SURVEILLANCE DE MASSE

Quel contrôle démocratique ?

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

SURVEILLANCE DE MASSE

Quel contrôle démocratique ?

Conseil de l'Europe

Édition anglaise :
Mass surveillance – Who is watching the watchers?
ISBN 978-92-871-8104-6

Couverture : SPDP, Conseil de l'Europe
Photo : iStock
Mise en pages : Jouve, Paris

Éditions du Conseil de l'Europe
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-8103-9

Imprimé dans les ateliers du Conseil de l'Europe

L'Assemblée parlementaire et la Commission européenne pour la démocratie par le droit (appelée Commission de Venise), deux instances du Conseil de l'Europe, œuvrent de concert pour mieux définir et défendre les valeurs fondamentales de l'Organisation : la protection des droits de l'homme, de l'État de droit et de la démocratie.

L'Assemblée parlementaire débat des grandes questions d'actualité en Europe, auxquelles la Commission de Venise apporte son expertise juridique.

Chaque ouvrage de la collection « Point de vue – Point de droit » expose, sur un thème d'actualité choisi, les positions des deux instances, offrant ainsi au lecteur une dimension politique et juridique unique.

Table des matières

Partie 1

Les opérations de surveillance massive

Rapport[1] de l'Assemblée parlementaire

Rapporteur: M. Pieter Omtzigt, Pays-Bas, PPE/DC[2]

I. RÉSUMÉ

La commission des questions juridiques et des droits de l'homme est profondément préoccupée par les pratiques de surveillance massive et d'intrusions à large échelle révélées depuis juin 2013 par M. Edward Snowden. Les informations divulguées ont fourni la preuve manifeste de l'existence de systèmes de grande envergure à la pointe des progrès technologiques, mis en place par les services de renseignement américains et leurs partenaires dans certains États membres du Conseil de l'Europe, en vue de collecter, de conserver et d'analyser à une gigantesque échelle les données des communications, y compris leur contenu, les données de géolocalisation et les autres métadonnées. Dans plusieurs pays, on assiste à l'évolution d'un gigantesque « complexe industriel de la surveillance », qui risque d'échapper au contrôle démocratique et à l'obligation de rendre des comptes, et menace le caractère libre et ouvert de nos sociétés.

Les opérations de surveillance révélées mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme – STE n° 5, « la Convention » ou CEDH), le droit à la liberté d'information et d'expression (article 10), ainsi que le droit à un procès équitable (article 6) et le droit à la liberté de religion (article 9). La commission est également profondément préoccupée par les menaces que font peser sur la sécurité d'internet les pratiques de certaines agences de renseignement qui recherchent systématiquement, utilisent et vont jusqu'à créer des « trappes » et autres failles dans les normes de sécurité et leur application, qui peuvent facilement être exploitées également par les terroristes et les cyberterroristes ou d'autres délinquants.

1. Doc. 13734 du 18 mars 2015 ; présentation et discussion du rapport le 21 avril 2015 lors de la deuxième partie de session 2015 de l'Assemblée parlementaire du Conseil de l'Europe (APCE) (12e séance).
2. Groupe du Parti populaire européen.

La commission reconnaît également la nécessité d'une coopération transatlantique dans la lutte contre le terrorisme et les autres formes de criminalité organisée. Mais elle estime que cette coopération doit reposer sur une confiance mutuelle, fondée sur le respect des droits de l'homme et de l'État de droit. Afin de rétablir la confiance, un cadre juridique et technique doit être mis en place aux échelons national et international pour garantir la protection des droits de l'homme, et surtout assurer l'exercice du droit au respect de la vie privée. À côté d'un contrôle judiciaire et parlementaire renforcé, l'extension de mesures de protection crédibles aux donneurs d'alerte qui dévoilent ces violations représente un moyen efficace de renforcer ce cadre juridique et technique.

II. TEXTES ADOPTÉS

A. Résolution 2045 (2015)[3]

1. L'Assemblée parlementaire est profondément préoccupée par les pratiques de surveillance massive révélées depuis juin 2013 par les journalistes auxquels un ancien fournisseur de l'Agence nationale de la sécurité (NSA) des États-Unis, M. Edward Snowden, avait transmis une grande quantité de données hautement secrètes qui démontrent l'existence d'opérations de surveillance massive et d'intrusions à large échelle jusqu'ici inconnues du grand public et même de la plupart des décideurs politiques.

2. Les informations divulguées à ce jour dans les fichiers Snowden ont déclenché un gigantesque débat planétaire sur les opérations de surveillance massive menées par les services de renseignement des États-Unis et d'autres pays, et sur l'éventuelle absence de dispositions légales et de protections techniques adéquates aux échelons national et international, et/ou de leur application effective.

3. Ces révélations ont fourni la preuve manifeste de l'existence de systèmes de grande envergure à la pointe des progrès technologiques, mis en place par les services de renseignement américains et leurs partenaires dans certains États membres du Conseil de l'Europe, en vue de collecter, de conserver et d'analyser à une gigantesque échelle les données des communications, y compris leur contenu, les données de géolocalisation et les autres métadonnées ainsi que des mesures de surveillance ciblées, qui englobent de nombreuses personnes pour lesquelles rien ne justifie de soupçonner qu'elles aient commis un acte répréhensible.

