3034 0

Noter

Mots-clés

amnesty-international (4)
Anti-terrorisme (3)
Assemblée-nationale (78)
cryptographie (1)
loi-renseignement (2)
neutralité-du-net (2)
Projet de loi renseignement (2)
quadrature-du-net (4)
surveillance (8)
vie-privée (3)
#PJLRenseignement (2)

Du même auteur


[Hollandie] Vous avez demandé la Loi sur le Renseignement, ne quittez pas

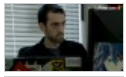

« Alabama Monroe » : l'Aventure Continue


Des Caricatures Contre les Kalachnikovs

Sur le même sujet


24h Avant 1984 : Appelle ton Député


La Dernière Colonie d'Afrique


NSA Made in France


Fin de Vie : Laisser Mourir ou Faire Mourir ?


Sénat : Chambre à Part ?

Publié le 6 mai 2015 | par **Lurinas**

[M.A.J. 26/06/2015] Voilà, c'est fait ! Nos députés français viennent d'adopter à une très large majorité la loi la plus attentatoire à nos libertés et nos droits. Ou comment basculer d'un État démocratique à un État Policier.

Imperceptiblement, nos petits renoncements quotidiens nous font passer d'un État de Droit à un État Policier. Volontairement ou involontairement, consciemment ou inconsciemment, les reculs sont sans doute minimes mais leur sommation rend la comparaison avec l'état initial vertigineuse. Aujourd'hui, c'est à l'abolition de notre première liberté que nous venons d'assister.

C'est pas moi qui le dit, c'est lui :

> *« Il n'y a, dans ce texte de loi, aucune – je dis bien : aucune – disposition*

> ***attentatoire aux libertés, qu'il s'agisse de la liberté d'aller et venir ou d'autres libertés individuelles ou collectives. Si vous estimez qu'un article de ce texte est susceptible de remettre en cause une liberté, dites-moi lequel. En revanche, il est des dispositions qui peuvent être considérées comme remettant en cause la vie privée et le droit à cette dernière »***

C'est assez effarant pour valoir à notre ministre de l'intérieur Cazeneuve le fameux **prix Busiris**.

Tous unanimes, sauf eux

La mobilisation a pourtant été conséquente. Des citoyens (réunis autour d'une **pétition** de plus de 130 000 signatures), des associations civiles, des ONG, des comités Théodule, etc.

Soit, sans volonté d'exhaustivité, Amnesty International, La Quadrature du Net, la Ligue des Droits de l'Homme, le Syndicat des Avocats de France, le Syndicat de la Magistrature, le juge anti-terroriste Trévidic, le Conseil National du Numérique, la Commission Nationale de l'Informatique et des Libertés (CNIL), Human Rights Watch, des hébergeurs Internet (OVH, Gandi), des sociétés de stockage en cloud, le commissaire aux Droits de l'Homme du Conseil de l'Europe, des vendeurs de sécurité en informatique, des experts informatiques, des hackers, l'Autorité de régulation des communications électroniques et des postes (ARCEP), des rapporteurs de l'ONU et du Conseil de l'Europe, etc. Et même Laurence Parisot et Henri Gaino ! Quand on vous dit que la mobilisation était trans-partisane.

Une **mobilisation de tous les instants**, vis-à-vis des 577 députés dans l'optique de les convaincre du caractère négatif de ce projet législatif.

Tous soulignaient le caractère intrusif de la proposition de loi, la légalisation de pratiques de surveillance de masse non ciblées restées jusque-là illicites, l'absence de contrôle par un juge judiciaire seul garant des libertés individuelles, la culture du soupçon et du profilage, le blocage des sites Internet sans autorisation judiciaire préalable, la collecte généralisée de données à titre préventif, le large périmètre d'application de cette loi, les dispositions renforçant les pouvoirs de police, l'opacité sur les dispositifs déjà en place et légalisés a posteriori, l'extension des moyens d'action du renseignement intérieur et extérieur, la conservation longue des données collectées, le contrôle exclusif des services de renseignement par le pouvoir exécutif, l'avis simplement consultatif d'une commission ad hoc, la mise en place d'un régime de surveillance internationale pour les communications émises ou reçues de l'étranger…

De quoi sonner le glas au droit au procès équitable, au droit au respect de la vie privée et familiale, au droit au recours effectif. Droits inscrits dans la **Convention Européenne des Droits de l'Homme**.

