceux qui veulent changer le système peuvent s'engager, créer de nouveaux partis politiques, participer à la vie publique et faire en sorte que ce genre de loi ne passe pas. C'est comme ça. Voilà.

Quelles sont les conséquences de cette loi pour les hébergeurs et les datacentres en France ?
OVH avec d'autres hébergeurs (AFHADS, Gandi, IDS, Ikoula, Lomaco, Online) ont alerté le gouvernement que si la loi renseignement passait telle quelle, elle serait extrêmement néfaste pour l'activité économique des datacentres en France. En effet, nous avons des clients qui ne sont pas uniquement français. Aussi notre activité se base sur la confiance que nos clients nous accordent en hébergeant leurs données dans nos datacentres.
Nous avons été invités par le gouvernement à discuter de la loi pendant deux jours. La première journée, il nous a été dit que les intérêts économiques ne primaient pas sur les problématiques antiterroristes. Le gouvernement ne voulait rien changer du tout.
Les choses ont évolué le lendemain et nous avons pu rédiger l'amendement pour l'activité d'hébergement. C'est a minima, c'est-à-dire que la loi n'allait pas être retirée et nous n'avons pas pu y inclure tout ce que nous voulions.
Mais la modification de la loi que nous avons obtenue nous permet aujourd'hui de dire que la loi est compatible avec les datacentres et l'activité d'hébergement.

Pourquoi la loi n'affecte-elle plus votre activité d'hébergeur en France ?
Habituellement c'est le juge qui demande de faire les écoutes. Il envoie une réquisition sur une cible précise et dans le cadre d'une enquête judiciaire. La loi renseignement permet d'effectuer les écoutes hors cadre juridique. Pour l'activité d'hébergeur, nous avons pu encadrer les conditions d'application de cette loi et réduire son champ d'action.

1) La loi s'applique uniquement dans le cadre de la lutte antiterroriste. Elle ne peut pas être appliquée pour d'autres cas, par exemple l'activisme politique. Uniquement pour les problématiques liées au terrorisme.

2) Les demandes doivent être ciblées et précises, comme dans le cadre d'une enquête judiciaire classique. On ne parle donc plus de boîtes noires installées au cœur des datacentres pour écouter toutes les communications, mais on parle d'une demande ciblée et limitée. Par exemple, on doit nous préciser l'IP ou l'e-mail qui doit être écouté. L'écoute est limitée dans le temps à 4 mois, renouvelables.

3) La demande ne peut porter que sur les métadonnées c'est à dire qui communique avec qui. Et donc la demande ne peut pas porter sur le contenu des communications elles-mêmes. Si la demande concerne une IP, les métadonnées consistent en une liste des IP qui se sont connectées sur l'IP écoutée. Si la demande est une boîte d'e-mail, les métadonnées sont une liste des adresses e-mails qui ont communiqué avec la boîte e-mail écoutée.

4) Comme dans le cadre d'une enquête judiciaire, la récupération des métadonnées doit être assurée par l'hébergeur lui-même. Il n'y a donc ni intervention d'une personne extérieure ni installation de boîtes noires au sein de datacentres.

5) L'exécution de la demande ne relève plus du cadre de l'urgence, c'est-à-dire qu'elle doit passer par une commission de contrôle qui doit donner son avis au préalable. Cela veut dire aussi que l'ensemble des documents partagés, les métadonnées, suivent des procédures strictes : tout est écrit et archivé, avec une traçabilité. L'ensemble de ces documents relève du secret Défense.

Donc, il n'y a pas de boîtes noires chez les hébergeurs ?
Non, chez les hébergeurs, il n'y a pas de boîtes noires. Précisons : lorsqu'on parle de boîtes noires, on parle d'écoute massive, permanente et totale. Ce n'est pas du tout le cas pour les hébergeurs.
Nous estimons que l'amendement que nous avons demandé ne règle pas l'ensemble des problèmes. Mais le champ d'application a été bien réduit.

Qu'en est-il pour les fournisseurs d'accès à Internet (FAI) ?
En plus d'être un hébergeur, OVH est aussi un fournisseur d'accès. Les deux activités utilisent deux réseaux séparés et isolés. Pour notre activité de fournisseur d'accès, nous sommes effectivement soumis à l'ensemble de la loi. C'est-à-dire qu'en tant que FAI, on pourra nous demander d'installer des boîtes noires sur notre réseau de FAI. La loi va, en effet, permettre de capter l'ensemble des échanges que la population effectue via les téléphones mobiles et Internet vers l'extérieur : vers les hébergeurs, vers Google, vers Facebook, vers tout.

Le FAI OVH a-t-il des boîtes noires ?
Non, nous n'en avons pas. Pas en tant qu'hébergeur, pas non plus en tant que FAI.
Par contre, techniquement parlant, lorsqu'on crée un réseau Internet, ce réseau passe par des NRA, par des bâtiments, par des villes et il est interconnecté à d'autres réseaux. Parfois, on utilise les réseaux tiers pour connecter nos équipements. Il est possible par exemple d'installer un coupleur sur une fibre optique et de copier, sans être vu, l'ensemble des informations qui passent par cette fibre. Techniquement parlant, on peut donc installer une boîte noire, en secret et à l'insu des fournisseurs d'accès.
Pour se prémunir il faut chiffrer les informations qui circulent entre les équipements avec par exemple la technologie MACsec. Ainsi, même si quelqu'un installe une boîte noire en secret, il ne pourra pas voir le contenu des échanges.
Il faut savoir aussi que, dans le cadre de la loi renseignement, si jamais les communications sont chiffrées par le gestionnaire du réseau, celui-ci pourra être obligé de fournir les clés de chiffrement aux équipes du Renseignement. En d'autres termes, le chiffrement permet d'éviter uniquement l'écoute passive à l'insu des FAI.

Le réseau FAI d'OVH est-il chiffré ?
Oui, mais pas en totalité. Aujourd'hui nous chiffrons une partie du réseau et progressivement nous allons installer le chiffrement sur l'ensemble de notre réseau, entre tous les routeurs et les switches pour éviter l'écoute passive à notre insu.

