Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13734
18 mars 2015

Les opérations de surveillance massive

Rapport[1]
Commission des questions juridiques et des droits de l'homme
Rapporteur: M. Pieter OMTZIGT, Pays-Bas, Groupe du Parti populaire européen

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 Etats 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), 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.

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'Etat 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. 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.

1. Renvoi en commission: Doc. 13288, Renvoi 4003 du 30 septembre 2013.

Sommaire **Page**

A. Projet de résolution[2]

1. L'Assemblée parlementaire est profondément préoccupée par les pratiques de surveillance massive révélées depuis juin 2013 par les journalistes auxquels un ancien membre de la sécurité nationale des Etats-Unis, M. Edward Snowden, avait confié une grande quantité de données hautement secrètes qui démontrent l'existence de pratiques 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 Etats-Unis et les services de renseignement d'autres pays et sur l'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 Etats 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 que rien ne justifie de soupçonner d'avoir 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 ne soit exercé compromettent également l'Etat de droit.

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.

7. L'Assemblée est aussi profondément préoccupée de l'usage extensif fait de lois et de tribunaux secrets ainsi que des interprétations secrètes données à de telles lois, qui ne sont pas contrôlées de manière adéquate.

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 aurait 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.

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 leur 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 Etats, la législation protège dans une certaine mesure la vie privée des ressortissants nationaux, mais pas des ressortissants étrangers. Les fichiers Snowden montrent que l'Agence nationale de sécurité (NSA) des Etats-Unis et ses partenaires étrangers, notamment au sein de l'alliance «Five Eyes» (Australie, Canada, Etats-Unis, Nouvelle-Zélande et Royaume-Uni), contournent les restrictions nationales en échangeant les données relatives aux ressortissants de leurs partenaires respectifs.

---

2. Projet de résolution adopté à l'unanimité par la commission le 26 janvier 2015.

11. L'Assemblée reconnaît la nécessité d'une surveillance ciblée et efficace des personnes soupçonnées de mener des activités terroristes ou 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 Etats-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. Mais elle estime que cette coopération doit reposer sur une confiance mutuelle, fondée sur le respect des droits de l'homme et de l'Etat de droit. Cette confiance a été gravement altérée par les pratiques de surveillance massive révélées par les fichiers Snowden.

13. Afin de rétablir la confiance parmi les partenaires transatlantiques, parmi les Etats membres du Conseil de l'Europe et 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 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, et 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 contribue 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 limiter le plus possible 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. 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 euro-atlantiques. L'Assemblée souscrit pleinement, en particulier:

16.1. 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 Etats Parties d'expliquer de quelle manière ils mettent en œuvre les dispositions pertinentes de la Convention;

16.2. 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 Etats voyous, les terroristes, les cyberterroristes et les criminels de droit commun.

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

17.1. à veiller à ce que le 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 tenus d'appliquer les mesures de sécurité les plus efficaces disponibles;

17.2. 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, ainsi qu'avoir le pouvoir d'examiner toute coopération internationale sans être tenus de respecter le principe de la maîtrise de l'information par son auteur, de manière réciproque;

17.3. à accorder une protection crédible et efficace aux donneurs d'alerte qui révèlent des activités de surveillance illégales, y compris en leur donnant asile lorsqu'ils sont menacés de poursuites injustes dans leur pays d'origine;

17.4. à convenir d'un «code du renseignement» multilatéral, destiné à leurs services de renseignement, qui définisse les principes qui régissent 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 de leurs ressortissants et résidents réciproques 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 Etats participants devrait être interdit. L'adhésion à ce code devrait être ouverte à tous les Etats qui mettent en œuvre à l'échelon national un cadre juridique correspondant aux dispositions énoncées aux paragraphes 16.1 à 16.3;

17.5. 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;

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

18. L'Assemblée invite également les organes compétents de l'Union européenne à utiliser tous les instruments dont ils disposent pour promouvoir le respect de la vie privée de tous les Européens dans leurs relations avec leurs homologues des Etats-Unis, 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. Projet de recommandation[3]

1. L'Assemblée renvoie à sa Résolution … (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 Etats 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 Etats 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 … (2015), paragraphes 16.1 à 16.3);

2.2. de prendre une initiative visant à la négociation d'un «Code du renseignement», destiné aux services de renseignement de tous les Etats participants, qui définisse les principes qui régissent la coopération aux fins de lutte contre le terrorisme et la criminalité organisée (voir Résolution … (2015), paragraphe 16.4);

2.3. 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 Etats-Unis et d'autres pays tiers, afin qu'ils fassent pression pour que les principes énoncés par la Convention européenne des droits de l'homme soient respectés, dans l'intérêt de tous les Etats membres du Conseil de l'Europe.