L'objet de la loi était tellement important que le texte a été soumis à une procédure accélérée dite d'urgence (quatre jours de débat, nombre d'examens par l'Assemblée Nationale et le Sénat limité). Que les discussions ont souffert d'un véritable examen approfondi, équilibré et réflexif, alors qu'il était tout de même question de libertés et de droits de l'Homme…

Pour le gouvernement, pressé par les derniers attentats terroristes de janvier 2015 (Charlie Hebdo, épicerie casher de la porte de Vincennes) ou des tentatives d'attentats déjoués, il en allait de notre sûreté territoriale. C'est faire grand cas des agressions terroristes métropolitaines, certes toujours traumatisantes, mais **si rares finalement**.

Pour trouver l'aiguille dans la botte de foin (aaahhh ! c'est ça la photo en Une ?!), notre exécutif a choisi le super-aimant monumental. C'est toujours mieux que la politique du brûlis, je vous le concède…

Ce dispositif est pourtant en contradiction avec la jurisprudence européenne qui impose à la loi de contenir des dispositions précises sur les catégories de personnes pouvant faire l'objet de mesures de renseignement.

Et pendant ce temps-là, **l'Assemblée parlementaire du Conseil de l'Europe** a adopté **une résolution** contre les politiques de surveillance massive mises en place par certains gouvernements européens. Cette Assemblée rappelle que « les opérations de surveillance révélées jusqu'ici mettent en danger les droits de l'homme fondamentaux ». Non pas uniquement le droit au respect de la vie privée, mais aussi le droit à la liberté d'expression qui en découle.

Ça va mieux en le disant par voie officielle !

La loi de rance saignement

Prism and co, le programme Échelon… étaient à nos portes. Les voilà enfoncées de l'intérieur par la **loi relative au renseignement**. Les dernières toutes récentes lois de programmation militaire de fin 2013 (autorisant l'administration française à intercepter et stocker toute donnée ou document hébergé sur un serveur en France) et antiterroriste de début 2014 (autorisant le blocage administratif de sites Internet faisant « l'apologie du terrorisme », sans intervention d'aucun juge)

Aidez-nous !
Faites un don de
10€ Valider

ne devaient pas y suffire ?

Cette nouvelle loi justifie la surveillance généralisée afin d'assurer l'indépendance nationale, l'intégrité du territoire et la défense nationale, de défendre 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, de prévenir le terrorisme, les atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale, de la reconstitution ou d'actions tendant au maintien de groupements dissous, de la criminalité et de la délinquance organisées et la prolifération des armes de destruction massive.

Voilà comment ce que la loi prétendait mieux encadrer se perd alors dans des termes flous et se noie en de vastes catégories. Du bel ouvrage que ce ciblage si précis et cette proportionnalité équilibrée, fondements même de l'histoire du Droit français. Une loi sécuritaire plus qu'une loi anti-terroriste finalement, donnant tort à ceux qui la comparent au **Patriot Act**.

Un champ d'action élargit d'autant que le renseignement ne se veut plus simplement défensif mais également offensif.

Un retour sur expérience aurait pourtant permis de statuer dans le bon sens pragmatique sur ce type de mesures législatives : le Patriot Act n'a officiellement permis d'incarcérer qu'une seule personne depuis 2001, personne qui fut condamnée pour avoir transféré 8500 dollars vers sa famille restée en Somalie, somme qui aurait été utilisée par une organisation terroriste… De quoi donner à libérer quatre jours de discussion pour l'étude d'autres travaux législatifs d'importance.

Mais cette loi permettait au moins, aux yeux du gouvernement, de rendre légal ce qui était illégal (une sorte d'amnistie générale pour nos services de renseignement). Tels l'installation de logiciels espions sur les ordinateurs, smartphones, tablettes, sites, serveurs cibles, de dispositifs de géolocalisation sur les voitures, de captation, de microphones dans les demeures… Et en élargissant et légalisant surtout ces pratiques des officiers de police judiciaire aux officiers de renseignement.

