Loi Renseignement : la boîte à outils pour apprendre à protéger votre vie privée, en chiffrant vos données et communications | Denis JACOPINI

Maintenant que la Loi Renseignement est votée, et en attendant la suite du processus législatif, apprenons à résister à la surveillance de masse avec quelques outils cryptographiques plus ou moins simples, mais efficaces et légaux.

Nous sommes le soir du mardi 5 mai, et c'est un jour funeste pour la démocratie. La France s'était autoproclamée « pays des Lumières » parce qu'il y a 250 ans notre pays éclairait l'Europe et le monde grâce aux travaux philosophiques et politiques de Montesquieu, qui prônait la séparation des pouvoirs, et de Voltaire et Rousseau.
À dater d'aujourd'hui, jour du vote en première lecture du projet de loi sur le renseignement, à cause d'une classe politicienne d'une grande médiocrité, s'enclenche un processus au terme duquel le peuple français va probablement devoir subir une loi dangereuse, qui pourrait s'avérer extrêmement liberticide si elle tombait entre de mauvaises mains, par exemple celles de l'extrême droite.
Même si la loi doit encore passer devant le Sénat puis peut-être revenir en seconde lecture à l'Assemblée Nationale, même si une saisine du Conseil Constitutionnel va être déposée par une soixantaine de courageux députés en complément de celle déjà annoncée par François Hollande, mieux vaut se préparer au pire, en imaginant que cette loi sera un jour promulguée. En faisant un peu de mauvais esprit, j'ai imaginé un nom pour le dispositif qui sera chargé de collecter nos données personnelles afin de détecter les comportements suspects : « Surveillance Totalement Automatisée via des Systèmes Informatiques » et bizarrement l'acronyme est STASI !
Dès lors, à titre préventif et sans préjuger de l'avenir, il me semble important d'apprendre à protéger sa vie privée. Ceci passe par le chiffrement de ses communications, qu'il s'agisse d'échanges sur Internet ou via SMS, et cela peut se faire au moyen de différents outils à la fois efficaces et légaux.
Bien évidemment, les « vrais méchants » que sont les terroristes, djihadistes, gangsters et autres trafiquants connaissent et utilisent déjà ces outils : vous vous doutez bien qu'ils n'ont pas attendu ce billet de blog pour les découvrir….

Une boîte à outils pour protéger votre vie privée

Anonymat sur Internet

Pour protéger votre identité sur Internet et notamment sur le web, vous pouvez combiner l'utilisation d'un réseau privé virtuel, ou VPN, et de TOR, un système d'anonymisation qui nécessite l'installation d'un logiciel spécifique, TOR Browser. Je ne vous donne pas de référence particulière en matière de VPN, car l'offre est pléthorique.

MAJ : un lecteur m'a indiqué l'existence de La brique Internet, un simple boîtier VPN couplé à un serveur. Pour que la Brique fonctionne, il faut lui configurer un accès VPN, qui lui permettra de créer un tunnel jusqu'à un autre ordinateur sur Internet. Une extension fournira bientôt aussi en plus un accès clé-en-main via TOR en utilisant la clé wifi du boîtier pour diffuser deux réseaux wifi : l'un pour un accès transparent via VPN et l'autre pour un accès transparent via Tor.

Chiffrement des données

Pour chiffrer le contenu de vos données, stockées sur les disques durs de vos ordinateurs ou dans les mémoires permanentes de vos smartphones, vous pouvez mettre en œuvre des outils tels que LUKS pour les systèmes Linux ou TrueCrypt pour les OS les plus répandus : même si TrueCrypt a connu une histoire compliquée, son efficacité ne semble pas remise en cause par le dernier audit de code effectué par des experts.

Je vous signale aussi que l'ANSSI – Agence nationale de la sécurité des systèmes d'information – signale d'autres outils alternatifs comme Cryhod, Zed !, ZoneCentral, Security Box et StormShield. Même si l'ANSSI est un service gouvernemental il n'y a pas de raison de ne pas leur faire confiance sur ce point

Chiffrement des e-mails et authentification des correspondants

GPG, acronyme de GNU Privacy Guard, est l'implémentation GNU du standard OpenPGP. Cet outil permet de transmettre des messages signés et/ou chiffrés ce qui vous garantit à la fois l'authenticité et la confidentialité de vos échanges. Des modules complémentaires en facilitent l'utilisation sous Linux, Windows, MacOS X et Android.