3. Projet de recommandation adopté à l'unanimité par la commission le 26 janvier 2015.

C. 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 et pour une entreprise privée agissant pour le compte de l'Agence nationale de sécurité (NSA) des Etats-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 Etats 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 Etats 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»[4] et le «Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte»[5]. A l'issue d'un premier tour de table le 6 novembre 2013, la commission a décidé au cours de sa réunion du 27 janvier 2014, sur la base de ma note introductive[6], 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) allemand, et M. Douwe Korff, professeur de droit international, London Metropolitan University[7].

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.

---

4. Proposition de résolution, Doc. 13288.
5. Proposition de résolution, Doc. 13278.
6. Document AS/Jur (2014) 2 du 23 janvier 2014.
7. L'enregistrement de l'audition est disponible sur le site web de l'Assemblée parlementaire. Le procès-verbal de la réunion du 8 avril 2014 en présente un résumé.

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 renseignement du monde entier. La surveillance ciblée à systématiquement été utilisée pour légitimer les mesures répressives et pour protéger les Etats 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. L'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, qui est 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[8]. 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[9].

2.1.2. La 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 Etats-Unis ou le Royaume-Uni, les services de renseignement des deux Etats 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 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. A l'heure actuelle, bon nombre de ces lieux se trouvent aux Etats-Unis et au Royaume-Uni[10]. 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[11].

---

8. *The Guardian*, 6 septembre 2013, «Revealed: how US and UK spy agencies defeat internet privacy and security».
9. *The Washington Post*, 30 octobre 2013, «NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say».
10. «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 notre commission 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»).

2.1.3. La collecte et l'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 *The 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 télécoms. Les partisans de la collecte sans entrave des métadonnées[12] 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 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»[13]. Le Haut-Commissariat aux droits de l'homme des Nations Unies 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»[14]. Ce point de vue me semble convaincant, d'autant plus si l'on considère que l'ancien chef de la NSA et de la CIA, le général Michael Hayden, a admis sans manifester aucun repentir «nous tuons des gens en nous fondant sur des métadonnées»[15].

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 Etats 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 Etats-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[16].

2.1.4. Ecoute des téléphones, collecte des textos, surveillance des faxes

14. Nous avons appris en janvier 2014 que la NSA conserve 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 d'un smartphone est éteinte, simplement en suivant le mouvement d'un téléphone d'une antenne de téléphonie mobile (émetteur local) à une autre[17]. La NSA collecte ces données de géolocalisation et relatives aux habitudes de déplacement pour «exploiter une cible», c'est-à-dire découvrir les associés inconnus des «cibles» qu'elle connaît déjà.

---

11. *The Guardian*, 21 juin 2013, «GCHQ taps fibre-optic cables for secret access to world's communications».
12. Par exemple la sénatrice américaine Dianne Feinstein, présidente de la commission du renseignement du Sénat (citée par USA Today).
13. Cour de justice de l'Union européenne, 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.
14. 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».
15. L'enregistrement vidéo d'une conférence donnée à l'Université Johns Hopkins le 1er avril 2014.
16. *The Guardian*, 8 juin 2013, «Boundless Informant: NSA explainer – full document text».

15. De plus amples précisions sur les nombreux autres programmes utilisés par la NSA et son homologue britannique pour intercepter les textos envoyés par téléphone portable, les appels téléphoniques et les faxes 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, 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 Etats-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 Etats 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[18]. 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[19].

