Document

Prism: comment les Français sont écoutés par la NSA, et par des services bien de chez nous

(Slate.fr)

12.06.2013

PRISM. Cinq petites lettres n'arrêtent pas de faire trembler le Net. Derrière ce mystérieux anagramme, un dispositif de surveillance américain révélé le 7 juin dernier par le Guardian et le Washington Post, qui permettrait à la NSA, l'agence de sécurité nationale américaine, d'aller farfouiller librement dans le flot d'infos que laissent des ressortissants non-américains dans les serveurs des colosses du Net, qui eux sont bel et bien 100% Yankee. Pratique, car potentiellement un sacré paquet de monde, population française incluse, rentre dans le spectre de cette surveillance massive.

Le scandale vaut donc son pesant de cacahuètes, sans compter qu'il s'appuie sur une base parfaitement légale aux Etats-Unis : une loi, le FISAAA (Foreign Intelligence Surveillance Act Amendments Act), et en particulier son article 1881 qui autorise depuis 2008 *«la surveillance de masse ciblée uniquement sur les données personnelles en dehors des Etats-Unis»*.

Si aujourd'hui des incertitudes demeurent sur le degré de collaboration des «géants du Net» (Microsoft, Google, Facebook et autre Apple ont démenti en bloc et en détails avoir activement aidé à passer le Net à la moulinette de la NSA), reste la question de la surveillance qui s'opère actuellement dans les tuyaux, et notamment en France. Qui scrute quoi, avec quelle loupe et surtout quels garde-fous, chez nous? On vous explique tout.

1. PRISM, les Américains dans vos emails

«Seuls les citoyens non-américains sont visés, donc potentiellement, vous, moi, et quiconque vivant en France rentrent aujourd'hui dans la cible de PRISM», explique Grégoire Pouget, en charge des nouveaux médias à Reporters sans Frontières. Potentiellement donc, vos mails, vos photos, vos discussions en ligne -entre autres réjouissances détaillées par Le Monde dans un schéma- ont donc pu se retrouver sous les yeux d'un agent américain.

La France était-elle au courant de la présence d'un tel couteau Suisse dans la poche des Etats-Unis? La situation embarrassante: s'ils en avaient connaissance, ses services risquent de passer pour complices de tels agissements, s'ils les ignoraient, ils risquent vaguement de passer pour les dindons de la farce -pour rester polie.

J'ai contacté l'Elysée, ainsi que de nombreux ministères afin d'obtenir une réaction officielle: sans succès pour le moment, même si la Défense nous invite déjà *«à ne pas faire d'amalgames un peu rapides de ce qui est fait aux USA avec leur cadre légal et le cadre national français où toutes les pratiques de ce type sont fermement encadrées»* - précisément, on ne manquera pas d'y revenir.

Si la position de la France n'est pas connue, en Europe néanmoins, on s'agite un peu davantage. La députée Françoise Casteix, active sur ces questions, a ainsi demandé à la Commission européenne de *«confirmer l'existence de telles pratiques.»*

Dès 2012, un rapport du Parlement européen s'alarmait de l'existence de ce fameux dispositif FISAA, passé inaperçu à l'ombre du très médiatique (et tout aussi symbolique) Patriot Act:

Le paragraphe 1881 de FISAA a crée pour la première fois un droit à la surveillance massive spécifiquement ciblé sur les données de personnes non américaines situées hors des Etats-Unis, qui s'applique au cloud computing. [...] En conséquence, l'article 1881 de FISAA peut être considéré comme un risque pour la souveraineté de l'UE en matière de données formellement bien plus grave que d'autres lois jusqu'ici considérée par les législateurs européens.

Si PRISM, l'outil permettant la mise en oeuvre de cette atteinte *«à la souveraineté»* européenne était jusqu'ici inconnu aux autorités du vieux Continent, ces dernières étaient donc en revanche bien conscientes de l'éventualité d'une surveillance massive sur leurs territoires.