MAJ : un lecteur m'a signalé PEPS, une solution de sécurisation française et Open Source, issue d'un projet mené par la DGA – Direction générale de l'armement – à partir duquel a été créée la société MLState.

Messagerie instantanée sécurisée

OTR, Off The Record, est un plugin à greffer à un client de messagerie instantanée. Le logiciel de messagerie instantanée Jitsi, qui repose sur le protocole SIP de la voix sur IP, intègre l'outil de chiffrement ZRTP.

Protection des communications mobiles

A défaut de protéger les métadonnées de vos communications mobiles, qu'il s'agisse de voix ou de SMS, vous pouvez au moins chiffrer les données en elles-mêmes, à savoir le contenu de vos échanges :

RedPhon est une application de chiffrement des communications vocales sous Android capable de communiquer avec Signal qui est une application du même fournisseur destinée aux iPhone sous iOS.

TextSecure est une application dédiée pour l'échange sécurisé de SMS, disponible pour Android et compatible avec la dernière version de l'application Signal. Plus d'information à ce sujet sur le blog de Stéphane Bortzmeyer.

MAJ : un lecteur m'a indiqué l'application APG pour Android qui permet d'utiliser ses clés GPG pour chiffrer ses SMS.

Allez vous former dans les « cafés Vie Privée »

Si vous n'êtes pas geek et ne vous sentez pas capable de maîtriser ces outils sans un minimum d'accompagnement, alors le concept des « cafés Vie Privée » est pour vous : il s'agit tout simplement de se réunir pour apprendre, de la bouche ceux qui savent le faire, comment mettre en œuvre les outils dont je vous ai parlé plus haut afin de protéger sa vie privée de toute intrusion, gouvernementale ou non.

Tout simplement, il s'agit de passer un après-midi à échanger et à pratiquer la cryptographie. Pour cela sont proposés des ateliers d'une durée minimum de 1 heure, axés autour de la sécurité informatique et de la protection de la vie privée.

Et comme le disent avec humour les organisateurs, « les ateliers sont accessibles à tout type de public, geek et non-geek, chatons, poneys, loutres ou licornes. ». Bref, le « café Vie Privée » est à la protection de la vie privée ce que la réunion Tupperware était à la cuisine

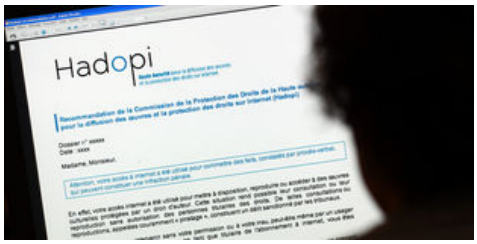
Voilà, vous avez je l'espère suffisamment d'éléments pratiques pour commencer à protéger votre vie privée… en espérant vraiment que le Conseil Constitutionnel abrogera les points les plus contestables de cette loi et nous évitera d'avoir à déployer un tel arsenal sécuritaire.

PS : l'image « 1984 was not a manual » a été créée par Arnaud Velten aka @Bizcom.