4. Les opérations de surveillance révélées jusqu'ici mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée (article 8 de la Convention européenne des droits de l'homme (STE n° 5)), le droit à la liberté d'information et d'expression (article 10), ainsi que le droit à un procès équitable (article 6) et le droit à la liberté de religion (article 9), surtout lorsque les communications confidentielles des avocats et des ministres du culte sont interceptées et les preuves numériques manipulées. Ces droits sont les pierres angulaires de la démocratie. Les atteintes qui leur sont portées sans qu'un contrôle juridictionnel acceptable soit exercé compromettent également l'État de droit.

3. Texte adopté par l'APCE le 21 avril 2015 (12e séance).

5. L'Assemblée est également profondément préoccupée par les menaces que font peser sur la sécurité d'internet les pratiques de certaines agences de renseignement, révélées par les fichiers Snowden : elles recherchent systématiquement, utilisent et vont jusqu'à créer des « trappes » et autres failles dans les normes de sécurité et leur application, qui peuvent facilement être exploitées également par les terroristes et les cyberterroristes ou d'autres délinquants.

6. Elle s'inquiète également de la collecte massive de données à caractère personnel par les entreprises privées et du risque que des acteurs étatiques ou non étatiques puissent accéder à ces données et les utiliser à des fins illégales. Dans ce contexte, rappelons que les entreprises privées doivent respecter les droits de l'homme en vertu de la Résolution 17/4 sur les droits de l'homme et les sociétés transnationales et autres entreprises, adoptée en juin 2011 par le Conseil des droits de l'homme des Nations Unies.

7. L'Assemblée condamne catégoriquement l'usage extensif fait de lois et de règlements secrets, appliqués par des tribunaux secrets sur la base d'interprétations secrètes des règles en vigueur, de telles pratiques sapant la confiance du public dans les mécanismes judiciaires de contrôle.

8. La présence, entre les mains de régimes autoritaires, d'outils de surveillance massive comparables à ceux qu'ont mis au point les services américains et alliés pourrait avoir des conséquences catastrophiques. En période de crise, il n'est pas impossible que le pouvoir exécutif tombe aux mains de responsables politiques extrémistes, même dans des démocraties bien établies. Un certain nombre de régimes autoritaires utilisent déjà des outils de surveillance de haute technologie, qui servent à traquer les opposants et à supprimer la liberté d'information et d'expression. À cet égard, l'Assemblée est profondément préoccupée par les récents changements législatifs intervenus en Fédération de Russie, qui ouvrent de nouvelles possibilités d'assurer une surveillance massive dans les réseaux sociaux et les services sur internet.

9. Dans plusieurs pays, on assiste à l'évolution d'un gigantesque « complexe industriel de la surveillance », favorisé par la culture du secret qui entoure les opérations de surveillance, leur haute technologie et le fait que les décideurs politiques et budgétaires ont du mal à évaluer, d'une part, la gravité des menaces alléguées et, d'autre part, les contre-mesures précises nécessaires et leurs coûts et avantages, sans faire appel à l'avis de groupes eux-mêmes intéressés. Ces structures puissantes risquent d'échapper au contrôle démocratique et à l'obligation de rendre des comptes. Elles menacent le caractère libre et ouvert de nos sociétés.

10. L'Assemblée observe que, dans la plupart des États, la législation protège dans une certaine mesure la vie privée de leurs propres citoyens, mais pas celle des ressortissants étrangers. Les fichiers Snowden montrent que la NSA des États-Unis et ses partenaires étrangers, notamment au sein de l'alliance Five Eyes (Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni), contournent les restrictions nationales en échangeant les données relatives aux ressortissants de leurs partenaires respectifs.

11. L'Assemblée reconnaît la nécessité d'une surveillance ciblée et efficace des personnes soupçonnées de mener des activités terroristes et d'autres groupes de criminels organisés. Cette surveillance ciblée peut être un outil efficace pour faire

respecter la loi et prévenir la criminalité. Parallèlement, elle observe que, d'après des études indépendantes réalisées aux États-Unis, les opérations de surveillance massive ne semblent pas avoir contribué à prévenir les attentats terroristes, contrairement à ce qu'affirmaient autrefois les hauts responsables des services de renseignement. Au contraire, des ressources qui pourraient servir à prévenir des attaques sont redirigées vers la surveillance massive, laissant des personnes potentiellement dangereuses libres d'agir.

12. L'Assemblée reconnaît également la nécessité d'une coopération transatlantique dans la lutte contre le terrorisme et d'autres formes de criminalité organisée. Elle estime que cette coopération doit reposer sur une confiance mutuelle, fondée sur des accords internationaux, le respect des droits de l'homme et de l'État de droit. Cette confiance a été gravement altérée par les opérations de surveillance massive révélées par les fichiers Snowden.

13. Afin de rétablir la confiance parmi les partenaires transatlantiques, parmi les États membres du Conseil de l'Europe et également entre les citoyens et leurs propres gouvernements, un cadre juridique doit être mis en place aux échelons national et international pour garantir la protection des droits de l'homme, et surtout pour assurer l'exercice du droit au respect de la vie privée. A côté d'un contrôle judiciaire et parlementaire renforcé, l'extension de mesures de protection crédibles aux donneurs d'alerte qui dévoilent ces violations représente un moyen efficace de renforcer ce cadre juridique et technique.