Brèfle, nos libertés commencent à être décapitées. Des saignements, l'hémorragie est à craindre !

Et quelques bricoles en sus…

Par défaut, la loi attribue la compétence de renseignement aux services spécialisés (SSR) « relevant des ministres de la Défense et de l'Intérieur ainsi que des ministres chargés de l'Economie, du Budget ou des Douanes ». Mais un décret en Conseil d'État peut aussi étendre ce champ des possibles. Mieux, le ministère de la Justice a été ajouté dans la liste afin notamment de propager ces technologies dans le système pénitentiaire.

Le rôle du premier ministre est ici primordial en ce qu'il va décider de la mise en œuvre technique du recueil du renseignement. Cette autorisation doit cependant passer par l'avis consultatif (!) de la Commission nationale de contrôle des techniques de renseignement (CNCTR). Cette dernière comptera 13 membres pour s'assurer de toute conformité : trois députés, trois sénateurs, trois magistrats du Conseil d'État, trois magistrats de la Cour de Cassation et un représentant désigné par l'ARCEP.

Quels seront les moyens humains et financiers dévolus à cette unique commission indépendante pour jouer son maigre rôle de contre-pouvoir ? Quelles seront les modalités d'intervention, d'action et de recours de et via la CNCTR pour les citoyens s'agissant de surveillance classée secret-défense et donc supposée a priori inconnue de la personne ciblée ? Le contrôle de la CNCTR ne devrait-il pas être systématique et immédiat par défaut plutôt qu'actif seulement sur leur propre demande ? Autant de questions importantes qui auront l'honneur d'éclaircissements dans les prochains décrets d'application et les lois de finance.

Il faudra être patient pour ces quelques ersatz d'assurances. Car en attendant, certaines exceptions perdurent. Telles les urgences "absolue" et "opérationnelle" : la première permettant aux agents de se passer de l'avis de la CNCTR (mais pas de l'autorisation du premier ministre) ; le seconde permettant à un chef de service d'autoriser "directement la mesure de surveillance" sans recourir ni à l'avis de la CNCTR, ni à l'autorisation du premier ministre. Bien faible autorité de contrôle que cette commission.

Est également prévu un accès administratif aux données de connexion (contrat d'abonnement, adresse IP, adresse postale, lieu de connexion, date, numéros de téléphone, etc.), pour lequel doit être installer une station de pompage ponctuelle permettant un accès en temps réel et direct sur les réseaux des opérateurs pour récupérer ces informations. Cela dans le cas d'une personne identifiée devant relever d'une situation de renseignement.

Dans l'hypothèse de personnes non identifiées, des boîtes noires (« dispositif destiné à détecter

une menace terroriste sur la base de traitements automatisés », voir infra) seront imposées à tous les acteurs des nouvelles technologies sur leurs infrastructures dans l'optique d'une anticipation aux menaces terroristes. Tous (fournisseurs d'accès, hébergeurs, éditeurs…) doivent maintenant répondre favorablement à une requête des services de renseignement demandant à installer un dispositif de surveillance des métadonnées à destination des sites ou via leurs sites.

Mieux encore, les fournisseurs de prestations de cryptologie sont tenus de remettre aux services de renseignement les clefs permettant de déchiffrer les communications, et ce sans délai. Tellement pratique pour pouvoir déchiffrer (à la volée ?).

D'autres techniques sont décrites, non limitées à la lutte contre le terrorisme mais élargies aux six catégories supplémentaires de la loi. Parmi icelles, les IMSI-catchers. Ce dispositif technique (une fausse antenne relais d'une portée de 0.5 à 1 kilomètre) vise à récupérer les données de connexion afin d'identifier un équipement terminal ou le numéro d'abonnement de son utilisateur et à géolocaliser l'équipement. Techniquement, les IMSI-catchers permettent « d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination » ou « d'en prendre connaissance » ou «d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ».

