La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux
Actualités Droits-Libertés | 2015

Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne

Droit a la vie privée et protection des données personnelles (Assemblée Parlementaire du Conseil de l'Europe)

Marine Farshian

revues.org

Éditeur
Centre de recherches et d'études sur les droits fondamentaux

Édition électronique
URL : http://revdh.revues.org/1300
DOI : 10.4000/revdh.1300
ISSN : 2264-119X

Référence électronique
Marine Farshian, « Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 28 mai 2015, consulté le 01 octobre 2016. URL : http://revdh.revues.org/1300 ; DOI : 10.4000/revdh.1300

Ce document a été généré automatiquement le 1 octobre 2016.

Quand la réalité de la surveillance massive tend à dépasser la fiction orwellienne

Droit a la vie privée et protection des données personnelles (Assemblée Parlementaire du Conseil de l'Europe)

Marine Farshian

1 « *Son courage et son dévouement à la cause de la liberté et au respect de la vie privée sur Internet, en dépit du danger que cette entreprise pouvait représenter pour sa sécurité et sa liberté, imposent le plus grand respect.* » C'est en ces termes qu'un rapport de l'Assemblée Parlementaire du Conseil de l'Europe adopté le 21 avril dernier évoque les révélations d'Edward Snowden.

2 Ce « *lanceur d'alerte* »[1] a révélé l'ampleur de la menace pour nos droits et libertés que constitue la surveillance massive des communications de centaines de milliers de personnes par la NSA et les services de renseignements d'Etats "partenaires" des Etats-Unis. Les citoyens de nombreux Etats membres du Conseil de l'Europe ont ainsi récemment appris que leurs communications et leurs métadonnées ont été – et sont encore - collectées puis conservées à grande échelle. Pour exemple, en l'espace d'à peine un mois, la NSA aurait recueilli 97 milliards d'informations à l'échelle du globe, et conservé les données de milliards de SMS échangés par des individus lambda[2].

3 De cette prise de conscience, il résulte que tout internaute a désormais connaissance de la possibilité – voire de la probabilité – d'être victime de surveillance, et donc des risques encourus lorsqu'il s'exprime ou s'informe sur la toile. **La surveillance de masse a déjà et aura demain davantage encore un effet délétère** sur l'exercice de libertés telles que la liberté d'expression ou d'information. Vivement préoccupée, l'Assemblée Parlementaire du Conseil de l'Europe adopte donc un rapport édifiant et extrêmement critique, justifiant une série de recommandations adressées aux Etats membres pour tenter de répondre à la menace.

4 S'il relaie certaines informations précédemment publiées dans la presse, le rapport parlementaire présente un état des lieux exhaustif nécessaire pour appréhender l'étendue de la menace représentée par la surveillance massive de nos communications pour la vie privée de tous (**1°**). Cette mise en perspective permet alors de saisir l'urgence et la nécessité de réformer, préciser et actualiser un cadre juridique manifestement inadapté, en ce qu'il a failli à assurer la protection effective de la vie privée de milliers de citoyens (**2°**). Sous l'impulsion du Conseil de l'Europe et de la Cour européenne des droits de l'homme, l'enjeu pour les Etats membres est désormais d'oser instaurer un véritable encadrement et contrôle des mesures de surveillance (**3°**).

1°/- L'étendue massive de la surveillance des télécommunications et des violations du droit à la vie privée

5 Si le web est un réseau sans frontière, **la localisation matérielle des infrastructures d'internet et la position dominante des sociétés américaines sur le marché** impliquent que les Etats-Unis et le Royaume-Uni sont en mesure de collecter puis de conserver un nombre incalculable de données concernant l'ensemble des habitants de la planète. Grâce à son programme PRISM, la NSA a accès aux données personnelles de clients de sociétés privées tenues de coopérer – avec ou sans le consentement de leurs clients – sur autorisation d'un juge, mais au terme d'une procédure secrète (§ 10 du rapport). Google, Microsoft et Yahoo ont ainsi permis à l'Agence d'accéder notamment aux emails de leurs clients et à leur contenu, aux historiques de conversations, aux communications téléphoniques ou encore aux données captées sur les réseaux sociaux. La NSA et son homologue britannique le GCHQ – partenaire privilégié – ont également obtenu de certaines sociétés spécialisées un accès aux « trappes » ou failles secrètes de leurs systèmes, qui leur permet de contourner le cryptage des communications (§ 63 à 65 du rapport).