Il est évidemment difficile de savoir avec certitude si des Français, ou des voisins européens, se sont faits attraper dans les e-filets de la NSA. En revanche, mes interlocuteurs s'accordent à dire que l'action des services secrets américains est contraire au droit prévalant dans ces Etats. La Convention européenne des Droits de l'Homme (CEDH), en particulier, garantit la protection de la vie privée des ressortissants de ses 47 membres, Union européenne comprise. *«Dans la mesure où il y a ici plusieurs fondements aux atteintes à la vie privée, on peut imaginer des recours»*, estime Estelle de Marco, juriste spécialiste de ces questions. Contre les acteurs du Net, d'abord, également tenus de se conformer au droit européen en matière de vie privée, mais, plus surprenant, contre les États eux-mêmes :

«L'Etat français, comme les autres signataires de la CEDH, pourrait être attaqué pour ne pas avoir protégé la vie privée de ses citoyens. Cette protection est une obligation positive : l'Etat ne doit pas simplement s'abstenir d'y porter atteinte, il doit aussi faire en sorte qu'il n'y ait pas de limitations arbitraires. Ce scénario ne s'est jamais vu à ce jour mais ce n'est pas inenvisageable.»

2.Echelon, papi fait de la surveillance

«Mais... vous avez oublié Echelon ?» Echelon, c'est un peu le grand papa de PRISM. Et surtout le grand oublié de cette affaire. Car la NSA est loin d'être à son premier coup d'essai en matière de surveillance massive des communications - en même temps, elle a été créée pour ça.

Tout comme PRISM aujourd'hui, Echelon est un système de surveillance planétaire, qui surveille appels, fax, mails, bref, l'ensemble des communications internationales (et donc y compris Internet). Mais depuis les années 1980. Et en collaboration avec la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande...

Entre ça, Prism, et les outils que nous ignorons certainement encore, on comprend mieux pourquoi la NSA avait besoin de son titanesque centre de stockage, classé secret-défense et sur le point d'être finalisé. Deux milliards de dollars pour 100.000 mètres carrés et une capacité de stockage jamais égalée de 5 zettaoctets, soit 5.000.000.000.000.000.000.000 octets, ou, comme le précise Le Monde, 250 milliards de DVD. A la NSA, on voit les choses en grand. Et qui sait? Vos informations auront peut-être l'honneur de se retrouver dans ses super locaux.

3.La Pnij, interceptions à la française

Géolocalisation, écoute, facture détaillée et j'en passe: la France est solidement dotée en matière d'interceptions des communications. Un système qu'elle tente d'ailleurs de moderniser et d'améliorer

en le centralisant au sein de la Pnij. C'est le petit nom de la Plateforme nationale des interceptions judiciaires, les futures grandes oreilles de l'Etat.

Lancé avec la bénédiction de Nicolas Sarkozy, ce grand chantier vise à centraliser en un lieu unique toutes les interceptions judiciaires. En clair, dès qu'un officier de police judiciaire, un gendarme ou un douanier obtiendra l'autorisation d'un juge, dans le cadre d'une enquête, d'intercepter des communications téléphoniques ou électroniques, tout ses faits et gestes se feront en ces lieux. C'est au sein de cette plate-forme que l'agent demandera par exemple les informations qui l'intéressent à l'opérateur de la personne surveillée (Orange, Free, SFR...). Mieux qu'un bouquet satelllite: il piochera dans un catalogue de prestations offertes par l'opérateur, et ce dernier renverra ces informations dans cette plate-forme, qui pourront alors être écoutées, disséquées et commentées.

Un peu à la manière de PRISM, signe de la volonté de la NSA d'automatiser sa relation avec les acteurs du Net pourvoyeurs de données personnelles, la Pnij a été justifiée par une recherche d'économie de coûts et de moyens. Mais à l'image des Google, Microsoft, Facebook et Apple dans l'affaire américaine, Orange, Free, SFR et Bouygues (contrairement au cas de figure américain, les opérateurs de télécommunications, qui fournissent abonnements téléphoniques et à Internet, sont les seuls acteurs sollicités dans le cadre de la Pnij) se défendent bien d'avoir mis en place un accès direct entre leurs serveurs et les surveillants. *«Ce sont des équipements qui parlent entre eux*, nous indique-t-on du côté des intéressés, *il y a toujours une passerelle d'intermédiation.»*

C'est l'épineuse question des «backdoors», ou «portes dérobées», qui donneraient aux autorités un accès direct et non contrôlé aux serveurs des différents acteurs sur lesquels nous nous appuyons pour accéder à Internet. Et qui donne aujourd'hui tant de fil à retordre aux géants du Net américains, qui se défendent en plein scandale PRISM de fournir un tel blanc-seing aux espions américains.