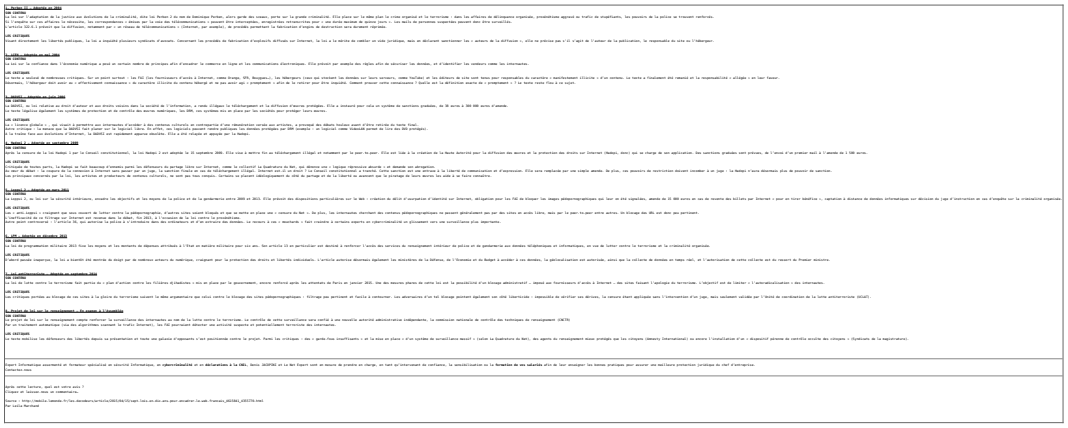
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/loi-renseignement-la-bo-te-a-outils-pour-apprendre-a-proteger-votre-vie-privee-en-chiffrant-vos-donnees-et-communications-39818894.htm
Par Pierre Col

Huit lois en dix ans pour encadrer le Web français | Denis JACOPINI



Huit lois en dix ans pour encadrer le Web français



L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

Cour de justice de l'Union européenne a jugé aujourd'hui qu'un fournisseur de hotspot n'était pas responsable des contrefaçons réalisées par ses utilisateurs. Cependant, cet acteur pouvait se voir enjoindre d'exiger un mot de passe par une juridiction ou une autorité administrative nationale.

Le litige est né en 2010 : Sony Music avait adressé une mise en demeure à Thomas Mc Fadden. Cet exploitant d'une entreprise de sonorisation outre-Rhin avait laissé son réseau Wi-Fi ouvert sans mot de passe. Or, un tiers a pu mettre à disposition une œuvre du catalogue de la major. L'affaire était remontée jusqu'à la CJUE où les juridictions allemandes ont déversé une série de questions préjudicielles.

FAI ou exploitant de hotspot Wi-Fi, même combat

Dans son arrêt (PDF) du jour, la Cour va d'abord considérer que la fourniture d'un tel accès Wi-Fi relève de la fourniture d'un service de la société de l'information, à l'instar donc des prestations d'un FAI (article 12 de la directive de 2000). Cela implique cependant que l'exploitant du hotspot ait un rôle « *purement technique, automatique et passif* » et qu'il n'a ni la connaissance ni le contrôle des informations transmises.

Ceci vérifié, la Cour rappelle qu'un tel prestataire n'est alors pas responsable des contenus qui passent dans ses tuyaux à la triple condition :

1. de ne pas être à l'origine d'une telle transmission,
2. de ne pas sélectionner le destinataire de cette transmission et
3. de ne ni sélectionner ni modifier les informations faisant l'objet de ladite transmission.

Si ces conditions sont remplies, alors un titulaire de droit ne peut demander la moindre indemnisation à cet intermédiaire ou le remboursement de ses frais…[lire la suite]

Qu'en est-il des professionnels de l'hôtellerie qui mettent à disposition de leurs clients du Wifi ? Réagissez

---

Réagissez à cet article

Original de l'article mis en page : CJUE : l'exploitant professionnel d'un hotspot Wi-Fi n'est pas responsable des contrefaçons

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

	Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.
En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « *si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace* » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.

Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.
Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « *alors même qu'aucune infraction n'est constatée* ».
L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.
Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».
Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence – Politique – Numerama