6 **En réaction, le Parlement Européen souhaite imposer aux sociétés américaines l'obligation de solliciter les autorités de l'Union avant de répondre à toute injonction** de transmettre les informations personnelles de consommateurs européens. La création d'un espace de stockage européen des données, « cloud » situé en Europe, est même envisagée comme une possible solution (§ 108 du rapport). Pourtant, les sociétés européennes n'apparaissent pas plus vertueuses. En effet, en France la DGSE coopère de manière « non-officielle » avec la société Orange et bénéficie – à l'insu de tout contrôle judicaire ou autre – d'un accès libre et total aux flux de données des clients de l'entreprise, grâce à des connexions « informelles » existant entre des ingénieurs qui naviguent entre les deux bords[3].

7 **Outre l'accès « officiel » dont elles bénéficiaient, la NSA et le GCHQ ont également intercepté « clandestinement » des données provenant de ces sociétés** dans le cadre d'un programme secret MUSCULAR. Le GCHQ a collecté et conservé en vrac des images extraites des webcams d'utilisateurs de la messagerie instantanée Yahoo, y-compris de nombreuses communications à caractère sexuel, sans qu'il s'agisse nécessairement de personnes ciblées par les services de renseignements[4]. Plus grave encore, ces agences ont volontairement fragilisé des systèmes de sécurité : soit en achetant certaines sociétés afin qu'elles abaissent le niveau de sécurité dont bénéficient leurs clients, soit en allant

jusqu'à utiliser des logiciels malveillants. Ces opérations de piratage consistent à prendre le contrôle d'un ordinateur pour activer secrètement le microphone ou la webcam, enregistrer des conversations ou réaliser des clichés, mais également à consulter l'historique du navigateur internet ou hacker une messagerie électronique.

8 Le GCHQ a également perpétré des cyber-attaques contre des personnes étrangères à toute entreprise terroriste et ne présentant aucune menace pour la sécurité nationale, en bloquant notamment l'accès à des forums de discussion utilisés par les cyber-militants d'Anonymous. De simples citoyens ont été placés sous surveillance simplement parce qu'ils cherchaient à protéger le caractère privé de leurs communications, notamment grâce à un logiciel de cryptage (le meilleur moyen de sécuriser vos télécommunications à l'heure actuelle), tandis que d'autres encore ont été espionnés en raison de leur activité politique, diplomatique, journalistique, d'avocat ou de militant en faveur des droits de l'homme (§ 43, 47, 53 et 60 du rapport). Autre exemple édifiant, l'accès à internet gratuit d'un aéroport canadien a été utilisé pour surveiller les dispositifs wifi de milliers de passagers ordinaires plusieurs jours après leur vol. Il s'agissait alors du test d'un nouveau logiciel puissant, désormais opérationnel, mis au point par les autorités canadiennes en collaboration avec la NSA[5].

9 Enfin, le GCHQ a tenté de manipuler l'opinion publique en publiant de faux documents sur internet attribués à certaines personnes ou sociétés, de faux commentaires, des faux témoignages de victimes[6], en gonflant artificiellement le nombre de visiteurs de certains sites, voire en connectant deux téléphones au cours d'un appel[7]. Or, de tels procédés reviennent à fabriquer de toutes pièces des preuves susceptibles d'être invoquées au cours d'un procès, en violation flagrante du droit à un procès équitable, des droits de la défense et des principes de l'Etat de droit (§ 60 du rapport). En tout état de cause, l'ensemble de ces pratiques de surveillance massive et d'espionnage politique s'avèrent difficilement justifiables par des impératifs de prévention du terrorisme ou liés à la sécurité nationale, et discréditent certainement le discours officiel.

*

2°/- La nécessaire actualisation d'un cadre juridique visiblement inadapté à la protection de la vie privée

10 La Convention européenne des droits de l'homme consacre le droit au respect de la vie privée (article 8-1), à l'instar d'autres instruments internationaux et de constitutions nationales. Dès 1978, **la Cour européenne fait entrer les communications téléphoniques dans le champ d'application de la « correspondance » dont le caractère privé est protégé** par la Convention[8]. Cependant, au-delà du contenu même des communications, les smartphones et autres génèrent désormais des métadonnées : de nombreuses informations de nature privée et extrêmement précises, concernant notamment nos déplacements, nos fréquentations etc.