Finalement, que conseillez-vous à vos clients ?
D'abord, pour nos clients hébergement français et étrangers, il n'y a pas de changements, sauf si le client a une activité terroriste. En dehors de ce cas de figure, l'hébergement en France n'est pas impacté par la loi renseignement et tout continue comme avant.
Héberger les serveurs en dehors de la France n'évitera pas les écoutes chez les FAI français. Les visiteurs français de sites web passeront obligatoirement par ces FAI qui eux sont soumis à la loi renseignement. On peut bien sûr utiliser un VPN pour administrer son serveur mais on ne peut pas obliger 100% des visiteurs de sites web à utiliser un VPN juste pour consulter un site web.
C'est pourquoi OVH ne va pas arrêter ou réduire l'activité de ses datacentres en France. Nous allons poursuivre nos investissements prévus. Ceci dit, OVH a également un plan d'investissements pour la création de datacentres hors de France dans les 12 mois à venir : 3 nouveaux datacentres en Europe et 3 en dehors de l'Europe. L'annonce des pays et des lieux précis sera faite à l'OVH Summit.
Pour notre activité de FAI, nous travaillons sur notre box qui cache quelques bonnes surprises … je vous invite à suivre les annonces du Summit le 24 septembre prochain.

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

Source : http://www.ovh.com/fr/news/articles/a1766.point-vue-ovh-loi-renseignement?pk_campaign=Renseignement&pk_kwd=btn

Pour voler vos empreintes digitales, il suffit de prendre vos mains en photo | Le Net Expert Informatique

Pour voler vos empreintes digitales, il suffit de prendre vos mains en photo

Les hackers du Chaos Computer Club ont démontré comment il était possible de pirater des empreintes digitales à l'aide d'un appareil photo standard.

Depuis qu'Apple a lancé son système d'identification par reconnaissance d'empreintes digitales, le Chaos Computer Club n'a de cesse de démontrer que son système peut être piraté. La plus importante association de hackers européenne a présenté lors de son congrès, une nouvelle méthode de vol d'empreintes à partir de photos prises avec un appareil standard.
Le hacker Jan Krissler, alias « Starbug », a démontré comment il avait réussi à photographier les empreintes de la ministre allemande de la Défense Ursula von der Leyen, lors d'une allocution publique, avec un objectif de 200 mm et à moins de 3 mètres de distance. Selon lui, il est ensuite possible de s'en servir pour berner les lecteurs d'empreintes comme celui d'Apple.
Cette technique évite d'avoir à dérober un objet doté d'une surface polie, comme du verre, touché par la cible. Une nouvelle raison de ne pas accorder à la biométrie une totale confiance.

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

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

Source : http://lexpansion.lexpress.fr/high-tech/pour-voler-vos-empreintes-digitales-il-suffit-de-prendre-vos-mains-en-photo_1636132.html

Surveillance de nos

Métadonnées. C’est à dire ? | Le Net Expert Informatique

	Surveillance de nos Métadonnées. C’est à dire ?

Divers événements récents survenus au Canada et dans d'autres pays nous ont amenés à nous demander si certains organismes gouvernementaux recueillent et utilisent des métadonnées dans le cadre de leurs activités et, le cas échéant, comment ils s'y prennent. Les programmes de collecte de métadonnées aux États Unis et au Canada ont récemment suscité de grands débats dans les médias.

Même si de telles données peuvent être créées et utilisées de façon légale dans le secteur aussi bien public que privé (sous réserve des restrictions et conditions appropriées), il semble y avoir un débat qui persiste sur la nature des métadonnées, ce qu'elles peuvent révéler, et sur le traitement à leur réserver en l'absence d'une disposition législative expresse. Diverses personnes et organisations reconnues continuent de faire valoir que l'on doit établir une distinction entre les métadonnées et le contenu réel des communications et, par conséquent, que les métadonnées sont moins dignes d'être protégées sous l'angle de la vie privée.

De nombreuses sources se sont penchées sur la nature des « métadonnées » et ce qu'elles peuvent révéler

Le Commissariat à la protection de la vie privée du Canada (le Commissariat) a déjà analysé en juillet 2006 les répercussions des métadonnées en lien avec la protection de la vie privée et il a publié une fiche d'information intitulée Les risques associés aux métadonnées. En mai 2013, nous avons également publié un rapport de recherche intitulé Ce qu'une adresse IP peut révéler à votre sujet, qui montre comment la connaissance d'éléments d'information concernant un abonné, notamment le numéro de téléphone et l'adresse IP, peut constituer un point de départ pour retracer les activités en ligne d'une personne. S'appuyant sur ces travaux effectués auparavant par le Commissariat, le présent document propose une analyse technique de ce que peuvent révéler les métadonnées et donne un aperçu de la façon dont les tribunaux ont interprété la notion de métadonnée.

Qu'est ce qu'une « métadonnée »?

Pour simplifier, disons qu'une métadonnée est une donnée qui fournit de l'information sur une autre donnée. Il s'agit en fait des renseignements qui sont générés lorsqu'on utilise la technologie et qui permettent de situer dans leur contexte (qui, quoi, où, quand et comment) diverses activités. Ces activités peuvent aller de la création d'un document à un appel téléphonique en passant par le clavardage. Dans le contexte des communications, les métadonnées fournissent certaines précisions sur la création, la transmission et la diffusion d'un message. À cet égard, les métadonnées peuvent, par exemple, indiquer la date et l'heure où un appel téléphonique a été fait ou le lieu à partir duquel un courriel a été consulté.

On décrit généralement les métadonnées comme de l'information sur un dossier électronique ou numérique, mais la notion de métadonnée est indéniablement vaste. Étant donné que le débat récent sur la nature et la valeur des métadonnées découle de l'interception de métadonnées associées à des communications, le présent document mettra l'accent sur les métadonnées créées par les communications Internet, filaires et sans fil.

Comme nous le verrons ci après, la distinction entre une « communication » ou un « contenu », d'une part, et l'information générée par cette communication ou son contenu ou s'y rapportant, d'autre part, n'est pas si claire.

Quelques exemples de métadonnées dans le contexte des communications

Chaque fois que nous communiquons, des métadonnées sont produites. Qu'il s'agisse d'une conversation en face à face avec une personne, de l'envoi de messages textes, de clavardage ou de conversations téléphoniques, certains renseignements concernant cette communication – autres que la communication en soi – sont produits.