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[20]. 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[21]. Les analystes sont censés n'écouter qu'une fraction de ces appels (environ 1 %), mais leur volume reste élevé en nombre absolu. L'instruction présidentielle générale 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 de 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

---

17. *The Washington Post*, 4 décembre 2013, «NSA tracking cellphone locations worldwide Snowden documents show».
18. Voir le témoignage d'Edward Snowden devant l'Assemblée parlementaire du Conseil de l'Europe du 8 avril 2014 (en anglais).
19. *The Intercept*, 19 mai 2014, «Data Pirates of the Caribbean: the NSA Is Recording Every Phone Call in the Bahamas».
20. *The Washington Post*, 18 mars 2014, «NSA surveillance program reaches 'into the past' to retrieve, replay phone calls».
21. *Russia Today*, 19 mars 2014, «Rewind and Play: NSA storing "100 percent" of a nation's calls».

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 millions 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. La 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 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[22]. 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 n'a pas voulu confirmer si elle avait accès à la base de données du Département d'Etat 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»[23].

2.2. L'utilisation de Five Eyes et d'autres partenariats: la collaboration entre le NSA et les services de renseignements 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 Etats, parmi lesquels figurent des Etats membres du Conseil de l'Europe.

2.2.1. Five Eyes: Etats-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 Etats-Unis en 1946, 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 homologue américain des données recueillies à l'aide du programme «TEMPORA», mis en place en 2011 pour intercepter une très grande quantité de communications internet et téléphoniques en accédant au réseau câblé de fibres optiques, le GCHQ a également eu partiellement accès au programme «PRISM» de la NSA depuis juin 2010 et pendant les Jeux

22. James Risen et Laura Poitras, «NSA Collecting Millions of Faces From Web Images», *The New York Times*, 31 mai 2014.
23. *Ibid*.

olympiques et a demandé à bénéficier d'un accès supplémentaire non surveillé aux données collectées par la NSA. Depuis avril 2013, le GCHQ est parvenu, à force de sollicitations, à obtenir un accès accru au trésor de données «supervisé» par la NSA.

23. Selon le *Guardian*, le programme «OPTIC NERVE» permettrait de collecter en vrac les images fixes de la messagerie instantanée (chat) avec webcam de Yahoo et de les conserver dans les bases de données de l'agence, que les particuliers concernés soient considérés comme une cible des services de renseignement ou non. D'importantes quantités de communications à contenu sexuel explicite ont ainsi été intégrées et, en 2008, en l'espace d'à peine six mois, l'agence a collecté des images webcam tirées de plus d'1,8 millions de comptes utilisateurs Yahoo dans le monde. Le programme conserve une image extraite toutes les cinq minutes des lecteurs de flux des utilisateurs, en partie pour se conformer à la législation relative aux droits de l'homme et pour éviter une surcharge des serveurs du GCHQ. D'après les explications données par le *Guardian*, l'agence s'est efforcée de restreindre la capacité des analystes à voir les images webcam, en limitant les recherches en vrac aux seules métadonnées. Yahoo nie avoir eu une connaissance préalable de ce programme.

24. Le Joint Threat Research Intelligence Group (JTRIG – Groupe conjoint des services de renseignement pour l'étude des menaces), une unité autrefois secrète du GCHQ, a effectué des missions de cyberattaque contre des personnes qui n'avaient aucun lien avec le terrorisme et ne présentaient aucune menace pour la sécurité nationale. Le JTRIG a ainsi eu recours à la tactique du déni de service distribué (DDoS) pour bloquer les forums de discussion sur internet utilisés par les membres du groupe de cybermilitants «Anonymous», affectant aussi d'autres utilisateurs des mêmes serveurs ou réseaux (une sorte de dégâts collatéraux).