«Attention à ne pas faire d'amalgame» comme s'est empressé de m'avertir le ministère de la Défense, la Pnij ne peut être comparé en tout point à l'outil de surveillance massive américain. De l'avis de tout nos interlocuteurs, c'est un système bien plus encadré, qui nécessite notamment l'accord d'un magistrat du siège dès qu'il s'agit de fouiller le contenu de nos communications. Ceci dit, il traîne tout de même son lot d'inquiétudes.

En particulier, le fait de concentrer entre les mains d'un unique prestataire, qui plus est privé (puisque c'est Thalès qui a été désigné pour s'occuper du bébé) des informations sensibles concernant potentiellement tous les Français pose de graves problèmes de sécurité.

4.Ecoutes administratives: la surveillance très très secrète

C'est la version gros bras du point précédent. Même principe, la puissance publique souhaite mettre son nez dans les communication d'un individu, sauf que le juge n'a aucun droit de regard. Ce qui en fait une procédure exceptionnelle, évidemment auréolée d'un secret plus grand encore que celui entourant les écoutes «classiques» décrites plus haut.

La décision de mener ce genre de surveillance fait suite à *«une proposition écrite et motivée des ministres en charge de la défense, de l'intérieur ou des douanes»*, peut-on lire sur le site du ministère de l'Intérieur. Elle appartient au Premier ministre et est limitée par un certains nombres de motifs, tels que *«la sécurité nationale»*, *«la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France»* ou bien encore la *«prévention du terrorisme»*. Une commission spéciale, la Commission nationale de contrôle des interceptions de sécurité, donne son avis *a posteriori*.

«Des garanties sont mises en oeuvre, estime la juriste Estelle De Marco, *mais elles sont opaques»*. En particulier, la liste des motifs invoqués, certes limitative, met en avant des concepts qui restent suffisamment généraux pour être flous.

5. *DPI comme chez Kadhafi ?*

DPI, pour *«Deep Packet Inspection»*. Ou, plus clairement, pour une technologie qui permet de sonder en profondeur et en détail le trafic Internet, jusque dans les mails et le type de pages consultées. Art dans lequel la France est experte.

Ce savoir-faire est devenu célèbre lorsque le monde a appris que deux entreprises bien de chez nous avaient vendu cette technologie de surveillance à deux dictatures: la Libye et la Syrie. Amesys pour feu Kadhafi, Qosmos pour Bachar Al-Assad. Grâce à ces outils, dits *«à double-usage»* (pile pour le civil, face pour une utilisation militaire), les deux tyrans ont pu contrôler toutes les communications qui entrent et sortent du pays. Pratique, lorsqu'on souhaite surveiller toute une population. Et lucratif: à en croire des documents révélés par WikiLeaks, le marché de la surveillance sur Internet est en effet en plein boom.

Forcément, avec de tels faits d'armes, beaucoup redoutent donc que cette technologie soit utilisée en France aux mêmes fins, sans garde-fous. Certains opposent que le DPI est depuis longtemps utilisé à des fins de gestion de trafic d'Internet, plus pour faire de la maintenance que de la surveillance.

Mais selon feu Owni, la société Amesys aurait vendu «au moins sept systèmes d'espionnage des télécoms aux militaires, services de renseignement et policiers français». Le Canard Enchaîné ou Le Figaro vont plus loin, évoquant en France des pratiques similaires à celles instaurées en Libye.

Lors de l'enquête menée avec Pierre Alonso sur la Pnij, que j'évoquais au point 1 de cet article, et qui nous a valu quelques démêlés avec le contre-espionnage français, le fantôme du DPI rôdait aussi. Pour certains médias, la plateforme d'écoutes s'appuierait en effet sur cette technologie, ce dont s'est défendu le service du ministère de la Justice en charge de ce chantier. Sans que ses explications soient très convaincantes, puisque comme il l'avoue lui-même: «*des technologies d'interceptions, il n'y en a pas des cents et des milles.»* Reste à savoir comment on les utilise et on les encadre.