En ce qui concerne les communications par Internet ou par téléphone, voici quelques exemples de métadonnées que peuvent générer certaines activités courantes :

Métadonnées produites

• Numéro de téléphone de l'appelant
• Numéro de téléphone composé
• Numéro de série unique des appareils téléphoniques utilisés
• Heure de l'appel
• Durée de l'appel
• Emplacement de chaque participant
• Numéro de carte d'appel

Activité

Métadonnées produites

• Nom, adresse de courriel et adresse IP de l'expéditeur
• Nom et adresse de courriel du destinataire
• Renseignements sur le transfert via le serveur
• Date, heure et fuseau horaire
• Identifiant unique du courriel et des courriels connexes (identifiant de message)
• Type de contenu et codage
• Dossier de connexion du client de la messagerie avec adresse IP
• Format de l'en-tête du client de la messagerie
• Priorité et catégorie
• Objet du courriel
• Statut du courriel
• Demande de confirmation de lecture

Activité

Métadonnées produites

• Votre nom et les renseignements biographiques indiqués dans votre profil, notamment votre date de naissance, votre ville natale, vos antécédents professionnels et vos centres d'intérêt
• Votre nom d'utilisateur et identifiant unique
• Vos abonnements
• Le lieu où vous vous trouvez
• L'appareil que vous utilisez
• La date et l'heure de l'activité ainsi que le fuseau horaire
• Vos activités, ce que vous aimez, le lieu où vous vous trouvez et les événements auxquels vous assistez

Activité

Métadonnées produites

• Votre nom, le lieu où vous vous trouvez, votre langue, les renseignements biographiques indiqués dans votre profil et votre URL
• La date à laquelle vous avez créé votre compte
• Votre nom d'utilisateur et votre identifiant unique
• Le lieu du gazouillis, la date, l'heure et le fuseau horaire
• Le numéro d'identification unique du gazouillis et celui du gazouillis auquel vous répondez
• Le code d'identification des contributeurs
• Le nombre d'abonnés, d'abonnements et de favoris
• Votre statut en matière de vérification
• L'application qui a servi à l'envoi du gazouillis

Activité

Métadonnées produites

• Les pages que vous visitez, et quand
• Les données sur l'utilisateur et peut être les détails de connexion de l'utilisateur avec la fonction de saisie automatique
• Les adresses URL
• Votre adresse IP, votre fournisseur de services Internet, les détails matériels de votre appareil, la version du système d'exploitation et du navigateur
• Les témoins et données en cache provenant des sites Web
• Vos requêtes de recherche
• Les résultats de recherche qui s'affichent
• Les pages que vous visitez par la suite

Lire la suite….

Conclusion

Tout en prenant acte de l'importance du contexte, les tribunaux ont observé à maintes reprises que les métadonnées peuvent être très révélatrices au sujet d'une personne et appellent une protection sous l'angle de la vie privée.
Les institutions gouvernementales qui recueillent ces renseignements, ou envisagent de le faire, ne peuvent sous estimer l'ampleur de l'information que les métadonnées peuvent révéler au sujet d'un individu. Il en va de même pour les organisations du secteur privé auxquelles on demande de divulguer de telles données aux institutions gouvernementales, y compris les organismes d'application de la loi. Compte tenu de l'omniprésence des métadonnées et des conclusions convaincantes qui peuvent en découler concernant des individus en particulier, les institutions gouvernementales et les organisations du secteur privé doivent baliser leurs activités de collecte et de communication en fonction de méthodes et de normes appropriées qui sont adaptées au niveau de sensibilité potentiel des métadonnées dans des circonstances données.

Source : https://www.priv.gc.ca/information/research-recherche/2014/md_201410_f.asp

Les facilités pour contourner la loi Renseignement | Le Net Expert Informatique

	Les facilités pour contourner la loi Renseignement

Le Projet de loi relatif au Renseignement impose aux hébergeurs et FAI d'installer un dispositif de surveillance de leurs communications, désigné sous le terme générique « boîte noire », pour recueillir les informations et documents « relatifs à des personnes préalablement identifiées comme présentant une menace ». Selon un article du JournalDuNet daté du 30 avril 2015, se référant à l'article 6 de la LCEN, le terme « hébergeur » désigne l'intermédiaire technique qui met à la disposition des tiers les outils permettant de communiquer des informations en ligne. Il peut donc désigner des éditeurs dès lors qu'ils mettent à disposition des espaces de publication « participatifs », édités par les internautes (forums, réseaux sociaux, espaces de commentaires, chronique ou tribune telle que celle-ci, etc.).
Les avis ci-dessous sont rédigés à titre personnel et ne sauraient engager ceux du groupe CCM Benchmark que je dirige (NDLA: société éditrice des sites Journaldunet, CommentCaMarche, Linternaute, etc.).