Dans son avis, la CNIL estime que « ces nouvelles techniques (sonde, dispositif de détection de « signaux faibles » et « IMSI-catcher ») caractérisent un profond changement de nature dans les mesures de surveillance légalement autorisées. Il ne s'agit en effet plus seulement d'accéder aux données utiles concernant une personne identifiée comme devant faire l'objet d'une surveillance particulière, mais de permettre de collecter, de manière indifférenciée, un volume important de données, qui peuvent être relatives à des personnes tout à fait étrangères à la mission de renseignement.

Le pouvoir exécutif se retrouve donc renforcé, avec des moyens disproportionnés en tout domaine, et le pouvoir judiciaire bien amoindri. Hollande fantasmait **les boîtes à outils**. En voilà une omnipotente et multiservice !

Les boîtes noires des Shadocks

La loi de renseignement prévoit l'utilisation d'une technique algorithmiques pour détecter en temps réel des « comportements suspects« d'internautes (radicalisation, etc.). Des enregistrements et des analyses automatiques de données, un pompage infini et sans discontinuer. Cela via des sondes posées au cœur du réseau, ce qui n'est pas des moins intrusifs. Des sondes certainement dotées d'un service DPI (**Deep Packet Inspection**) que nos sociétés françaises Amesys, Qosmos voire Orange maitrisent assez bien (doux euphémisme).

La prédiction de la criminalité sur les réseaux n'est pas nouvelle. Était déjà à l'étude il y a quelques années **Indect** (projet de recherche porté par la communauté européenne sur la précognition, soit la détection et la prévention des comportements criminels et du terrorisme).

Cette traque aux comportements suspects est une innovation en ce qu'elle diffère de la surveillance de suspects et de ses proches, jusque-là classique dans l'univers policier et anti-terroriste. Une mesure maintenant plus proactive, par la détection précoce. Le « a priori » en lieu et place du « a posteriori » (à ce jour, en dehors de la lutte contre le terrorisme, l'intention ne valait pas l'action ; en droit commun, il n'y avait pas de tentative sans un commencement d'exécution et donc pas de délit).

Mais qu'est-ce qu'un comportement suspect du point de vue d'un algorithme ? Quid du contrôle démocratique de cette mesure ?

Car cette loi permet non seulement de mettre sur écoute les « cibles » des services de renseignement, mais surtout de surveiller ceux qui n'ont pas encore été identifiés comme « cibles ». Par le truchement de boîtes noires installées au cœur des réseaux de télécommunication, à « titre expérimental » (sic) jusqu'en 2018 (sur quelle partie du réseau des FAI ? Chez les hébergeurs et/ou les fournisseurs d'accès et/ou les opérateurs de téléphonie mobile ? Quelles données recueillies ?…).

Un algorithme est une « méthode générale pour résoudre un ensemble de problèmes », et donc, en informatique, une suite d'actions données à une machine. Ce qui n'est pas qu'une question de « mots-clés ». La base algorithmique des sondes est un calcul probabilistique appliqué aux réseaux, ce qui suppose des échantillons de données de plus en plus grands et de plus en plus représentatifs pour que le dispositif soit de plus en plus efficace dans le profilage (à l'instar du Trading Haute Fréquence et du marketing prédictif). Ce n'est donc, semble-t-il, que le début de la surveillance massive boulimique…

Problème intrinsèque : celui des faux positifs, inhérent à ce type de surveillance, quelque soit la qualité performante et la robustesse de l'algorithme. Des erreurs qui pourraient coûter cher aux

concernés (cf. **erreurs** et conséquences sur les **fichés** du **STIC**).

Enfin, car il ne faut pas prendre nos satanés « terroristes barbus » pour plus hydrocéphales que la moyenne (même s'ils oublient négligemment leur carte d'identité ou se tirent une balle sur eux-mêmes…), l'algorithme ne surveillera que ceux qui ne se cachent pas. Comprendre : les vrais apprentis terroristes viseront certainement à ne pas utiliser les moyens de communications technologiques, ce qui diminuera à terme d'autant l'efficacité du dispositif.