11 Or, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, seul instrument international contraignant dans ce domaine, **définit précisément les « données à caractère personnel » comme « toute information concernant une personne physique**

identifiée ou identifiable ». Les données captées massivement par les programmes de surveillance s'apparentent donc à des données personnelles, et doivent par conséquent être protégées. Il s'avère que la collecte et la conservation de métadonnées constituent per se une ingérence dans la vie privée d'une personne, que ces données soient utilisées ou non par la suite[9]. Même des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et conservées dans des fichiers détenus par les pouvoirs publics[10].

12 Pourtant, les révélations d'Edward Snowden ont fait apparaître **non seulement la cruelle absence de dispositions censées protéger les citoyens, mais surtout des carences manifestes dans l'application effective** des dispositions en vigueur. Du point de vue de la Cour Européenne, il est impératif qu'en matière de surveillance, la loi pose un minimum de garanties contre les abus des pouvoirs publics. La loi doit énoncer de manière suffisamment claire et précise la nature, l'étendue et la durée des mesures, les motifs exigés pour les ordonner, les autorités compétentes pour les autoriser, les exécuter et les contrôler, et le type de recours prévu par le droit interne[11].

13 Sur le territoire européen, les législations internes encadrent plus ou moins strictement la possibilité pour un gouvernement donné d'espionner des particuliers sans aucun motif et en dehors du contrôle d'un juge. Des Etats tels que la France ou l'Allemagne collaborent donc avec leurs partenaires et reçoivent des données collectées par des services de renseignements étrangers tels que la NSA, y compris relatives à leurs propres ressortissants[12]. Selon le rapport, **les gouvernements de ces Etats européens ont ainsi entendu contourner leur propre législation** et les restrictions censées protéger les personnes placées sous leur juridiction (§ 30-37 du rapport). Cependant, le rapport insiste moins sur la coopération active des autorités de pays européens avec la NSA, cela en flagrante violation du droit à la vie privée tel que protégé par la Convention Européenne. Ainsi, la DGSE livre pour sa part à la NSA sans aucun tri des millions de données relevant de la vie privée de Français ou d'étrangers, en captant les données transmises par des câbles sous-marins transitant sur le territoire français[13].

14 **En tout état de cause, l'absence de dispositions prévoyant et réglementant un quelconque transfert d'informations captées par des services de renseignements étrangers permet de sérieusement questionner la licéité de ces pratiques**. En effet, l'absence de dispositions légales, de quelconques garanties ou mécanismes de contrôle, n'est certainement pas assimilable à un prétendu « vide juridique ». Dès lors que, selon un principe fondateur de l'Etat de droit, les particuliers doivent pouvoir régler leur conduite en prévision des conséquences que leurs actions peuvent emporter. Il s'agit au contraire de constater un grave manquement des Etats à l'exigence de prévisibilité de la loi posée par l'article 8-1 de la Convention[14].

15 Ayant rappelé l'urgence pour les Etats membres de modifier leur législation afin de se conformer aux dispositions de la Convention, le Conseil de l'Europe milite également pour la consécration à l'échelon régional et international de principes fondamentaux applicables en matière de surveillance. Ainsi, l'Assemblée Parlementaire défend l'élaboration d'un « Code du renseignement » censé définir des standards communs que les Etats s'engageraient à respecter (Projet de recommandation, § 2.2). De fait, la coopération européenne des services de renseignement aux fins de lutte contre le terrorisme ou la criminalité organisée inscrirait toute mesure de surveillance ou échange d'informations privées dans un cadre juridique commun, et exclurait toute surveillance des particuliers à visée politique ou économique.

*

3°/- Le strict encadrement et le contrôle effectif des mesures de surveillance, conditions du respect de la vie privée

16 **Les instances européennes entendent désormais demander des comptes aux Etats membres sur les mesures prises** par ces derniers à la suite des récentes révélations pour garantir le respect effectif du droit à la vie privée (ceci au moyen d'une enquête diligentée par le Secrétaire Général, tel que le prévoit l'article 52 CESDH). Si la Cour reconnaît pour sa part l'utilité des dispositifs secrets de surveillance pour lutter contre des menaces telles que le terrorisme ou la criminalité organisée, elle insiste également sur le caractère exceptionnel de ces mesures et sur la nécessité de cibler des « éléments subversifs ». La Cour a d'ailleurs toujours rappelé aux Etats que la fin ne justifie pas tous les moyens, et qu'il importe de ne pas fragiliser l'Etat de droit au motif de le défendre. La Cour fait ainsi preuve de cohérence en considérant que, malgré la menace terroriste, « *les Etats ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction* »[15].