Jusqu'à ce jour, lorsque des échanges entre individus ont lieu sur un espace de publication hébergé en France, la justice peut à tout moment demander à l'éditeur, sur simple réquisition judiciaire, de lui fournir les données de connexion de l'utilisateur (adresse IP et horodatage) afin de demander l'identification de l'individu auprès de son fournisseur d'accès. Dans la pratique, cela se pratique parfois sans réquisition dans des cas de force majeure, en infraction avec la loi. A partir du moment où il est de notoriété publique que les sites hébergés en France sont équipés d'une boîte noire, il faudrait être un terroriste idiot pour utiliser un espace de discussion hébergé dans un pays ayant installé de tels dispositifs, alors même qu'il existe un grand nombre de services similaires dans des pays n'en ayant pas déployé. Ainsi, l'information qui était jusqu'ici la plupart du temps accessible risque de devenir petit à petit inaccessible aux services de renseignement.
Il restera malgré tout une trace de la connexion chez le FAI me direz-vous ? A partir du moment où des personnes ayant des choses à se reprocher auront besoin de communiquer, pensez-vous qu'ils le feront à découvert ? Evidemment non, il est à la portée de tout le monde d'ouvrir un tunnel crypté vers une connexion située à l'étranger. Toute communication chiffrée (y compris légalement) est dès lors suspecte, ce qui signifie qu'il sera nécessaire de mettre en oeuvre des moyens pour décrypter toutes les communications chiffrées afin d'en vérifier le contenu. Les moyens de cryptologie utilisables en France sont certes soumis à une réglementation spécifique (http://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie), encore faut-il qu'elle soit respectée et on imagine mal des terroristes appliquer à la lettre la réglementation française…
Ainsi, en mettant en place un tel niveau de contrôle des communications, le risque est de faire monter le niveau de sophistication des échanges entre terroristes. Pour peu que la loi soit votée, on peut compter sur le gouvernement pour médiatiser rapidement quelques prises afin d'illustrer la pertinence de la loi. Il est toutefois évident, à terme, que les premières mesures des organisations terroristes consisteront à former leurs membres aux techniques de chiffrement, afin de devenir invisibles sur la toile, alors même que la formation des agents de la force publique prendra des années. L'agilité joue là encore en la faveur des extrémistes.
Il est vrai que l'on ne peut pas rester inactifs face à la menace terroriste, mais une solution clé-en-main basée uniquement sur le numérique et votée en urgence est-elle la meilleure solution ? Certes le projet de Loi permet de mieux encadrer des pratiques qui existaient déjà sans support légal, mais cette Loi risque bien de rendre ces pratiques plus difficiles à mettre en oeuvre, voire caduques. Enfin, sur le fond, la réaction du public suite à l'affaire Charlie Hebdo était sur le thème « Nous n'avons pas peur, nous continuerons à être libre ». Avec ce projet de loi, le message me semble plutôt être « Nous avons peur, mais nous sommes prêts à être moins libres pour y remédier, quitte à ce que cela ne serve à rien ».

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

Source : http://www.journaldunet.com/ebusiness/expert/60824/la-loi-renseignement-sera-contournee.shtml
Par Jean- François Pillou – CCM Benchmark

TVA. Bercy s’attaque aux systèmes informatiques des fraudeurs | Le Net Expert Informatique

	TVA. Bercy s’attaque aux systèmes informatiques des fraudeurs

Depuis ces derniers jours, le ministère de Finances a mené diverses opérations qui visent les systèmes informatiques des entreprises fraudeuses à la TVA.

Une opération ayant mobilisé « une centaine d'agents » de divers services rattachés à Bercy, en liaison avec le ministère de l'Intérieur, a selon un communiqué permis de démanteler « une filière de diffusion d'un programme informatique spécifique dans le secteur pharmaceutique », en procédant à des perquisitions à la fois des locaux de l'éditeur de ce programme informatique, mais aussi de « certains de ses revendeurs et clients utilisateurs ».

Des « conséquences fiscales et juridiques »

Peu avant, la Direction générale des finances publiques (DGFip) avait, toujours selon le communiqué, mené une « opération d'envergure auprès de 200 utilisateurs » d'autres programmes informatiques frauduleux, cette fois dans le commerce de détail.

Il s'agit selon le ministère de la première mise en œuvre de « la nouvelle procédure de contrôle inopiné informatique ». Ces opérations auront des « conséquences fiscales et juridiques », avertit enfin Bercy.

140 milliards d'euros de recette annuelle

La fraude à la TVA, parfois très sophistiquée, coûte cher à l'État français, même si le phénomène est difficile à mesurer.

En 2013, la Commission européenne avait estimé le manque à gagner pour la France à une trentaine de milliards d'euros par an, tandis que le ministère des Finances avait plutôt évoqué un ordre de grandeur de 10 milliards. La taxe sur la valeur ajoutée représente à elle seule la moitié des recettes fiscales de l'État, auquel elle rapporte près de 140 milliards d'euros chaque année.

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

Source : http://www.ouest-france.fr/tva-bercy-sattaque-aux-systemes-informatiques-des-fraudeurs-3378229

Les 5 dangers du projet de loi sur le renseignement | Denis JACOPINI

	**Les 5 dangers du projet de loi sur le renseignement**

Dernière ligne droite pour le projet de loi sur le renseignement. Le vote solennel du texte est prévu ce mardi 5 mai à l'Assemblée, malgré une mobilisation des opposants, lundi soir au Trocadéro, à Paris.
Que dit le texte ? Au fil des débats, les députés ont fait évoluer le projet de loi. « Il a été considérablement enrichi », estime son rapporteur, Jean-Jacques Urvoas (PS), dans une note envoyée aux députés dont « l'Obs » a eu connaissance. Au total, 260 amendements ont été adoptés. Cela répond en partie aux demandes des adversaires du texte, mais ne lève pas toutes les inquiétudes, loin de là.

Ce que l'Assemblée a modifié :
Une commission de contrôle renforcée
Est surtout renforcé « la composition, l'indépendance et les pouvoirs de la [nouvelle] Commission nationale de contrôle des techniques de renseignements » (CNCTR). Celle-ci remplacera l'actuelle Commission nationale des interceptions de sécurité (CNCIS) et, comme réclamé dans « l'Obs » par son actuel président, cette nouvelle instance disposera d'un « accès aux locaux des services, aux dispositifs de traçabilité, aux opérations de transcription, d'une saisine élargie du Conseil d'Etat ». De plus, les renseignements collectés seront bien centralisés par le Groupement interministériel de contrôle (GIC), que « l'Obs » a pu visiter en exclusivité.

Des professions moins exposées
Le texte exclut désormais certaines professions de la procédure d'urgence. Pour les magistrats, les avocats, les journalistes et les parlementaires, les écoutes ne peuvent être mises en œuvre que sur autorisation du Premier ministre, après avis de la commission. (Art. L. 821-7)

Un statut de lanceur d'alerte
De même, un « statut de lanceur d'alerte a été créé afin d'apporter une protection juridique à tout agent souhaitant révéler des illégalités commises ». N'est en revanche pas précisé si ce statut pourra être étendu à tous ceux qui révèlent des illégalités, à la manière d'Edward Snowden sur la NSA.

Les hackers plus fortement sanctionnés
Les députés ont également profité du texte pour renforcer l'arsenal de sanctions contre les hackers. Dans le sillon de la cyberattaque contre TV5 Monde, ils ont décidé de doubler les sanctions pécuniaires pour tout piratage (actuellement puni au maximum de 75.000 euros), voire de les tripler s'il s'agit d'un service de l'Etat.