14. La réticence des autorités américaines compétentes et de leurs homologues européens à apporter leur concours à l'éclaircissement des faits, notamment leur refus d'assister aux auditions organisées par l'Assemblée et le Parlement européen, ainsi que le traitement sans ménagement réservé au donneur d'alerte Edward Snowden ne contribuent pas à rétablir la confiance mutuelle et la confiance des citoyens.

15. L'Assemblée se félicite des initiatives prises par le Congrès américain pour revoir la législation en vigueur afin de réduire au minimum les abus, ainsi que de la décision du Bundestag allemand de constituer une commission d'enquête sur les répercussions de l'affaire de la NSA en Allemagne. Elle appelle la commission du Bundestag à exercer son mandat, qui consiste à amener l'exécutif à répondre de ses actes et à rechercher la vérité sans tenir compte de considérations de politique partisane, et encourage les autres parlements à ouvrir des enquêtes similaires.

16. Rappelant les conclusions présentées dans le rapport sur le contrôle démocratique des services de sécurité adopté par la Commission européenne pour la démocratie par le droit (Commission de Venise) en 2015, l'Assemblée souligne que les parlements doivent jouer un rôle important dans le suivi, l'examen et le contrôle des services de sécurité nationaux et des forces armées nationales pour garantir le respect des droits de l'homme, de l'État de droit et de la responsabilité démocratique, ainsi que du droit international. La sous-traitance d'opérations de sécurité ou de renseignement à des sociétés privées doit être exceptionnelle et ne doit pas entraver le contrôle démocratique de ces opérations.

17. L'Assemblée se félicite de l'enquête approfondie menée par le Parlement européen, qui a conduit à l'adoption, le 12 mars 2014, d'une résolution très complète sur

l'affaire de la NSA et ses répercussions sur les relations transatlantiques. L'Assemblée souscrit pleinement, en particulier :

17.1. à l'invitation, adressée par le Parlement européen au Secrétaire Général du Conseil de l'Europe, à utiliser les pouvoirs que lui confère l'article 52 de la Convention européenne des droits de l'homme pour demander aux États parties d'expliquer de quelle manière ils mettent en œuvre les dispositions pertinentes de la Convention ;

17.2. à l'appel lancé par le Parlement européen pour promouvoir l'utilisation généralisée du cryptage et résister à toute tentative de fragilisation du cryptage et des autres normes de sécurité d'internet, non seulement pour protéger la vie privée, mais également pour écarter les menaces que font peser sur la sécurité nationale les États voyous, les terroristes, les cyberterroristes et les criminels de droit commun.

18. L'Assemblée invite l'Union européenne à accélérer ses travaux de mise au point du règlement général sur la protection des données et le système des dossiers passagers (PNR – Passenger Name Record), à conclure des accords de coopération internationale sur la base du système d'information de Schengen et à adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

19. L'Assemblée invite par conséquent instamment les États membres et observateurs du Conseil de l'Europe :

19.1. à veiller à ce que leur droit interne autorise la collecte et l'analyse des données à caractère personnel (métadonnées comprises) uniquement avec le consentement de l'intéressé ou à la suite d'une décision de justice rendue sur la base de motifs raisonnables de soupçonner la cible de prendre part à des activités criminelles ; il importe d'incriminer la collecte et le traitement illégaux des données de la même manière que la violation du secret de la correspondance classique ; la création de « trappes » ou toute autre technique visant à fragiliser ou à contourner les mesures de sécurité, ou à exploiter les failles existantes, devrait être rigoureusement interdite ; l'ensemble des institutions et entreprises qui détiennent des données à caractère personnel devraient être tenues d'appliquer les mesures de sécurité les plus efficaces disponibles ;

19.2. à veiller, pour faire respecter ce cadre juridique, à ce que leurs services de renseignement soient soumis à des mécanismes de contrôle judiciaire et/ou parlementaire appropriés. Les mécanismes de contrôle nationaux doivent disposer d'un accès suffisant aux informations et aux connaissances expertes, et permettre d'examiner toute coopération internationale sans être tenus de respecter le principe de la maîtrise de l'information par son auteur, de manière réciproque ;

19.3. à accorder une protection crédible et efficace aux donneurs d'alerte qui révèlent des activités de surveillance illégales, – y compris en accordant l'asile, dans la mesure où le droit national l'autorise, – et à ceux qui sont menacés de représailles dans leur pays d'origine, sous réserve que leurs révélations réunissent les conditions nécessaires à leur protection au titre des principes énoncés par l'Assemblée ;

19.4. à convenir d'un « code du renseignement » multilatéral, destiné à leurs services de renseignement, qui définisse les principes régissant la coopération aux fins de lutte contre le terrorisme et la criminalité organisée. Ce code devrait prévoir un

engagement mutuel à appliquer à la surveillance des ressortissants et résidents des pays partenaires les mêmes dispositions qui s'appliquent à leurs propres ressortissants et résidents, ainsi qu'à échanger les données obtenues par des mesures de surveillance légales uniquement dans le but pour lequel elles ont été collectées. Le recours aux mesures de surveillance à des fins politiques, économiques ou diplomatiques entre les États participants devrait être interdit. L'adhésion à ce code devrait être ouverte à tous les États qui mettent en œuvre à l'échelon national un cadre juridique correspondant aux dispositions énoncées aux paragraphes 19.1 à 19.3 ;

19.5. à promouvoir la mise au point de nouveaux systèmes de protection des données faciles à utiliser (automatiques), qui soient capables de parer à la surveillance massive et à toute autre menace pour la sécurité d'internet, y compris celle que représentent les acteurs non étatiques ;

19.6. à s'abstenir d'exporter vers les régimes autoritaires une technologie de pointe en matière de surveillance.