Et dire pourtant que la **loi Informatique et libertés**, tout en anticipation (1978), était claire :

> ***« Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité »***

Neutralité du Net

Il est un fait inéluctable : ce qui est cédé aux services de renseignements est difficile à récupérer. Cette loi et ces dispositifs seront donc une nouvelle valeur, un nouveau jalon référence de nos libertés. Le retour en arrière sera malaisé.

Il ne fait aussi aucun de doute que le périmètre, les mesures, les techniques déployées seront chaque fois respectivement repoussé, élargies, sans cesse plus innovantes (cf. **élargissement de l'objet initial et restreint du FNAEG**). Sans que ne soit jamais remise en doute l'efficacité de telles mesures de surveillance.

Et la question de la **neutralité du Net** se posera. Si ce n'était déjà fait. A savoir : l'assurance que le tuyau ne change pas l'eau en vin, que la molécule originelle n'est pas scindée, ou qu'aucun électron surnuméraire ne vient la dénaturer par une action volontaire du contenant, etc.

Une modification de l'algorithme, par exemple, dont le code source restera de facto inaccessible car sous couvert de secret-défense (donc invérifiable), permettrait d'intercepter (dans un futur forcément hypothético-paranoïaque) à volonté le contenu de toutes communications, mais également de les altérer, de les modifier, sans que les opérateurs n'en soient eux mêmes informés (encore moins les utilisateurs finaux). Ce qui n'est pas complètement utopique : le gouvernement fait déjà cela en renvoyant un site listé vers leur **page officielle de blocage** (selon le principe du **serveur menteur**).

Je n'ai rien à cacher

Le **fameux argument rabattu** et pourtant si néfaste au débat. Quand bien même n'aurions-nous rien à cacher, tout le monde a droit et besoin d'un espace privé, même si cela doit donc être à son corps défendant. Pour permettre l'introspection, se forger une intime conviction, hors de toute pression. C'est la liberté ultime, celle de pouvoir encore penser et réfléchir en libre arbitre.

La vie privée est un droit fondamental, liberté inaliénable et imprescriptible au sens de la Constitution. Et donc, il ne peut en ce sens y avoir ingérence de l'autorité publique dans l'exercice de ce droit ! Voilà qui est factuellement paradoxal au regard de la loi qui vient de nous être imposée.

> ***« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance », article 8 de la Convention Européenne des Droits de l'Homme***

Et c'est un réflexe : on ne se comporte pas de la même manière quand on se sait potentiellement observé, espionné. A minima, **l'autocensure guette**. On n'agit ni ne pense librement. L'effet de la surveillance sur le droit à la liberté d'expression peut avoir un effet paralysant, inspirer la crainte et inhiber les personnes concernées en les contraignant à la prudence dans leurs expressions et leurs agissements. Soit : les gens honnêtes s'autocensurent, tandis que les criminels ou terroristes contournent la surveillance.

> ***« La surveillance de masse crée une prison dans l'esprit qui est bien plus subtile mais bien plus efficace pour favoriser la conformité aux normes sociales, bien plus effective que la force physique ne pourra jamais l'être », selon Gleen Greenwald (journaliste à l'origine des révélations de Snowden)***

Encore n'aborde-t-on pas les **dérives inhérentes** à ce genre de techniques de surveillance quand elles sont ouvertes à de si nombreux services régaliens et organismes habilités.

En sus, **nous l'avions abordé**, ce qui intéresse au premier chef les autorités, ce sont nos réseaux de relation, les interconnexions dans la population. Qui communique avec qui ? Quand ? Où ?

Comment ? A quelle fréquence ? Combien de temps ?… Des précisions aussi violentes qu'une intrusion dans votre chambre à coucher. Et, par ces jeux de relations interhumaines quotidiennes, nous n'avons donc plus de vie privée si celle des autres est observée et enregistrée dans le même temps.

Aussi, si les gouvernements changent, les outils resteront. Pour quel nouvel usage alors ?

Dans un tel contexte, quelle solution citoyenne ? Comme il n'est pas question de s'isoler technologiquement, il convient d'adopter la stratégie de la pollution de masse à cette surveillance généralisée. Car cette dernière est une question technique, mais aussi totalement économique ! Ainsi, plus nous serons à **utiliser des outils de cryptographie**, plus il en coûtera de pratiquer ces renseignements de masse (stockage, décryptage, analyse).