Un fichier des personnes mises en cause pour terrorisme
Le gouvernement a également profité de cette loi pour créer un nouveau fichier (FIJAIT) qui recensera les noms et adresses de toutes les personnes condamnées ou mises en examen pour terrorisme.

Malgré des améliorations notables du texte, certains points continuent de poser problème.

1 – Le Premier ministre, seul maître à bord
La loi dote les six services de renseignement français de nombreux moyens supplémentaires pour enquêter, et la plupart n'auront plus besoin de l'aval d'un juge. En effet, le Premier ministre se positionne comme seul décisionnaire.
Les autorisations sont délivrées, après avis de la CNCTR, par le Premier ministre », pointe le texte.
Surtout que le Premier ministre pourra passer outre l'avis de la CNCTR, mais devra alors motiver sa décision (et risquer une saisine du Conseil d'Etat). Et tout ceci s'applique, sauf « en cas d'urgence absolue »…

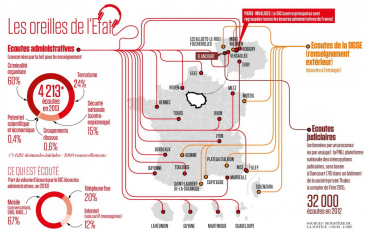
2 – Des données conservées longtemps
Afin de surveiller une personne, le projet de loi prévoit de nombreuses interceptions à distance (e-mails, conversations téléphoniques, SMS…) mais aussi la pose de micros et caméras dans des lieux ou des véhicules. Le texte prévoit que l'ensemble des renseignements ainsi collectés seront détruits au terme de certaines durées :
• 30 jours pour les correspondances,
• 90 jours pour les sonorisations, les géolocalisations et les images vidéo,
• 5 ans pour les données de connexion, aussi appelées métadonnées (qui donnent le détail de qui écrit un e-mail à qui, à quelle heure, etc.).
Et, en cas de cryptage des données, ces délais ne s'appliquent qu' »à compter de leur déchiffrement ».

3 – Eviter de croiser la route d'un suspect
Le projet de loi prévoit que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les « personnes appartenant à [son] entourage » s'il « existe des raisons sérieuses de croire [qu'elles ont] joué un rôle d'intermédiaire, volontaire ou non ». En somme, n'importe qui se trouvant au mauvais endroit, au mauvais moment, et ayant croisé une mauvaise route, pourra être mis sous surveillance.

Lors de la manifestation contre le projet de loi sur le renseignement, le 13 avril (CITIZENSIDE/ANTHONY DEPERRAZ/AFP)

4 – Tous suspects sur internet
Le projet de loi entend mettre à profit les opérateurs internet. Fournisseurs d'accès, moteurs de recherche, réseaux sociaux… Tous pourront fournir « en temps réel » les données techniques de connexion des internautes suspectés de terrorisme. Concrètement, il s'agit de pister une connexion (exprimée par une adresse IP) pour savoir quel site elle a visité, à quelle heure, si elle a envoyé un message Facebook à telle personne, si elle a tapé tel mot clef sur Google…
Le texte souhaite aussi contraindre les opérateurs internet à « mettre en œuvre sur leurs réseaux un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés ». Concrètement, les services de renseignement installeront une « boîte noire » dotée d'un algorithme qui passera au crible l'ensemble du trafic internet pour détecter automatiquement des internautes soupçonnés d'être des terroristes. A terme, cette boîte noire pourra être mise en place chez les fournisseurs d'accès à internet, mais aussi les Américains Google, Facebook, Apple ou Twitter.
L'ensemble du système surveille l'ensemble des internautes de manière anonyme pour détecter des « signaux faibles ». Et, en cas de suspicion, les opérateurs devront dénoncer la personne correspondant aux enquêteurs.
La CNCTR aura accès « au code source » de cette boîte noire afin de limiter la collecte des données aux seuls terroristes. Du moins, tant qu'un décret n'a pas étendu le champ d'action de ce dispositif qui s'apparente à « une surveillance de masse » inspirée par l'agence de renseignement américaine NSA.

5 – Surveiller les terroristes, mais pas seulement
Finalement, il convient de rappeler que, malgré les présentations du texte par François Hollande ou Manuel Valls, il ne s'agit pas d'une loi anti-terroriste, mais bien d'un texte sur le renseignement. Le projet prévoit sept finalités pour recourir aux diverses techniques de renseignement :
• l'indépendance nationale, l'intégrité du territoire et la défense nationale,
• les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère,
• les intérêts économiques, industriels et scientifiques majeurs de la France,
• la prévention du terrorisme,
• la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale ou de la reconstitution de groupements dissous,
• la prévention de la criminalité et de la délinquance organisées,
• la prévention de la prolifération des armes de destructions massives.
Pour rappel, en 2014, 60% des écoutes administratives visaient la criminalité organisée, 24% le terrorisme, 15% la sécurité nationale (contre-espionnage), 0,6% les groupements dissous, et 0,4% la protection du potentiel scientifique et économique. Depuis l'attaque meurtrière contre « Charlie Hebdo », la part dédiée au terrorisme est montée à 48%.



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

Note de Jean-Jacques Urvoas publié par NouvelObs.com

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

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150504.OBS8368/les-5-dangers-du-projet-de-loi-renseignement.html?cm_mmc=EMV-_-NO-_-20150505_NLNOACTU08H-_-les-5-dangers-du-projet-de-loi-renseignement##xtor=EPR-1-Actu8h-20150505
Par Boris Manenti

Loi sur le renseignement ou pratique de la surveillance automatisée ? | Le Net Expert Informatique

Un expert du Big Data m'a adressé ce texte. Il y expose clairement pourquoi, selon lui, la « détection automatisée de comportements suspects » prévue par la Loi Renseignement est très dangereuse. En un mot, mettre les gens dans des cases au moyen d'un algorithme forcément imparfait, ce n'est pas grave s'il ne s'agit que d'envoyer de la publicité ciblée, mais ça l'est beaucoup plus s'il s'agit d'envoyer des policiers interpeller des gens chez eux à 6 heures du matin.