20. L'Assemblée invite également les organes compétents de l'Union européenne à utiliser tous les instruments dont ils disposent, comme la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), dans leurs relations avec leurs homologues des États-Unis pour promouvoir le respect de la vie privée de tous les Européens, notamment lorsqu'ils négocient ou mettent en œuvre le Partenariat transatlantique de commerce et d'investissement (TTIP), la décision sur la Sphère de sécurité, le Programme de surveillance du financement du terrorisme (TFTP) et l'accord sur les données des dossiers passagers (PNR).

B. Recommandation 2067 (2015) [4]

1. L'Assemblée renvoie à sa Résolution 2045 (2015) sur les opérations de surveillance massive et invite le Comité des Ministres à faire usage des instruments dont il dispose pour défendre le droit fondamental au respect de la vie privée dans l'ensemble des États membres et observateurs du Conseil de l'Europe.

2. L'Assemblée invite notamment le Comité des Ministres à envisager :

2.1. d'adresser une recommandation aux États membres en vue de garantir la protection de la vie privée à l'ère du numérique et la sécurité d'internet à la lumière des menaces que représentent les techniques de surveillance massive qui ont fait l'objet de récentes révélations (voir Résolution 2045 (2015), paragraphes 19.1 à 19.3);

2.2. de poursuivre l'étude des problèmes de sécurité sur internet que posent les pratiques de surveillance massive et d'intrusion, notamment sous l'angle des droits de l'homme et des libertés fondamentales des usagers de l'internet ;

2.3. de prendre une initiative visant à la négociation d'un code du renseignement destiné aux services de renseignement de tous les États participants, qui définisse les principes régissant la coopération aux fins de lutte contre le terrorisme et la criminalité organisée (voir Résolution 2045 (2015), paragraphe 19.4) ;

4. Texte adopté par l'APCE le 21 avril 2015 (12e séance).

2.4. de renforcer la coopération avec les organes compétents de l'Union européenne qui prennent part aux négociations sur les questions commerciales et la protection des données avec les États-Unis et d'autres pays tiers, afin que ces organes fassent pression pour que les principes énoncés dans la Convention européenne des droits de l'homme (STE n° 5) soient respectés, dans l'intérêt de tous les États membres du Conseil de l'Europe.

III. EXPOSÉ DES MOTIFS

Par M. Omtzigt, rapporteur

« Notre liberté repose sur ce que les autres ignorent de notre existence » (Alexandre Soljenitsyne)

1. Introduction et procédure

1. Depuis juin 2013, les révélations faites par les journalistes auxquels M. Edward Snowden, qui travaillait autrefois pour la CIA (Central Intelligence Agency) et pour une entreprise privée agissant pour le compte de l'Agence nationale de sécurité (NSA) des États-Unis, avait confié une grande quantité de données secrètes sur les opérations de surveillance massive menées par la NSA et d'autres organismes, ont provoqué un gigantesque débat public sur le respect de la vie privée à l'ère d'internet. L'étendue des programmes de surveillance massive de la NSA et des services de renseignement d'autres pays appliqués dans le monde entier est stupéfiante. Les révélations faites confirment que le Conseil de l'Europe doit encourager ses États membres et observateurs à réévaluer leurs propres programmes de surveillance, à apprécier les failles qui permettent à ces programmes de faire de leurs propres citoyens la cible de services de renseignement étrangers, ainsi qu'à réfléchir aux remèdes possibles, notamment par des moyens législatifs, des accords internationaux et la promotion du cryptage massif. Il est ici question non seulement de la protection de nos droits fondamentaux, mais également de la sécurité nationale, qui se trouve menacée par des États voyous, des terroristes, des cyberterroristes et des criminels de droit commun qui peuvent faire d'énormes dégâts en profitant des faiblesses du cryptage et des autres mesures de sécurité sur internet délibérément créées par les services de renseignement pour faciliter les opérations de surveillance massive.

2. La manière dont M. Snowden a rendu ces divulgations possibles a également relancé le débat sur la protection des donneurs d'alerte. Ces deux débats ont donné lieu à des propositions de résolution au sein de l'Assemblée parlementaire.

3. Le 6 novembre 2013, la commission des questions juridiques et des droits de l'homme m'a nommé rapporteur pour deux sujets intimement liés : « Les opérations de surveillance massive »[5] et le « Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte qui révèlent des agissements des pouvoirs publics constituant une violation du droit international et des droits fondamentaux»[6]. À l'issue d'un premier tour de table le 6 novembre

5. Proposition de résolution, Doc. 13288.
6. Proposition de résolution, Doc. 13278.

2013, la commission a décidé, au cours de sa réunion du 27 janvier 2014, sur la base de ma note introductive[7], de remplacer le titre en anglais du futur rapport, « Massive Eavesdropping », par « Mass Surveillance », et d'organiser une audition avec la participation de M. Snowden lors de la partie de session de printemps de l'Assemblée, le 8 avril 2014.