25. Entre-temps, au Canada, le Centre de la sécurité des télécommunications Canada (CSTC) a utilisé les informations obtenues grâce à l'accès internet gratuit d'un grand aéroport canadien pour observer les dispositifs sans fil de milliers de passagers aériens ordinaires plusieurs jours après qu'ils avaient déjà quitté le terminal. La législation canadienne interdit de cibler des ressortissants canadiens ou toute personne se trouvant au Canada sans mandat judiciaire et cette agence est censée collecter du renseignement extérieur en interceptant les communications téléphoniques et internet à l'étranger. Mais le CSTC rétorque dans une déclaration écrite que «la législation l'autorise à collecter et à analyser les métadonnées» qui, semble-t-il, permettent d'identifier les dispositifs sans fil des voyageurs, mais pas le contenu des appels effectués ou des courriers électroniques envoyés depuis ces appareils. D'après CBC, ce programme était un essai grandeur nature d'un programme d'utilisation d'un nouveau logiciel puissant, mis au point par le Canada avec l'aide de la NSA; la technologie testée en 2012 est depuis devenue pleinement opérationnelle.

2.2.2. Un partenariat complémentaire avec d'autres pays d'Europe

26. D'autres informations ont été publiées à propos de la collaboration entre les Etats-Unis et l'Europe et des initiatives prises individuellement par les Etats européens pour la mise en place de programmes de surveillance massive. En France, *Le Monde* a révélé que la Direction générale de la sécurité extérieure (DGSE) disposait d'un libre accès intégral aux réseaux et aux flux de données qui transitent par la société française de télécommunications Orange, y compris les informations relatives aux ressortissants étrangers et français[24]. Toutefois, contrairement au programme américain Prism, la France n'a pas officialisé la coopération entre la DGSE et France Telecom-Orange, mais recourt à des connexions informelles effectuées par des ingénieurs qui «naviguent» entre les deux institutions depuis au moins les 30 dernières années.

27. Selon certaines informations, les Pays-Bas ont intercepté d'énormes quantités de communications téléphoniques somaliennes, qu'ils ont mises en commun avec la NSA[25]. Les autorités néerlandaises ont affirmé qu'elles ne collectaient pas d'informations à la demande des Etats-Unis, mais pour appuyer la mission de lutte contre la piraterie menée par la marine néerlandaise dans le golfe d'Aden. Le *NRC Handelsblad* a indiqué que les Etats-Unis pourraient avoir utilisé ces informations pour lancer des attaques de drones contre des personnes soupçonnées d'activités terroristes[26].

28. Le Danemark a lui aussi collaboré étroitement avec les Etats-Unis à des activités de surveillance à la fin des années 1990. Des documents secrets ont révélé que le Danemark était soumis à de «fortes pressions» de la part des Etats-Unis pour qu'il modifie sa législation et autorise l'écoute des communications, afin de conserver ses «bonnes fréquentations», autrement dit le «Réseau Echelon» ou les «9-eyes», qui collaborent étroitement avec la NSA. Au cours de la période 1998-2000 évoquée dans les documents secrets,

24. *Le Monde*, 20 mars 2014, «Espionnage: comment Orange et les services secrets coopèrent».
25. *NRC Handelsblad*, «The secret role of the Dutch in the American war on terror».
26. *Ibid*.

le service de renseignement de la Défense nationale danoise aurait bénéficié d'une «aide technique» pour décrypter les codes des communications sur écoute et de techniques de surveillance destinées à l'écoute d'internet et à «l'identification des téléchargements illicites sur internet»[27]. Le directeur du service de renseignement de la Défense danoise n'a ni confirmé ni nié le partenariat avec la NSA[28].