Je vous livre ce texte :
« Depuis plusieurs années je travaille sur le big data appliqué au marketing en ligne. J'ai les mains dans le moteur du matin au soir, et lorsque j'ai appris quelle était la teneur du projet de loi qui devrait être voté le 5 mai prochain, je n'ai pu m'empêcher de frémir en essayant d'imaginer les usages possibles des techniques et des procédés annoncés. Voici quelques réflexions qui me sont venues sur ce dispositif qui pourrait transformer radicalement notre société. Je ne suis pas certain que nos députés aient une idée claire de la boîte de Pandore qu'ils s'apprêtent à ouvrir sur ordre de l'exécutif.
Je me souviens de l'aventure advenue il y a longtemps à l'un de mes oncles, militant fortement engagé dans une association (pacifique) classée franchement à gauche. Il avait vu un jour débarquer chez lui deux personnes des Renseignements Généraux, munies d'un gros dossier qui recensait en détail toutes ses activités. Juste histoire de lui faire comprendre qu'ils savaient qui il était, où il habitait, ce qu'il faisait – pourtant rien d'illégal – et qu'on le tenait à l'oeil. Une simple visite de courtoisie; ou peut-être peut-on appeler ça de l'intimidation? Tout ça s'est passé bien avant la généralisation d'Internet, des fichiers numériques et des téléphones portables. Aujourd'hui, le dossier n'aurait peut-être pas pu être porté sous le bras, ou plutôt si, sur une clé USB, contenant dix ou dix mille fois plus d'informations.
Je me souviens aussi, lorsque j'ai commencé à travailler sur des clusters, du choc que j'ai ressenti la première fois où nous avons tracé une carte utilisant des adresses IP de visiteurs (il est très facile d'obtenir des données géographiques assez fiables pour une adresse IP résidentielle). La carte mettait en évidence de manière saisissante des comportements liés directement à la provenance géographique. Les gens de mon quartier (on était déjà descendus à une échelle plus fine que celle d'une ville) avaient exactement les mêmes comportements que moi; je me suis vu dans la carte. Mon estime en a pris un coup, car j'étais rétrogradé en une seconde au rang de mouton.Mais j'ai réalisé, en regardant ce découpage coloré, à quel point ce nouvel outil nous offrait une puissance et une justesse d'analyse dont nous n'avions même pas rêvé.
Parmi les nombreux problèmes que posent cette loi, se trouve la pose de « boîtes noires » chez les fournisseurs d'accès et les hébergeurs, espionnant potentiellement tout le trafic Internet. Un malentendu assez fréquent est que l'on saura ce que vous faites en inspectant effectivement vos différentes activités en ligne. Qu'on cherchera *individuellement* vos traces d'activité suspecte. Et qu'il vous suffira de visiter quelques sites pour être visé par des investigations plus poussées. Et l'on se dit que l'on n'a rien à craindre, puisqu'on n'a certainement rien de commun avec les terroristes en puissance. Mais ce n'est pas comme ça que ces systèmes fonctionnent.
Pour qu'ils soient efficaces, ils ont besoin de modèles, dont l'utilisation s'apparente à des techniques de pêche au chalut. On attrape tout, on trie, et on garde ce qui est intéressant. Mais comment savoir ce qui est intéressant a priori ? Justement, on ne peut pas vraiment. Ça fonctionne en gros comme ça :

• Première phase, on collecte tout en vrac, sur beaucoup de monde, pendant un moment.
• Deuxième phase, on identifie le groupe d'individus que l'on recherche (mais pas directement, ou en tout cas pas uniquement en utilisant ces données), et on l'indique au système.
• Troisième phase, à partir des données qui ont été collectées sur les membres identifiés de ce groupe, le système fabrique un modèle, selon différentes méthodes.
• Et quatrième phase, on identifie tous les autres, éventuellement vous, qui ne font pas partie du groupe, parce qu'ils se conforment au même modèle.
• On continue à alimenter le système itérativement, on affine le modèle, et on continue.

Dans la pratique, le jugement humain intervient, mais si l'on cherche à étendre ce système, on peut laisser aux machines le soin d'en faire plus, et finalement opérer elles-mêmes le choix des marqueurs d'une activité « suspecte ». C'est à la fois un peu moins inquiétant (vous pouvez continuer sereinement vos recherches de nitrate d'ammonium en ligne si vous êtes agriculteur sans être soupçonné de vouloir fabriquer une bombe) et pire, car à mesure que la quantité de données disparate augmente, il va devenir compliqué de savoir pourquoi une personne a un score élevé dans une catégorie recherchée. Il ne s'agit pas de cases virtuelles que le système coche au fur et à mesure, mais de relations mathématiques et d'enchaînements entre des données dont le sens est éventuellement complètement obscur. Et on peut fort bien tomber dans la mauvaise case.

Dans le domaine du marketing, tomber dans la mauvaise case n'est pas dramatique : une publicité mal ciblée ou les recommandations absurdes d'un site de commerce en ligne n'ont jamais changé dramatiquement la vie de quiconque ; j'avais eu un bel exemple de ce genre sur le plus gros site d'e-commerce du monde il y a quelques années, où mes collègues et moi-même n'avions vu l'espace d'une matinée que des recommandations étonnantes, composées à 50% environ de prothèses de jambes. Bug manifeste du moteur de recommandations, dont nous avions eu toutes les peines du monde à nous extraire. Une fois que vous êtes lancé dans un tunnel, dans ce domaine, il est parfois difficile d'en sortir. Donc cette fois-là c'était plutôt amusant. Si un problème semblable advient sur des systèmes de surveillance, la personne qui atterrira d'un coup sur les radars des services de renseignement risque de trouver l'expérience moins ludique.

Mais on ne pourra pas surveiller tout le monde, se dit-on. En fait, si, on peut. Une des caractéristiques des systèmes dédiés au big data c'est la scalabilité linéaire. En termes moins techniques, ça signifie que pour doubler votre capacité de stockage ou de traitement, il suffit grosso modo de doubler le nombre machines dans le cluster. Un cluster, c'est un ensemble de machines (des centaines, des milliers ou plus) qui fonctionnent en parallèle et stockent chacune une partie des données dont vous les nourrissez en permanence. Le principe est d'assembler toutes ces données en les découpant d'abord en de multiples morceaux, traités en parallèle, chacun sur une machine. Au lieu d'un seul programme, vous avez mille programmes qui traitent chacun un morceau de données, tournant sur mille machines, comme s'il s'agissait d'un seul ordinateur gigantesque. Vous avez deux fois plus de données à stocker ? Rajoutez autant de machines et des disques durs. Vos traitements prennent trop de temps ? Rajoutez des machines. La beauté de la chose, c'est que ces systèmes ne sont pas plus durs à gérer quand vous passez de cent à dix mille machines. La même équipe peut s'en charger, la seule limite est le budget. Le système est extensible à l'infini. La capacité et le prix des disques durs aujourd'hui rendent éventuellement inutile la purge des données; on peut tout conserver à tout jamais. Ce n'est qu'une question de moyens.