6. Chère conservation des données

En France, les acteurs du Net, qu'ils soient fournisseurs d'accès (Orange, Free et compagnie) ou hébergeurs (comme Google) ont l'obligation de conserver les données liées aux communications en ligne de leurs utilisateurs. Dans le but assumé, indique la loi dite sur la confiance en l'économie numérique (LCEN), de *«permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne.»*

Adresse IP, date et heure du début et de fin de la connexion, mais aussi informations laissées lors de la création de compte sur les sites Internet (de l'adresse au numéro de téléphone) peuvent ainsi être demandées par un officier de police judiciaire, dans le cadre d'une enquête. Mais attention, prévient Estelle De Marco: *«cette conservation ne doit pas porter sur les données liées au contenu de la communication.»*

Une différence de taille: si les enquêteurs veulent connaître le détails des activités en ligne de la personne surveillée, il faudra alors passer par la case juge. A savoir la procédure détaillée au point 1. de cet article.

Une subtilité essentielle pour garantir la préservation de la vie privée des citoyens, mais qui n'empêche pas certains officiers de police judiciaire de tenter leur chance auprès de certains acteurs du Net. *«Certains semblent avoir tendance à demander aux FAI et aux fournisseurs de service des informations qu'ils ne sont pas censés obtenir dans ce cadre là»*, raconte Estelle de Marco.

Information qui nous a été confirmée par nombre de ces acteurs. Et qui se révèle particulièrement efficace *«du côté des plus petits acteurs,* ajoute Cédric Manara, autre juriste spécialiste de ces questions, qui, *lorsqu'ils sont sous le coup d'une lettre recommandée des autorités, forcément répondent.»* Voir débouler une demande d'accès aux informations siglée d'une jolie Marianne et enveloppée d'une lettre recommandée, ou recevoir un coup de fil de policiers, fait à coup sûr son petit effet.

Seules les grosses boîtes, disposant de services juridiques musclés, ont la capacité de dire non à ces demandes excessives.

C'est par exemple le cas de Google, qui a retourné cette obligation légale en arme marketing: dans son *«Transparency report»*, la firme américaine fait ainsi publiquement étalage du nombre de demandes de renseignements qu'elle reçoit, pays par pays. En France, elle indique par exemple n'avoir accédé qu'à la moitié de ces requêtes sur la période 2010-2012.

7.L'Hadopi, surveiller la propriété

Bientôt enterrée, mais loin d'être oubliée, l'Hadopi aura marqué une nouvelle ère en matière de surveillance du Net français. Et a priori, c'est loin d'être fini! Avatar symbolique de la banalisation du palpage de réseaux, le bras armé de la Haute autorité permet de coincer les individus dont la connexion à Internet aurait servi à se procurer illégalement des oeuvres protégées par le droit d'auteur. Un dispositif qui permet de scruter les réseaux peer-to-peer à la recherche de ceux qui téléchargeraient des œuvres puisées dans un catalogue périodiquement renouvelé mais limité (10.000 chansons et une centaine de films seulement).

«On est passé d'une surveillance au motif de lutte contre le terrorisme à une surveillance pour la propriété intellectuelle!», s'offusque Cédric Manara.

Une sorte de radar automatique placé sur Internet au nom de la propriété intellectuelle et mis à la disposition des industries culturelles. L'analogie devrait prochainement s'avérer d'autant plus exacte que le gouvernement souhaite remplacer la suspension de l'accès à Internet, menace ultime de la riposte graduée, mais également inapplicable, par une amende qui serait elle, nettement plus effective.

8.Peur sur les routeurs

C'est un murmure récurrent sur les réseaux: les routeurs, ces équipements incontournables situés au coeur du Net, seraient les mouchards rêvés des services secrets. Témoins du passage de tout le trafic Internet, ces machines permettraient à leurs pays d'origine de garder un œil attentif sur ce qui circule dans les tuyaux.