C'est un dessein général conscient ou inconscient de nos législateurs : les sanctions pénales sont de plus en plus remplacées par des sanctions administratives, l'administration contrôlant étant aussi celle qui inflige, sans contrôle d'un juge judiciaire. Et une autorité administrative, fut-elle indépendante, n'est pas le véritable contre-pouvoir judiciaire indispensable à notre **tryptique démocratico-montesquiesque** ! Voilà un sacré paradoxe que de voir un pays démocratique sacrifier les libertés de ses citoyens pour faire face à une attaque menée par des gens qui haïssent cette liberté. Et pour un rapport coût/bénéfice bien faible, rappelons-le.

Mais les enjeux de cette loi ne sont pas simplement d'ordre sécuritaire. Il en va aussi d'un choix de société. Celle qui nous est offerte est de l'ordre de la gouvernance informatique (algorithmique), sans concertation nationale large, sans que la « justice judiciaire » ne puisse être partie prenante. L'humain sera ou devra se reléguer à des comportements archétypaux, stéréotypiques, à toutes fins de ne pas sortir de la majorité gaussienne, ne pas être catalogué « différent », « déviant ». Le différent (pour ne pas restreindre l'idée au seul étranger) étant le suspect, voire le danger.

Et plus généralement, comme l'avance Jean-Marc Manach

> ***« Ce vers quoi on va c'est beaucoup plus Minority Report [que Big Brother, ndr]. À savoir un monde où il y aura tellement de machines interconnectées et de plus en plus de machines qui vont décider à la place d'êtres humains et où, à des moments, il y a des machines qui vont vous dire non ».***

> ***« Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux », Benjamin Franklin***

Je vais vous faire une confidence. Moi aussi je rêve de trouver cette satanée aiguille dans cette fichue botte de foin.

Pour mieux dégonfler le monstrueux zeppelin qui nous est imposé au beau milieu de notre ciel bleu (parsemé certes de quelques nuages ombrageux, je ne suis pas atteint de cécité)…

Mise à jour (26/06/15)

Voilà. C'est fait. Après 3 petits mois de débat, **la loi sur le Renseignement** a été votée au Sénat le 23 juin, à l'Assemblée Nationale le 24 juin 2015). A nous les pratiques de surveillance intrusives et les atteintes aux libertés fondamentales !

Une loi finalement amendée et qui se retrouve plus attentatoire aux droits que prévu. Encore a-t-on échappé à cet amendement farfelu : « par dérogation au premier alinéa, lorsque la mise en œuvre sur le territoire national d'une technique de renseignement ne concerne pas un Français ou une personne résidant habituellement sur le territoire français, l'autorisation est délivrée par le Premier ministre sans avis préalable de la Commission nationale de contrôle des techniques de renseignement (CNCTR) ». Brèfle, de la surveillance sans contrôle contre les étrangers de passage finalement retoquée.

Vivement l'intervention de la Cour de Justice de l'Union Européenne (CJUE) pour tout le reste. Car au final, dans ces termes larges et flous, la loi permettra toutes les dérogations.

> ***« Il s'agit désormais de permettre aux services, quels qu'ils soient, de faire ce que bon leur semble », dixit Jean-Marie Delarue, ci-devant président de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), appelée à être remplacée par la CNCTR…***

Les associations et ONG restent mobilisées. Elles viennent de publier un **mémoire** pour accompagner la saisine parlementaire au Conseil Constitutionnel. Toutes les mesures y sont passées au crible. Lecture citoyenne indispensable donc pour la mise à jour des tenants et aboutissants de cette loi !

Soit, en résumé car cela vous a été signifié en détails (voir supra), un élargissement des finalités du renseignement, une légalisation massive de pratiques illégales des services de renseignement et introduction de techniques de surveillance de masse des communications électroniques, une absence de contrôle réel et indépendant et un recours des citoyens illusoire.