Alors bien sûr, il faut des analystes (des statisticiens ou des spécialistes de l'intelligence artificielle) et des programmeurs pour créer les programmes qui vont établir des relations entre des données disparates. Mais là encore, beaucoup de choses peuvent être accomplies par des équipes réduites. Les algorithmes qui permettent de partir à la pêche dans l'océan des données sont maintenant rôdés, et il n'est point besoin de réinventer la roue à chaque nouveau problème. L'important est de poser la bonne question, le reste n'est qu'un détail d'exécution. De plus, grâce la puissance de ces architectures, on peut poser de multiples questions dans un temps raisonnable, ce qui n'a jamais été possible auparavant. On peut affiner la question posée, jusqu'à un grand niveau de détail. On peut obtenir des réponses à des questions que l'on n'a pas pensé à poser. Et plus le volume de données est important, plus la fiabilité des réponses, en général, augmente. Enfin, ces données restent accessibles sans délai et s'offrent pour toujours à de nouvelles analyses. Elles permettent de définir des modèles de plus en plus fins, auxquels sont comparées en temps réel les nouvelles données qu'ingurgite en continu le système. Elles permettent de classer, d'identifier, et souvent de prévoir.

Cela dit, et c'est là que la prétention d'empêcher les actes terroristes trouve sa limite, elles permettent de prévoir en termes de probabilités. Elles permettent de vous classer dans un groupe, pas de savoir vraiment si oui ou non vous allez effectivement faire telle ou telle chose, ni quand. A moins que vous n'ayez acheté une grande quantité du nitrate d'ammonium suscité par CB (ce qui serait franchement stupide), que vous ne fréquentiez assidument des individus connus pour leurs appels à la guerre sainte, et que vous n'ayez donné rendez-vous à vos copains par e-mail pour le feu d'artifice, le système ne va pas pouvoir dire quel jour et à quel endroit vous allez poser une bombe artisanale. A moins de disposer des données de centaines de personnes effectivement parties faire le jihad, et qu'elles ne permettent de construire un modèle fiable, ce qui reste à démontrer, il ne pourra pas non plus identifier de manière fiable le départ des prochains candidats. On baigne là dans l'illusion technologique. Ainsi, malgré les considérables moyens déployés aux Etats-Unis, il ne semble pas que la NSA ait atteint dans ce domaine des records d'efficacité. La France ferait-elle mieux ?

Donc, à quoi ça sert ? N'étant pas dans le secret des décideurs, je ne peux qu'imaginer : si j'étais au pouvoir et que j'avais ce gros jouet à disposition, je pourrais toujours avoir une longueur d'avance sur… tout ! Pour prévoir les grèves, les mouvements sociaux, l'agitation étudiante, les ZAD, les contestations diverses, les tendances pour les élections. Même pour la politique étrangère, l'intelligence économique, les possibilités sont infinies. Un outil extraordinaire, mille fois meilleur et plus riche en volume que tous les sondages et les compte-rendu des ex-RG. Les utilisateurs de big data dans le domaine du marketing le savent très bien: les gens mentent (sans le savoir, et croient donner des réponses sincères), mais leurs actions, elles, ne mentent pas.

Exemple au hasard, les « intérêts économiques essentiels de la nation » (un parmi la liste très large des objectifs de la loi). J'imagine fort bien des IMSI-catchers dans le quartier de la Défense, à l'écoute des managers discutant de contrats avec des firmes étrangères concurrentes de firmes françaises. Étant donnée la perméabilité entre les grandes entreprises et la haute fonction publique, je peine à croire qu'aucun conseil amical ne filtrera jamais des services de renseignement vers les directions de ces entreprises. Bien sûr on n'écoutera pas toutes les conversations des concurrents – ce qui demande trop de temps – mais il est déjà démontré qu'il suffit de connaître la liste de vos correspondants, la durée et la fréquence de vos appels pour savoir à peu près tout de votre activité et de vos projets. Les fameuses métadonnées, dont les partisans de la loi vantent la quasi-innocuité, suffiront pour tout leur dire sur vous. Le secret des affaires ? Obsolète. On pourrait faire un concours de pronostics sur tous les usages possibles de cette loi, vu son champ d'application tellement large. On serait sans doute encore à cent lieues de prévoir ce qui se passera exactement.

Mais il y a le contrôle par la commission, objectera-t-on. Je l'imagine cette commission, inondée de requêtes, combien par jour ? Dix, cent, mille ? Combien de temps passé sur chacune d'entre elles ? Comment prétendre qu'il s'agira d'autre chose qu'une chambre d'enregistrement ? Les moyens techniques permettront de rédiger des demandes par centaines, sans effort, à tel point que le contrôle de celles-ci ne deviendra plus qu'un processus de pure forme, sous l'avalanche continuelle. De toutes manières, qui garantira l'indépendance et la compétence des nominés ? Comment prétendre que remplacer tous les juges par une seule commission n'effectuant qu'un contrôle a posteriori, et dont le silence vaut accord, pourra garantir les droits de chacun ? Comment croire qu'un seul « expert technique » pourra valider tous les algorithmes utilisés ? Rien que ce dernier point me semble absurde. Ensuite, il y a la durée de conservation des données, qui est limitée. Techniquement, purger des données disparates est déjà un peu compliqué. Quant à purger des données dérivées des données brutes, pour de multiples raisons, c'est encore plus complexe. Il faudra que cet impératif soit au coeur du système dès le départ pour que cela ait une toute petite chance de fonctionner. Les paris sont ouverts.