17 Or, afin de se conformer aux principes et droits fondamentaux qui sous-tendent leur adhésion au Conseil de l'Europe, les Etats membres doivent amender leur propre législation de sorte que la collecte de données personnelles ne soit permise que lorsque l'intéressé y a préalablement consenti, ou à défaut de manière exceptionnelle, lorsqu'un juge l'autorise sur la base de motifs raisonnables de soupçonner la participation de l'intéressé à des activités criminelles. Toute collecte ou conservation de données privées en dehors de ce cadre doit relever de sanctions pénales, au même titre que la violation du secret des correspondances classiques. De même, la création de failles de sécurité telles que celles orchestrées par la NSA doit être aussi sévèrement condamnée (§ 113 du rapport).

18 **Néanmoins, en pratique, le secret qui entoure le fonctionnement de ces systèmes de surveillance massive implique qu'il s'avère relativement difficile pour les dirigeants politiques d'apprécier l'étendue de la menace, mais également de déterminer les mesures adaptées pour permettre un réel contrôle démocratique** de ces systèmes – impartial, indépendant et transparent (§ 100-102 du rapport). De nombreux responsables politiques ont ainsi affirmé n'avoir eu aucune connaissance des mesures de surveillance opérées par leurs services de renseignement. Qu'il s'agisse d'une ignorance feinte ou avérée, il y a lieu de s'inquiéter de la perte de contrôle sur ces programmes de surveillance et de l'emballement de cette machine infernale, dont une partie des activités a été externalisée au profit de sociétés privées.

19 **La Cour européenne s'est d'ailleurs montrée extrêmement prudente, formulant une mise en garde contre les risques d'abus inhérents à tout système de surveillance secrète et rappelant la difficulté de mettre en place des mécanismes de contrôle effectifs**[16]. « *Le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret* »[17]. Seule la conjugaison de mécanismes de contrôle administratif, judiciaire et/ou parlementaire convaincants des programmes de

surveillance permettra de garantir effectivement le respect du cadre juridique en vigueur, et de protéger efficacement la vie privée de tous. Cela implique nécessairement d'instaurer davantage de transparence dans le fonctionnement de ces systèmes de surveillance, afin que les instances en charge de ces contrôles puissent accéder aux informations pertinentes (§ 96 et 114 du rapport). Dans le cadre de son examen, la Cour observe ainsi le fonctionnement des instances de contrôle afin d'apprécier si celles-ci sont réellement indépendantes des autorités en charge de la surveillance, et si ces instances bénéficient de compétences suffisantes pour exercer un contrôle effectif et constant sur le processus de surveillance[18].

*

* *

20 Tout particulièrement depuis la chute des tours du World Trade Center, se pose la question du délicat équilibre entre la protection des droits et libertés de chacun, et la sécurité de tous au moyen d'outils efficaces et proportionnés. Si la surveillance de télécommunications peut s'avérer nécessaire dans une société démocratique, le Conseil de l'Europe entend rappeler que celle-ci doit naturellement s'inscrire dans le respect des principes de l'Etat de droit.

21 Dans le cadre du débat lancé **aux Etats-Unis et en Europe**, **des études indépendantes ont depuis démontré l'inefficacité de la surveillance de masse** par rapport aux techniques classiques de surveillance ciblée**,** en ce qu'elle disperse inutilement les moyens et fonds alloués au lieu de les focaliser sur des cibles pertinentes[19]. En somme, à force d'espionner tout le monde, les services de renseignements perdent de vue les véritables suspects et accroissent inévitablement le risque de manquer une information essentielle permettant, par exemple, de déjouer un attentat ou une entreprise criminelle.

22 Paradoxalement, c'est au nom d'un sacro-saint impératif de sécurité nationale que **les agences de renseignement ont pris le risque d'accroître la vulnérabilité** de citoyens ordinaires ou d'instances politiques aux attaques de cyber-terroristes, mais également l'exposition de certains opposants politiques à la répression des autorités de régimes non démocratiques. Or, contrairement au discours tenu par de nombreux responsables politiques afin de légitimer l'adoption de lois toujours plus liberticides, l'impératif de sécurité nationale peut et doit être concilié avec la protection de la vie privée. En effet, garantir la sécurité des télécommunications et la protection des données personnelles permettra de protéger plus efficacement un Etat et ses ressortissants contre la cybercriminalité.