---

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

---

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

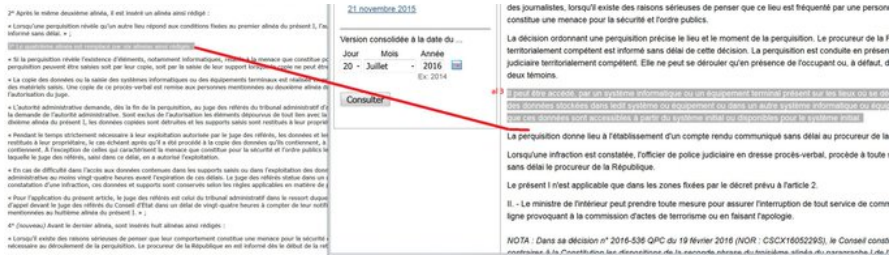
---

État d'urgence : la police pourra bien copier des données trouvées dans le Cloud

État d'urgence : la police pourra bien copier des données trouvées dans le Cloud

Contrairement à ce que nous écrivions mardi avec étonnement, il sera bien possible pour la police d'utiliser l'ordinateur ou le smartphone d'un suspect pour accéder à tous ses services en ligne, puis de copier les informations obtenues pour les exploiter si elles sont pertinentes.

Il faudrait toujours retourner son clavier sept fois sur le bureau avant de donner un satisfecit au gouvernement. Mardi, nous détaillions le cadre prévu dans le projet de loi de prorogation de l'état d'urgence, pour la copie des données informatiques dont Manuel Valls avait annoncé le retour. Il fallait vérifier si les exigences du Conseil constitutionnel en matière de respect de la vie privée étaient bien respectées.
À cette occasion, nous faisions remarquer à tort que le gouvernement n'avait pas prévu la possibilité de copier des données stockées dans les services en ligne des suspects, se limitant curieusement aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* ».
Pris dans un élan de naïveté, nous n'avions pas fait attention au fait que l'ensemble du dispositif n'était pas réécrit, et que le gouvernement avait laissé intacte une disposition non censurée par le Conseil constitutionnel, qui change toute l'analyse. Elle dit qu'en cas de perquisition administrative, « *il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Créé en novembre 2015, cet alinéa de l'article 11 de la loi du 3 avril 1955 relative à l'état d'urgence n'a pas été supprimé, comme le fait justement remarquer Marc Rees deNext Inpact :
Voir l'image sur Twitter



Suivre
marc rees @reesmarc
. @p_estienne j'ajoute que PJL #EtatdUrgence ne supprime pas accès au cloud cc @gchampeau (gauche PJL droite, L55)
11:03 – 20 Juil 2016
•
•
77 Retweets
•
1 j'aime
Il reste donc possible pour la police d'accéder sur place à toutes données disponibles sur le Cloud, en profitant des sessions ouvertes sur des services en ligne (ou dont le mot de passe est mémorisé). Dès lors, à partir du moment où ils sont affichés à l'écran ou téléchargés, ces messages Facebook, e-mails, documents Google Docs, historiques WhatsApp ou autres fichiers stockés à distance deviennent bien des « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », qui peuvent être copiées et analysées après autorisation du juge, dans le cadre désormais fixé.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : la police pourra bien copier des données trouvées dans le Cloud – Politique – Numerama

---

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
• N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle.

Jean-Jacques Urvoas, ministre de la Justice, au Sénat.

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE,…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « *données accessibles à partir du système initial ou disponibles pour le système initial* », qui a disparu.

« *Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les* ***données contenues dans tout système informatique ou équipement terminal présent sur les lieux*** *de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.*

La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui ***en indique les motifs*** *et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition.* ***À compter de la saisie, nul n'y a accès avant l'autorisation du juge****.*

L'autorité administrative ***demande au juge des référés du tribunal administratif d'autoriser en tout ou partie leur exploitation****. Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il* ***statue dans un délai de quarante-huit heures*** *à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative.* ***Sont exclus de l'autorisation les éléments dépourvus de tout lien avec la menace*** *que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics.* ***En cas de refus*** *du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa,* ***les données copiées sont détruites*** *et les supports saisis sont restitués à leur propriétaire.*

Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont ***restitués à leur propriétaire****, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent,* ***à l'issue d'un délai maximal de quinze jours*** *à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent.* ***À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les données copiées sont détruites à l'expiration d'un délai maximal de trois mois*** *à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.*

En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. ***Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables*** *en matière de procédure pénale.*

Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. ***Ses décisions sont susceptibles d'appel*** *devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article.* »

Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».

Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement obtenir au préalable une autorisation du Premier ministre, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même possible de se passer de l'avis de la CNCTR.

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

Article original de Guillaume Champeau

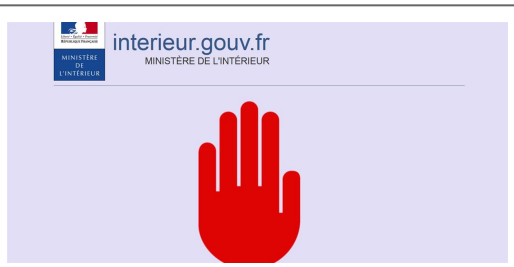
Réagissez à cet article

Original de l'article mis en page : État d'urgence : open bar

pour la police sur les données de connexion ? – Politique – Numerama

---

Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?



Vers un délit d’entrave au blocage des sites faisant l’apologie du terrorisme ?

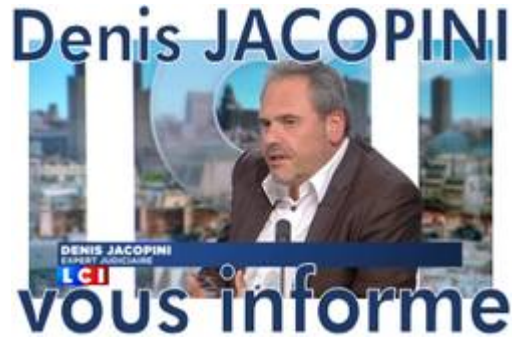
Dans le cadre du projet de loi sur la réforme pénale, le rapporteur Michel Mercier veut instaurer en France un délit d'entrave au blocage des sites « terroristes ».

En préparation de l'examen en Commission des lois, le sénateur a déposé un amendement visant à condamner ceux qui viennent entraver les procédures de blocage des sites faisant l'apologie ou provocant au terrorisme. Celui qui viendrait extraire, reproduire et transmettre intentionnellement les données concernées par ces mesures, « en connaissance de cause », serait ainsi éligible à cinq ans de prison et 75 000 euros d'amende.
Cette mesure, puisée directement dans une proposition de loi sénatoriale contre le terrorisme (UDI/LR), viendra épauler les mesures de blocage administratif de ces sites, permises depuis la loi du 13 novembre 2014 sur le terrorisme, ou celles décidées par un juge en application de l'article 706-23 du code de procédure pénale.
« *Ces blocages, administratif ou judiciaire, ont pour but de lutter contre la diffusion de contenus faisant l'apologie d'actes de terrorisme,* explique l'auteur de l'amendement dans son exposé des motifs. *Néanmoins, ces blocages peuvent être entravés par certains comportements. Ces derniers, s'ils ne consistent pas en la diffusion publique de ces contenus, ne peuvent être appréhendés sous le délit d'apologie d'actes de terrorisme ou de provocation à de tels actes* ».
Cette mesure est rédigée en des termes suffisamment larges pour qu'on puisse imaginer la sanction de celui qui viendrait tweeter ou publier sur Facebook les données litigieuses, puisqu'il n'est pas possible de bloquer l'un ou l'autre de ces réseaux. Remarquons surtout que le texte n'exige pas nécessairement de diffusion publique. Il joue dès lors qu'on extrait, reproduit et transmet ces données d'une manière ou d'une autre, à destination par exemple d'un serveur distant. Du coup, l'amendement est également taillé pour frapper ceux qui multiplient des contre-mesures aux blocages par IP ou DNS… [Lire la suite]