Cet élargissement des pouvoirs des services de renseignement français intervient alors que sont révélées (via des documents Snowden à nouveau) les pratiques américaines en matière d'espionnage des trois derniers présidents de la République. Outre la présidence de la République, plusieurs ministères ont été mis sous surveillance par la NSA. Cette dernière avait collecté les numéros de téléphone de responsables du ministère des affaires étrangères, de conseillers du président de la République sur les questions internationales (Afrique, Europe…). Et, semble-t-il, avait procédé au piratage de satellites de communication.

L'arroseur arrosé ? Des révélations accablantes en tout cas. Et toujours aucune information judiciaire ouverte !

En « marge », le GCHQ serait parvenu à pirater des routeurs de la marque américaine Cisco. De quoi intercepter les communications et dévier des pans entiers du trafic Internet vers ses propres dispositifs de surveillance. Les espions anglais se sont aussi attaqués à de nombreux logiciels grand public, notamment des programmes antivirus afin d'empêcher la détection de leurs activités.

Lurinas

Bonus : La société qui nous est promise

C'est un fait, les orpailleurs se reportent désormais sur les métadonnées, autrement plus lucratives.

Croire que ces données électroniques ne sont que piètres renseignements et que l'anonymisation d'icelles protègent ce qui nous reste de vie privée relève de l'inconscience sinon de la bêtise. C'est un fait démontré : les **données de connexion sont plus précises que le contenu** lui-même pour confondre une identité, les méta-données étant particulièrement bavardes. D'autant qu'elles sont infiniment plus faciles à analyser que les données complètes car plus structurées. Il n'y a, sur le net, de données qui ne puissent être identifiantes. La CNIL elle-même a déjà eu l'occasion de noter le paradoxe de données anonymes permettant de découvrir l'identité d'une personne lorsqu'un risque de terrorisme est détecté.

En cette prochaine étape, nous ne vivrons plus subséquemment de la même manière quand nos assurance, banque, complémentaire santé… sauront tout de nous, via des données en ligne sur nos recherches, nos déplacements, nos achats, etc.

C'est ce que tente de faire comprendre Thierry Collet dans son dernier spectacle « **je clique donc je suis** ». Nul besoin de télépathie hypertrophiée, désormais le mentaliste pourra se contenter des données personnelles des spectateurs directement accessibles sur les réseaux. L'expérience convaincra les présents que les nouveaux outils de captation et d'utilisation des données personnelles des grandes sociétés de l'Internet sont assez puissants pour géolocaliser, ficher, croiser à notre corps défendant.

Recommandations, pour aller plus loin dans la réflexivité

Le **livre en cours de confection** de Tristan Nitot

Citizenfour

Matin brun

Neuroland de Sébastien Bohler

Do Not Track, le Web-documentaire (7 épisodes accessibles ou à venir)

Sources

NextInpact

Les décodeurs de Le Monde

À la une

- Fous, et Alors ?
- Israël – Palestine : Un Festival pour se Toucher
- [Vox Pop] Le DG d'UBER en Garde à Vue
- [DOC] Daivika, Un Corps à Croquer
- Start Up Contest : 2 min pour Convaincre !

Le meilleur

- SEMAINE DE LA PRESSE ET DES MÉDIAS À L'ÉCOLE : LE MONTEUR
- PUTES PRIDE 2008
- SAUVER KOKOPELLI ? MAMÈRE A UNE IDÉE...
- SOUS LES PAVÉS... DENIS ROBERT – 1/3
- SOUS LES PAVÉS... DENIS ROBERT – 2/3

Journal

- [DOC] La Villeneuve : Objectif 8000€
- J'ai le SIDA. Touche moi...
- USA : Vortex Géant dans le Lac Texoma
- Tiny Hamster is a Giant Monster !
- [Rediff] Qui a Peur de l'Islam? Ce Soir sur France 4

À propos

- Qui sommes-nous ?
- L'association
- Ils nous soutiennent
- Charte éditoriale
- Mentions légales
- Nous contacter

Culture Économie Médias Monde Politique Société Sport

Le site LaTéléLibre.fr est propulsé par Wordpress • Conception : eGeny | Design : Stigmates Design.

(cc) BY-NC-ND — Tous les contenus, sauf exception signalée, sont sous licence Creative Commons.

LaTeleLibre.fr