4. Il n'a malheureusement pas été possible d'obtenir toutes les assurances qui auraient permis à M. Snowden de venir en toute sécurité à Strasbourg et de se rendre librement dans un pays de son choix après l'audition. La commission a en conséquence dû se contenter d'auditionner M. Snowden par liaison vidéo en direct depuis son asile provisoire de Moscou, tandis que son avocat allemand, M. Wolfgang Kaleck, a suivi ces échanges au moyen d'une ligne téléphonique fixe qui lui permettait, le cas échéant, de dispenser des conseils à son client.

5. J'aimerais remercier M. Snowden d'avoir bien voulu s'adresser à la commission et répondre en direct aux questions qui lui étaient posées, malgré les risques judiciaires qu'il encourait. 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.

6. J'aimerais également remercier les deux autres experts qui ont participé à l'audition du 8 avril 2014, à savoir M. Hansjörg Geiger, ancien directeur du Bundesnachrichtendienst (BND), le service allemand de renseignement extérieur, et M. Douwe Korff, professeur de droit international, à la London Metropolitan University[8].

7. J'ai déjà convenu du fait qu'il ne s'agira pas d'un rapport consacré à M. Snowden, mais aux pratiques qu'il a contribué à révéler. Mais nous ne pouvons fermer les yeux sur le fait que l'acte courageux de M. Snowden a déclenché un débat public sur la protection de la vie privée. Son cas offre également un exemple particulièrement intéressant de juste équilibre entre des intérêts contradictoires, sur lequel reposent les principes de la protection des donneurs d'alerte que j'ai été chargé d'examiner dans un deuxième rapport distinct.

2. Nature et étendue des opérations de surveillance massive

8. Les révélations de M. Snowden ont fait apparaître tout un éventail stupéfiant de programmes de surveillance massive mis en place par la NSA, mais également par les services de renseignement d'autres pays. Ces programmes secrets menacent directement la protection des droits de l'homme et la coopération internationale.

2.1. Les programmes de surveillance massive de la NSA : aucun moyen de communication n'est épargné

9. Toutes les formes de communication sont interceptées grâce à une multitude d'instruments et de programmes mis au point par la NSA et les autres services de

7. Document AS/Jur(2014)2 du 23 janvier 2014.
8. L'enregistrement de l'audition est disponible sur le site web de l'APCE. Le procès-verbal de la réunion du 8 avril 2014 en présente un résumé.

renseignement du monde entier. La surveillance ciblée a systématiquement été utilisée pour légitimer les mesures répressives et pour protéger les États contre les menaces qui pèsent sur leur sécurité nationale. Mais les révélations sur la NSA ont fait naître de sérieuses préoccupations à propos de la collecte et de l'analyse indistinctes de données provenant de citoyens qui ne sont pas soupçonnés d'avoir des liens avec le terrorisme ou avec d'autres formes de criminalité. Les éléments qui suivent sont désormais connus ; ils concernent les différentes méthodes utilisées par les services de renseignement pour intercepter, conserver et analyser les données.

2.1.1. Accès aux données des sociétés internet : accès officiel et accès clandestin

10. Les fichiers de la NSA révèlent que l'agence a eu accès aux données clients des sociétés internet avec ou sans leur consentement et que la Special Source Operations (SSO), une division interne de l'agence chargée des programmes de collecte par l'intermédiaire d'entreprises privées, a été qualifiée dans les documents divulgués de « joyau de la couronne » de la NSA. Grâce à son programme PRISM, considéré comme le plus important contributeur aux activités de collecte du renseignement de la NSA, cette dernière dispose d'un accès officiel aux données de neuf sociétés internet, dont Google, Microsoft et Yahoo. La NSA accède ainsi aux données clients détenues par les sociétés avec l'autorisation d'un juge (obtenue dans une procédure secrète) et a pu de la sorte recueillir les courriers électroniques, les historiques des conversations, les données conservées, les communications téléphoniques, les transferts de dossier ou les données des réseaux sociaux provenant de ces sociétés. Les entreprises en question ont tout d'abord nié avoir connaissance de ce programme, puis ont finalement insisté sur le fait qu'elles étaient tenues par la législation de coopérer avec les services de renseignement[9]. Les révélations ultérieures ont également montré que la NSA et son homologue britannique, le GCHQ (Government Communications Headquarters – Direction gouvernementale des communications), avaient également bénéficié d'un accès « clandestin » : ces agences étaient en mesure d'intercepter les données provenant de ces sociétés, sans qu'elles en soient informées, grâce à un programme secret affublé du nom de code « Muscular », en plus des données qu'elles recueillaient au vu et au su des entreprises concernées[10].

2.1.2. Surveillance du réseau câblé de fibres optiques

11. Selon certaines sources, le Royaume-Uni procéderait à la surveillance du réseau câblé de fibres optiques par lequel transitent les communications planétaires et partagerait ces données avec la NSA. Comme une bonne part du flux des communications mondiales passe par les États-Unis ou le Royaume-Uni, les services de renseignement des deux États disposent, sur leur territoire même, d'un avantage sur le terrain qui leur permet d'intercepter le flux de communications qui arrive dans leur pays ou passe par celui-ci. Bien que le système « virtuel » de communications électroniques

9. « Revealed: how US and UK spy agencies defeat internet privacy and security », *The Guardian*, 6 septembre 2013.