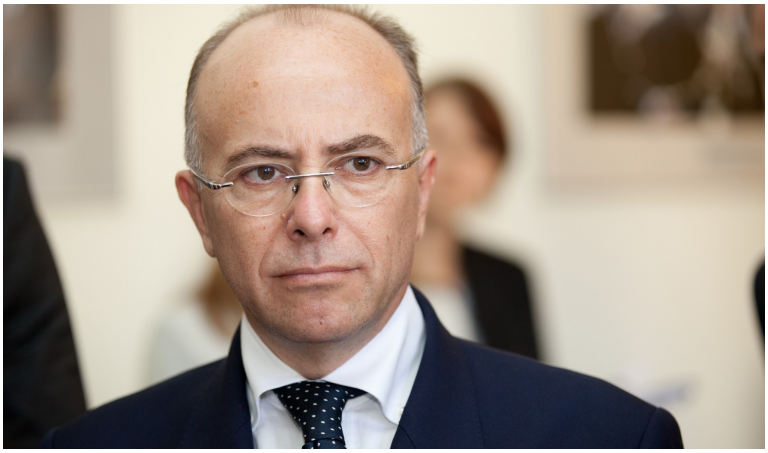
Réagissez à cet article

Source : *Vers un délit d'entrave au blocage des sites faisant l'apologie du terrorisme ? – Next INpact*

Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement



Wi-Fi interdit, Tor bloqué, backdoors… les nouvelles idées au gouvernement



La liste des mesures envisagées par le gouvernement pour renforcer la sécurité au détriment de la liberté et de la vie privée s'allonge. Alors que le gouvernement envisage déjà de nouvelles lois sécuritaires qui permettraient par exemple de croiser tous les fichiers de données personnelles détenues par l'État, d'obliger à l'installation d'émetteurs GPS sur les voitures louées, d'allonger la durée de conservation des données de connexion ou encore de faciliter le recours aux IMSI-catchers, Le Monde révèle samedi de nouvelles mesures recensées par le ministère de l'Intérieur.
Le quotidien a en effet pu consulter un tableau édité en interne le mardi 1er décembre par la direction des libertés publiques et des affaires juridiques (DLPAJ), qui dépend du ministère de l'Intérieur de Bernard Cazeneuve. C'est elle qui prépare les projets de lois et de décrets relatifs aux libertés publiques et à la police administrative. C'est donc dans ce cadre, pour rédiger deux nouveaux textes législatifs – l'un sur l'état d'urgence, l'autre sur l'anti-terrorisme, que la DLPAG a dressé les mesures demandées par la police ou la gendarmerie qui pourraient être inscrites dans les textes attendus pour janvier 2016.

Interdire et bloquer TOR en France
Parmi ces mesures qui ne sont encore que des hypothèses de travail figure une série de nouvelles restrictions aux libertés sur Internet :
« Interdire les connexions Wi-Fi libres et partagées » et fermer toutes les connexions Wi-Fi publiques pendant l'état d'urgence, « sous peine de sanctions pénales ».
Jusqu'à présent la loi impose par principe aux abonnés à internet de sécuriser leur connexion pour éviter qu'elle soit utilisée à des fins illicites, mais le seul risque que prennent les abonnés généreux et récalcitrants qui laissent leur Wi-Fi ouvert est de recevoir un avertissement Hadopi si quelqu'un l'utilise pour pirater des films ou de la musique. En obligeant à fermer toute connexion, la police s'assurerait d'avoir un identifiant précis pour chaque adresse IP, ou au moins de réduire la liste des suspects possibles dans un même foyer. C'est en tout cas l'idée.
« Interdire et bloquer les communications des réseaux TOR en France » : Même à supposer que ça soit techniquement possible, ce serait une mesure totalement disproportionnée qui enverrait un très mauvais signe à l'international, alors que le réseau d'anonymisation TOR est utilisé par de très nombreux activistes et dissidents de pays autoritaires. L'un des premiers pays à avoir bloqué Tor était l'Iran.
« Identifier les applications de VoIP et obliger les éditeurs à communiquer aux forces de sécurité les clefs de chiffrement » : C'est la fameuse grande guerre du chiffrement à laquelle se prépare La Quadrature du Net, la France ayant sans aucun doute la volonté de se joindre à la Grande-Bretagne pour obtenir que les éditeurs de messagerie chiffrée fournissent des backdoors pour que les autorités puissent écouter les conversations interceptées.

Réagissez à cet article
Source : http://www.numerama.com/politique/133795-wi-fi-ouvert-interdit-tor-bloque-les-nouvelles-idees-de-la-police.html