23 En outre, faut-il rappeler que lorsque le « scandale » de la NSA a éclaté, l'agence a persisté à nier qu'Edward Snowden avait pu avoir accès aux données qu'il prétendait détenir. Or, **le cours des évènements a démontré que l'agence est incapable de garantir la sécurité des informations qu'elle intercepte** et conserve en toute illégalité dans le cadre de ses opérations massives de surveillance. Si ces informations devaient tomber entre de mauvaises mains, la sécurité nationale en serait inévitablement compromise... Partant, si le plus fervent défenseur de la NSA n'était pas encore convaincu à ce stade de l'illégalité doublée de l'inefficacité de ses activités, il ne pourrait que constater une telle évidence. La conclusion logique étant que la NSA ne peut et ne doit manifestement pas

continuer à intercepter et conserver des informations privées qu'elle n'est pas même en mesure de protéger.

*

24 **Assemblée Parlementaire du Conseil de l'Europe, Commission des questions juridiques et des droits de l'homme, « Les opérations massives de surveillance », Rapport adopté le 21 avril 2015 – AS/Jur (2015) 01**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Sur cette notion en droit européen, v. not. Jean-Philippe Foegle, « Un renforcement en demi-teinte du statut du lanceur d'alerte dans l'"Europe des droits de l'homme" », in Revue des droits de l'homme, 11 mars 2015.

2. "Boundless Informant: NSA explainer", The Guardian, 8 juin 2013.

3. « Espionnage : comment Orange et les services secrets coopèrent », Le Monde, 20 mars 2014.

4. Sur un semestre, plus d'1.8 millions de comptes sont concernés, « Optic Nerve : millions of Yahoo webcam images intercepted by GCHQ », The Guardian, 28 février 2014.

5. "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents", CBC News, 30 janvier 2014.

6. "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations", The Intercept, 24 février 2014.

7. "Hacking Online Polls and Other Ways British Spies Seek to Control the Internet", The Intercept, 14 juillet 2014.

8. Cour EDH, 6 septembre 1978, Klass et autres c. Allemagne, Requête n° 5029/71.

9. Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, 20 juin 2014, « Le droit à la vie privée à l'ère du numérique » §20.

10. Cour EDH, G.C. 4 mai 2000, Rotaru c. Roumanie, Req. n° 28341/95, § 43.

11. Cour EDH, 28 novembre 2011, Shimovolos c. Russie, Requête n° 30194/09, § 68.

12. "Cover Story: How the NSA Targets Germany and Europe", Der Spiegel, 1er juillet 2013.

13. « Surveillance : la DGSE a transmis des données à la NSA américaine », Le Monde, 30 octobre 2013.

14. 1 suivre, l'affaire pendante Big Brother Watch et autres c. Royaume-Uni, requête n° 58170/13.

15. Cour EDH, 6 septembre 1979, Klass et autres c. Allemagne, Req. n° 5029/71, §48-49.

16. Cour EDH, 28 novembre 2011, Shimovolos c. Russie, Req. n° 30194/09, §68.

17. Cour EDH, 6 septembre 2006, Segerstedt-Wiberg et autres c. Suède, Req. n° 62332/00, §76.

18. Cour EDH, 6 septembre 1979, Klass et autres c. Allemagne, Req. n° 5029/71, §48-49.

19. V. SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act, FP7-SEC-2011-284725, publiée le 29 mai 2014.

RÉSUMÉS

Après l'effervescence et le débat qu'ont généré les révélations d'Edward Snowden relatives à la surveillance massive des télécommunications, le « soufflé » est quelque peu retombé. Or l'Assemblée Parlementaire du Conseil de l'Europe, en publiant un rapport édifiant et extrêmement critique ainsi qu'une série de recommandations adressées aux Etats membres, entend remettre au goût du jour l'encadrement et le contrôle des mesures de surveillance. La réflexion succédant à la réaction, le rapport rappelle la gravité de la situation et insiste sur la nécessité d'amender un cadre juridique manifestement inadapté, afin d'instaurer un encadrement strict et un véritable contrôle des mesures de surveillance.

AUTEUR

MARINE FARSHIAN

Avocate et membre d'une équipe de Défense près la Cour pénale internationale