10. « NSA [National Security Agency] infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say », *The Washington Post*, 30 octobre 2013.

offert par internet soit, par sa nature même, transnational, voire planétaire, son infrastructure (qui se compose de toutes sortes de commutateurs, routeurs, serveurs et réseaux câblés) a une réalité matérielle et se situe dans des lieux bien réels. À l'heure actuelle, bon nombre de ces lieux se trouvent aux États-Unis et au Royaume-Uni[11]. Le GCHQ a ainsi pu avoir accès à au moins 200 réseaux câblés de fibres optiques, ce qui lui permet de surveiller jusqu'à 600 millions de communications par jour. Les informations relatives à internet et aux communications téléphoniques seraient conservées pendant une période pouvant aller jusqu'à 30 jours, afin de permettre leur passage au crible et leur analyse[12].

2.1.3. Collecte et analyse des métadonnées : mieux tirer parti d'une quantité « inférieure » de données

12. Les « métadonnées » sont des informations relatives à l'heure et au lieu d'un appel téléphonique ou d'un courrier électronique, par opposition au contenu proprement dit de ces conversations ou messages. Le premier document Snowden publié par le *Guardian* était une ordonnance judiciaire secrète, qui révélait que la NSA recueillait les enregistrements téléphoniques de millions de clients américains de Verizon, l'un des principaux fournisseurs américains de télécommunications. Les partisans de la collecte sans entrave des métadonnées[13] ne considèrent pas cette activité comme de la surveillance. D'autres sont en total désaccord avec cette pratique et avec l'emploi même du terme « métadonnées » (dont le sens est simplement celui de données décrivant d'autres données), auquel ils préfèrent celui de « sommaires » ou de « résumés analytiques ». De fait, la Cour de justice de l'Union européenne (CJUE) a fait remarquer que les métadonnées des communications « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées »[14]. Le Haut-Commissariat des Nations Unies aux droits de l'homme a adopté la même position dans son rapport de juin 2014 sur le caractère privé des données – à savoir le fait que la distinction entre les métadonnées et les données n'était pas convaincante – et a ainsi conclu que « tout captage de données sur les communications constitue potentiellement une immixtion dans la vie privée et qu'en outre la collecte et la conservation de ces données constituent également une telle ingérence, que les données soient ou non consultées ou utilisées par la suite »[15]. Ce point de vue me semble convaincant, d'autant plus si l'on considère que l'ancien chef de la NSA

11. « La prééminence du droit sur l'internet et dans le monde numérique en général », document thématique établi par le professeur Douwe Korff (l'un des experts invités à l'audition organisée par la commission des questions juridiques et des droits de l'homme de l'APCE en avril) et publié par le Commissaire aux droits de l'homme du Conseil de l'Europe en décembre 2014 (p. 8) (ci-après « La prééminence du droit sur l'internet »).
12. « GCHQ taps fibre-optic cables for secret access to world's communications », *The Guardian*, 21 juin 2013.
13. Par exemple la sénatrice américaine Dianne Feinstein, présidente de la commission du renseignement du Sénat (citée par *USA Today*).
14. Cour de justice de l'Union européenne (CJUE), arrêt rendu dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger et autres*, arrêt du 8 avril 2014, paragraphes 26-27 et 37.
15. 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 ».

et de la CIA, le général Michael Hayden, a admis, sans manifester aucun repentir : « nous tuons des gens en nous fondant sur des métadonnées »[16].

13. Comme les « métadonnées » permettent aux agences d'obtenir une représentation bien plus concise de l'immense quantité de communications qu'elles interceptent et comportent cependant des informations à caractère personnel, qui peuvent servir à la réalisation d'un « profil » plus détaillé encore d'une personne que l'écoute du contenu de ces communications, la NSA a eu abondamment recours à la collecte des métadonnées. En mars 2013, la NSA aurait recueilli jusqu'à 97 milliards d'informations ou de métadonnées dans les réseaux informatiques du monde entier. Plus de 14 milliards provenaient d'Iran, 13,5 milliards du Pakistan et 12,7 milliards de Jordanie, les États européens n'étant pas épargnés. Selon un document de présentation de « Boundless Informant », un outil utilisé par la NSA pour analyser les métadonnées qu'elle détient et pour connaître les informations actuellement disponibles sur un pays donné, il est possible que l'agence ait aussi collecté des métadonnées auprès des alliés européens des États-Unis. Ce document précise la quantité de métadonnées associée à un pays : plus de 70,3 millions d'unités proviennent de France, 471 millions d'Allemagne, 45,9 millions d'Italie et 60,5 millions d'Espagne, notamment. Les gouvernements norvégien et allemand affirment que les chiffres indiqués pour la collecte des métadonnées pour leurs pays dans ce document de présentation concernent les métadonnées réunies par eux-mêmes en Afghanistan et partagées avec la NSA. Mais un journaliste, M. Glenn Greenwald, a contesté cette explication, en se fondant sur les questions les plus fréquemment posées présentées par la NSA elle-même à propos de « Boundless Informant » : l'agence explique que cet « outil permet aux utilisateurs de choisir un pays sur une carte, de visionner la quantité de métadonnées et d'obtenir des précisions sur les données collectées au détriment du pays » et non communiquées par celui-ci[17].