L'exécutif se retrouverait donc doté d'un outil par définition opaque, surpuissant, qui lui permettrait de s'abstraire presque totalement du pouvoir judiciaire. Exécutif élu, rappelons-le, pour cinq ans. C'est très court, et c'est prendre un bien gros pari sur l'avenir que de mettre dans les mains de quelques personnages-clés une arme qui permet de contrôler aussi totalement tous les aspects de la vie des personnes. Et de les influencer, voire de les contraindre, quelle qu'en soit la raison. Mais après tout, si vous n'avez ni l'intention de vous syndiquer, ni de donner un avis controversé sur un forum, ni de tromper votre conjoint(e), ni de revendiquer quoi que ce soit, ni de critiquer qui que ce soit, en somme de ne pas faire quoi que ce soit que vous ne vouliez pas que la terre entière apprenne, qu'avez-vous à craindre ? C'est ce qu'on appelle une société de surveillance. La vie privée est un concept désormais obsolète, c'est presque inévitable. »

Voilà, maintenant que vous avez lu ce texte qui est bien plus argumenté que l'exemple caricatural que je vous avais donné, je vous invite à vous faire votre propre opinion, et à le partager autour de vous si vous jugez que cela peut être utile. N'hésitez pas à le transmettre aux députés qui, demain, voteront sur ce projet de loi !

PS : si mon ami a choisi l'anonymat, ce n'est pas par crainte de la police ou de la justice de la République, mais juste parce qu'il ne souhaite pas qu'un lien soit fait avec son employeur.

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

Source : http://www.zdnet.fr/actualites/loi-renseignement-un-ami-expert-du-big-data-explique-le-danger-de-la-surveillance-automatisee-39818832.htm
Par @PierreCol

La Maison Blanche victime d’une cyberattaque « préoccupante » | Le Net Expert Informatique

La Maison Blanche victime d’une cyberattaque « préoccupante »

Des e-mails non classés secrets adressés au président des Etats-Unis, Barack Obama, et envoyés par lui ont été lus l'année dernière par des hackeurs russes qui ont pénétré une partie du système informatique de la Maison Blanche, a affirmé samedi 25 avril le New York Times.

Au début du mois d'avril des responsables américains avaient reconnu qu'il y avait eu un « événement » relatif à la sécurité à la fin de l'année dernière, mais avaient refusé de confirmer les informations selon lesquelles des Russes seraient derrière ces cyberattaques. Selon le quotidien américain, qui cite des responsables ayant été informés de l'enquête sur ces faits, l'attaque a été « beaucoup plus intrusive et préoccupante » que cela n'a été officiellement reconnu. Les personnes cités laissent entendre que les hackeurs étaient liés au pouvoir russe.

« Aucun réseau classé secret atteint »

Les pirates ont réussi à accéder aux archives des e-mails de personnes employées à la Maison Blanche et avec lesquelles M. Obama communiquait régulièrement, écrit le New York Times. C'est dans ces archives que les hackeurs ont pu voir des e-mails que le président avait envoyés et reçus, selon les sources citées par le quotidien. Son compte mail lui-même ne semble pas avoir été piraté. Les hackeurs auraient par ailleurs également pénétré le système non secret du département d'Etat américain.

Les pirates ne semblent en revanche pas avoir pénétré les serveurs qui contrôlent le trafic de messages du BlackBerry de Barack Obama, et la Maison Blanche a assuré qu'aucun réseau classé secret n'avait vu sa sécurité compromise. « Mais des responsables ont reconnu que le système non classé secret contient régulièrement beaucoup d'informations considérées comme hautement sensibles : horaires, échanges d'e-mails avec des ambassadeurs et des diplomates (…) et, inévitablement, débats politiques », écrit le quotidien.

On ignore combien de courriels du président ont été lus par les pirates. « Néanmoins, le fait que les communications de M. Obama étaient parmi celles qui ont été ciblées par les hackeurs – qui sont suspectés d'être liés au pouvoir politique russe, voire de travailler pour lui – a été l'une des conclusions de l'enquête les plus étroitement protégées », selon le New York Times.

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

Source : http://www.lemonde.fr/ameriques/article/2015/04/26/la-maison-blanche-victime-d-une-cyberattaque-preocucupante_4622869_3222.html

---

Internet au bureau : 50 minutes par jour sont consacrées au surf perso | Le Net Expert Informatique

Internet au bureau : 50 minutes par jour sont consacrées au surf perso

Selon une étude sur les habitudes au travail, pas moins de 50 minutes sont quotidiennement réservées à du surf pour des motifs personnels. Les services les plus consultés sont les sites d'actualités et les réseaux sociaux.

L'éditeur Olfeo publie une étude (.pdf) portant sur les usages des internautes au travail. Dans son document, la société explique que le Web est utilisé en moyenne 1 heure et 53 minutes par jour par chaque collaborateur. Dans la grande majorité des cas, cette connexion se fait par le biais d'un câble, le Wi-Fi n'étant réduit qu'à une portion minime (12%).
Environ la moitié de ce temps (44%), soit 50 minutes est consacré à du surf pour des motifs personnels. Sur une semaine, cela représente pas moins de 4 heures et 10 minutes. Ces visites personnelles sont principalement concentrées sur le début de la journée, soit entre 8 h et 9 h ou entre 11 h et 15 h.
Pour réaliser son étude, Olfeo précise avoir interrogé plus d'une centaine d'entreprises, pour un total de 150 000 collaborateurs. Pour parvenir à compiler ces résultats, la société se base sur l'analyse des journaux de connexion au Web fournis par les serveurs proxy. Le journal contient ainsi les requêtes demandées, la durée de connexion, le type de sites visités… C'est donc à partir de ces éléments que la société mesure, via un algorithme, le temps moyen passé sur chaque site.
Les sites d'actualité et les réseaux sociaux sont ceux qui reçoivent le plus de visites. L'étude informe également que les plateformes de streaming ou même les sites à caractère pornographiques sont consultés pendant les heures de travail.

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

S o u r c e :
http://pro.clubic.com/actualite-e-business/actualite-762516-internet-bureau-50-minutes-consacrees-perso.html?&vc_mode=MG&vc_campaign=NL_ClubicPro_New_11/04/2015&partner=-&vc_position=933831174&vc_misc=-&crmID=639453874_933831174&estat_url=http%3A%2F%2Fpro.clubic.com%2Factualite-e-business%2Factualite-762516-internet-bureau-50-minutes-consacrees-perso.html