Un doute *«qui a toujours existé»*, nous confirme-t-on du côté des opérateurs, et qui s'est surtout porté, ces derniers mois, sur les constructeurs chinois de tels équipements: Huawei, ou encore ZTE, étant priés de ne pas mettre leur nez dans l'infrastructure des réseaux américains et européens. En France, un récent rapport sur la cyberdéfense préconise carrément de ne pas faire appel aux services de ces entreprises, jugées trop proches du régime chinois et présentant donc *«un risque pour la*

sécurité nationale». Même rengaine aux Etats-Unis, où l'on redoute comme la peste la présence (là encore!) de «backdoors» dans ces boîtiers. Pourtant, les Etats-Unis, qui fournissent depuis longtemps ce genre d'équipements (par exemple via Cisco), ne sont pas à l'abri de ces mêmes critiques. Et d'autant plus aujourd'hui, avec le scandale PRISM!

Un dispositif qui se révélerait bien pratique, mais difficile à prouver. Comme à réaliser. *«Les routeurs ont des processeurs de très faible capacité,* commente l'ingénieur réseaux Stéphane Bortzmeyer. *Cela signifie que si on veut traiter les données qui passent par là, il faut les transporter vers Washington ou Pékin. Or balancer 100 Gigabits par seconde d'informations, c'est compliqué en termes techniques. Et ça se voit.»* Un manque de discrétion confirmé par certains opérateurs, parfois témoins de ce genre de pratiques.

«Chaque ressource, tuyau ou machine, permettant d'aller sur Internet peut être l'objet de surveillance publique ou privée», rebondit Cédric Manara. *«Nos communications laissent forcément des traces, le problème est qui y a accès et jusqu'à quel point.»*

...*Surveillance : vers l'infini et au-delà*

Et justement, sur ce point, l'histoire est loin d'être terminée. Car les données, publiques ou privées, aiguisent tous les appétits. Police, entreprises, scientifiques et même services fiscaux: ils ne pensent qu'à ça! Ruée vers l'or des temps modernes, espoir d'une nouvelle économie, voire d'un modèle de société inédit, l'intérêt croissant pour les données multiplie aussi les outils qui permettent de mieux les extraire et de les analyser. Ainsi que les motifs et les personnes qui y ont accès.

Cédric Manara raconte ainsi que dans le cadre de contentieux commerciaux, il arrive de plus en plus souvent qu'une des parties demande au juge d'accéder à l'historique Internet de la partie adverse. *«Une personne peut donc, sous réserve d'acceptation du juge, accéder aux données personnelles d'autres personnes dans le cadre d'une affaire privée»,* conclut-il.

Estelle De Marco quant à elle, explique son engagement au sein du projet européen ePoolice. Une recherche qui vise à développer un outil de détection précoce du crime organisé qui, s'il n'est *«pas vraiment une collecte de données»,* peut *«aussi permettre de surveiller les citoyens»*. La juriste a pour tâche, aux côtés d'autres spécialistes, *«d'éviter ces risques.»* Sans forcément puiser dans les données personnelles, ce genre de programmes permet aussi d'assembler des informations publiques, des informations annexes, qui, une fois agrégées, permettent de donner un profil très détaillé des individus. *«La valeur des métadonnées est très importante*, souligne Stéphane Bortzmeyer, *ce qu'on a tendance à sous-estimer.»*

«Ce type de projets est à la mode», ajoute la juriste. A tel point qu'ils en sont devenus presque banals. *«En 1998, la conservation des données et la surveillance faisaient peur*, se souvient la juriste. *Depuis quinze ans, tous les acteurs qui s'alarmaient très facilement considèrent désormais comme acquises certaines surveillances alors perçues comme inacceptables.»*

Preuve en est la réaction blasée parfois suscitée par les révélations sur PRISM. Par confort, habitude et peut-être lassitude, nombre d'entre nous ne s'offusquent pas (ou plus) de l'existence de tels outils, qui permettent de tripoter les données qui nous concernent comme de la pâte à modeler, sans assurer les garde-fous essentiels à la protection de notre vie privée. Finalement, *«le vrai problème de Prism, c'est sa base légale*, conclut Cédric Manara. *Qu'un outil aussi puissant soit autorisé et utilisé par un Etat. Prism a juste prouvé qu'en matière de surveillance, nous avons pris des réflexes funestes.»*