2.1.4. Écoute des téléphones, collecte des textos, surveillance des fax

14. Nous avons appris en janvier 2014 que la NSA conservait les données de centaines de millions de téléphones portables partout dans le monde. Elle a notamment conservé environ 5 milliards de séries de données de géolocalisation par jour, auxquelles elle peut accéder même lorsque la fonction GPS *(global positioning system)* d'un smartphone est éteinte, simplement en suivant le mouvement d'un téléphone d'une antenne de téléphonie mobile (émetteur local) à une autre[18]. La NSA collecte ces données de géolocalisation et celles relatives aux habitudes de déplacement pour « exploiter une cible », c'est-à-dire découvrir les associés inconnus des « cibles » qu'elle connaît déjà.

15. De plus amples précisions sur les nombreux autres programmes utilisés par la NSA et son homologue britannique pour intercepter les textos envoyés par

16. L'enregistrement vidéo d'une conférence donnée à l'université Johns-Hopkins le 1er avril 2014.
17. « Boundless Informant : NSA explainer – full document text », *The Guardian*, 8 juin 2013.
18. « NSA tracking cellphone locations worldwide Snowden documents show », *The Washington Post*, 4 décembre 2013.

téléphone portable, les appels téléphoniques et les fax sont désormais disponibles. Les documents du GCHQ ont révélé, comme cela a été confirmé par la suite par la NSA, qu'un système baptisé du nom de code « Dishfire » permettait de traiter et de conserver les données des SMS *(short message service)*, en collectant « à peu près tout ce qui peut l'être », au lieu de se contenter de stocker les communications des cibles existantes de la surveillance. Une présentation de la NSA de 2011 indique que le programme avait collecté en moyenne 194 millions de textos par jour au cours du mois d'avril de cette année et que leur contenu avait été partagé avec le GCHQ. La NSA a utilisé sa vaste base de données de textos pour extraire des informations sur les itinéraires des déplacements, les listes de contacts, les transactions financières et d'autres éléments encore des personnes visées, parmi lesquelles figuraient des individus qui n'étaient soupçonnés d'aucune activité illicite.

16. La NSA a également mis au point le programme d'interception des communications vocales « Mystic » pour recueillir les appels téléphoniques passés dans un pays par une population combinée de plus de 250 millions de personnes. Il a été indiqué par la suite que les États-Unis avaient pu mener une opération de ce type sous le nom de code de « Somalget » aux Bahamas et enregistrer l'intégralité des appels téléphoniques du pays sans que son gouvernement n'en soit informé ou y consente, en traitant environ 100 millions d'appels par jour concernant les Bahamas et un deuxième pays non révélé. La NSA a recueilli cette immense quantité de données à laquelle a eu accès l'Administration américaine de lutte contre le trafic de drogue (Drug Enforcement Administration – DEA), qui peut demander la mise sur écoute judiciaire des réseaux téléphoniques étrangers dans le cadre de la coopération internationale des services répressifs. Avec 80 bureaux disséminés à travers le monde, la DEA est le service administratif américain le plus largement déployé sur la planète. Mais les États étrangers ne sont pas conscients du fait que son mandat comprend, au-delà de la lutte contre le trafic de drogue, la collecte d'informations à des fins de renseignement. Au cours de son audition par la commission, Edward Snowden a donné des précisions sur la technique de la « construction parallèle », qui consiste à utiliser illégalement, à des fins répressives, les informations secrètes des activités de renseignement, dont les tribunaux saisis des affaires en question ne sont pas informés. Cette méthode prive l'accusé de son droit de contester la légalité de la surveillance initiale[19]. M. Snowden a observé que, dans ces affaires, les informations initialement recueillies par les activités de renseignement étaient bien souvent collectées sans mandat judiciaire, contrairement à ce qu'exige le cadre répressif habituel. Cette utilisation illégale d'éléments de preuve secrets, dont l'existence ou la source est dissimulée à la fois au prévenu et au juge, menace gravement le droit à un procès équitable et le droit à être confronté à ses accusateurs. En outre, de nombreux pays, dont les Bahamas, ont recours à des entreprises privées pour installer et faire fonctionner le matériel d'interception sur leurs infrastructures de télécommunications, afin de faciliter les écoutes. Un technicien supérieur de l'American Civil Liberties Union a fait observer que ces systèmes fragilisaient toujours les réseaux de communication[20].

19. Voir le témoignage d'Edward Snowden devant l'Assemblée parlementaire du Conseil de l'Europe du 8 avril 2014 (en anglais).

20. « Data Pirates of the Caribbean : the NSA Is Recording Every Cell Phone Call in the Bahamas », *The Intercept*, 19 mai 2014.

17. La NSA n'est pas seulement capable d'intercepter les appels téléphoniques d'un pays tout entier, elle peut également remonter le temps et écouter des appels téléphoniques enregistrés au cours des mois précédents, ce qui lui permet de procéder à une « récupération rétrospective » des données, c'est-à-dire de déterminer le contenu des communications de ses cibles à l'occasion d'appels passés avant même qu'elles ne soient identifiées comme cibles[21]. Contrairement aux affirmations antérieures de la NSA, qui prétendait intercepter uniquement les métadonnées relatives aux appels, le programme « Retro » de la NSA permet aux analystes de revenir aux conversations téléphoniques qui ont eu lieu un mois plus tôt et de les récupérer[22]. Les analystes sont censés n'écouter qu'une fraction de ces appels (environ 1 %), mais leur volume reste élevé en nombre absolu. La directive présidentielle *(Presidential Decision Directive)* (PDD) n° 28, prise par le Président Obama, précise à la NSA et aux autres agences que le recours à la collecte en vrac de données est uniquement possible pour recueillir des informations relatives à une des six menaces particulières, parmi lesquelles figurent la prolifération nucléaire et le terrorisme ; mais elle fait remarquer que les limites applicables à la collecte de masse ne valent pas pour les informations des activités de renseignement « recueillies provisoirement pour faciliter une collecte ciblée ». La Maison Blanche a chargé un groupe indépendant de faire le bilan des politiques américaines de surveillance, mais le Président Obama a refusé de suivre les recommandations formulées par ce groupe, qui préconisaient de purger les données conservées des appels et des courriers électroniques de ressortissants américains dès lors que les agences en avaient connaissance. Les agents américains interviewés par le *Washington Post* ont au contraire reconnu qu'un grand nombre de conversations de ressortissants américains étaient interceptées dans des pays où le programme « Retro » était appliqué et que la NSA ne cherchait pas à filtrer ces appels en vue de leur suppression puisque ces communications étaient récupérées de manière fortuite à l'occasion de la collecte de données visant les cibles pertinentes des services de renseignement extérieur.

18. Grâce au programme « Prefer », la NSA peut extraire chaque jour en moyenne plus de 5 millions d'alertes d'appels manqués utilisées pour l'analyse des contacts en chaîne (c'est-à-dire pour établir le réseau social d'une personne à partir des individus qu'elle contacte et des dates de ces contacts), des précisions sur 1,6 million de franchissements quotidiens de frontières, plus de 110 000 noms tirés des cartes de visite électroniques (elle est également capable d'extraire et de conserver des images), plus de 800 000 opérations financières (sous forme de paiement par SMS ou avec une carte de crédit reliée à un utilisateur de téléphone), ainsi que les données de géolocalisation de plus de 76 000 SMS par jour. Les documents pertinents laissent penser que les communications des numéros de téléphone américains ont été supprimées des bases de données, mais que celles des autres pays ont été conservées.

2.1.5. Collecte de millions de visages tirés des images diffusées sur internet

19. Outre les communications écrites et orales, la NSA a collecté chaque jour des millions de visages à partir d'images trouvées sur internet, en vue de tirer parti de

21. « NSA surveillance program reaches "into the past" to retrieve, replay phone calls », *The Washington Post*, 18 mars 2014.

22. « Rewind and Play : NSA storing "100 percent" of a nation's calls », *Russia Today*, 19 mars 2014.

l'immense potentiel inexploité de l'utilisation des images faciales, des empreintes digitales et des autres éléments d'identification destinés à rechercher des personnes soupçonnées d'activités terroristes et d'autres cibles des services de renseignement[23]. L'une de ses plus importantes initiatives est celle du programme « Wellspring », qui extrait les images des courriers électroniques et d'autres communications, ainsi que celles qui sont susceptibles de contenir des images de passeports. Parallèlement aux programmes mis au point par ses soins, la NSA recourt également en partie à la technologie de reconnaissance faciale commercialisée ; le secteur public et le secteur privé ont investi des milliards de dollars dans la recherche et le développement de la reconnaissance faciale. Selon le *New York Times*, on ignore le nombre d'images récupérées par la NSA, qui a déclaré ne pas avoir accès aux photos des permis de conduire et passeports américains, mais qui n'a pas voulu confirmer si elle avait accès à la base de données du Département d'État qui regroupe les photos des auteurs d'une demande de visa étranger ou si elle collectait les images faciales des ressortissants américains sur Facebook ou d'autres réseaux sociaux, ou en utilisant d'autres moyens. Le Congrès américain a largement négligé cette question ; le sénateur El Franken a déclaré à ce propos que « la législation [américaine] relative au respect de la vie privée ne prévoit pas expressément la protection des données de reconnaissance faciale»[24].

2.2. Utilisation de Five Eyes et d'autres partenariats : collaboration entre la NSA et les services de renseignement d'autres pays du monde

20. Les révélations de M. Snowden comportent des précisions sur la collaboration établie dans le cadre de l'alliance « Five Eyes », ainsi que sur les partenariats étendus entre la NSA et d'autres États, parmi lesquels figurent des États membres du Conseil de l'Europe.

2.2.1. Five Eyes : États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada

21. L'alliance de mise en commun des activités de renseignement « Five Eyes » repose sur l'accord de renseignement sur les transmissions passé entre le Royaume-Uni et les États-Unis en 1946 (traité Ukusa), qui a été par la suite étendu à l'Australie, à la Nouvelle-Zélande et au Canada. Ses cinq membres partagent par exemple le réseau de mise en commun planétaire des services de renseignement « Echelon », géré pour le compte de l'alliance Five Eyes, qui vise à intercepter les communications privées et commerciales (plutôt que militaires). Ce système serait capable d'intercepter tout « message envoyé par une personne au moyen d'un téléphone, d'un fax, d'internet ou d'un courrier électronique ».

22. Les fichiers de M. Snowden ont également révélé les activités de surveillance individuelle et collective du Royaume-Uni. Outre la mise en commun avec son

23. J. Risen, L. Poitras, « NSA Collecting Millions of Faces From Web Images », *The New York Times*, 31 mai 2014.

24. *Ibid*.