29. Les révélations de M. Snowden ont également fait apparaître une collaboration étendue entre l'Allemagne et les Etats-Unis. En juin 2014, *Der Spiegel* a révélé que les activités de la NSA étaient plus importantes en Allemagne que dans n'importe quel autre pays d'Europe et a fait état des rapports de plus en plus étroits que l'agence américaine avait établis au cours de ces treize dernières années avec le *Bundesnachrichtendienst* (*BND*), le service allemand de renseignement extérieur, qui rend directement compte des ses activités à la chancellerie[29]. De nombreux sites de collaboration et de surveillance ont été recensés. Le siège européen de la NSA à Stuttgart surveille attentivement l'Afrique et certains documents des services de renseignement précisent que les indications données par ces derniers ont permis «la capture ou la liquidation de plus de 40 terroristes et ont contribué à mener avec succès la guerre planétaire contre le terrorisme et une politique régionale en Afrique» en transmettant des informations au commandement européen de l'armée américaine ou à divers gouvernements africains. Un accord passé en 2004 entre l'Allemagne et les Etats-Unis a permis la création de ce qui est à présent le Centre européen de cryptologie (European Cryptologic Centre – ECC), actuellement la plus importante station d'écoute en Europe. Cet organisme collecte, traite, analyse et diffuse des informations à des fins réputées militaires, mais un document de présentation de 2012 laisse penser que les flux de données européens font également l'objet d'une surveillance à grande échelle. L'ECC a pour cible l'Afrique et l'Europe, car «la plupart des terroristes font une halte en Europe», comme l'affirme un document de présentation de la NSA[30]. Le Centre technique européen (European Technical Centre) de Wiesbaden servirait également de «principale plate-forme des communications» de la NSA, en interceptant d'immenses quantités de données et les transmettant aux agents et aux combattants de la NSA, ainsi qu'aux partenaires étrangers d'Europe, d'Afrique et du Moyen-Orient. Enfin et surtout, le Service spécial de collecte de données du consulat général américain de Francfort s'est retrouvé au centre d'une enquête ouverte par les autorités allemandes au sujet des écoutes du téléphone de la chancelière Merkel. Les agents qui travaillent au sein de ce poste d'écoute, ainsi que ceux de l'ambassade américaine à Berlin, seraient protégés par une accréditation diplomatique, alors même que leur activité n'est pas visée par les accords internationaux qui garantissent l'immunité diplomatique. Quant à la coopération entre le BND et la NSA à Bad Aibling, établie sur la base d'un mémorandum d'accord qui remonte à 2002, la commission d'enquête du Bundestag sur l'affaire de la NSA[31] a déjà procédé à un certain nombre d'auditions publiques de témoins qui ont expliqué en quoi consistaient ces activités, lesquelles ont pris fin en 2012.

2.2.3. Une collusion visant à se soustraire aux restrictions

30. Ces partenariats entre les Etats-Unis et les services alliés permettent aux gouvernements de pratiquer ce qui pourrait être qualifié de «collusion visant à se soustraire aux restrictions». Ainsi, le service de renseignement britannique GCHQ est autorisé à espionner toute personne à l'exception des ressortissants britanniques; la NSA peut espionner toute personne à l'exception des ressortissants américains et le BND allemand toute personne à l'exception des ressortissants allemands. Les partenariats d'échange d'informations permettent à chaque service de se soustraire à ses propres restrictions nationales qui protègent les ressortissants de son pays, puisqu'il peut accéder aux données collectées par les services des autres pays[32].

31. Cette «collusion visant à se soustraire aux restrictions» a d'importantes ramifications à l'échelon national dès lors qu'elle est utilisée stratégiquement pour contourner la législation interne et se soustraire aux restrictions imposées à la capacité du gouvernement à mettre sur écoute les communications de ses propres citoyens. L'ancien président de la Cour constitutionnelle fédérale, Hans-Jürgen Papier, un ancien juge de la Cour constitutionnelle, M. Wolfgang Hoffmann-Riem, et un autre éminent expert, le professeur Matthias Bäcker, ont déclaré qu'en travaillant à l'aide de données reçues de la NSA, le BND pouvait commettre une violation de la Constitution allemande. Ils ont en outre affirmé que les droits constitutionnels fondamentaux, comme le respect de la confidentialité de la correspondance, des colis postaux et des télécommunications, étaient applicables aux ressortissants allemands à l'étranger et aux ressortissants étrangers en Allemagne et

27. Andreas Jakobsen, «Spying programs with NSA goes back years», *The Copenhagen Post*, 30 juin 2014.
28. Anton Geist, Sebastian Gjerding, Henrik Moltke et Laura Poitras, 19 juin 2014, www.information.dk/501280.
29. *Der Spiegel*, 18 juin 2014, «New NSA Revelations: Inside Snowden's Germany File».
30. *Ibid*.
31. Paragraphe 77.
32. *Der Spiegel*, 1er juillet 2013, «Cover Story: How the NSA Targets Germany and Europe».

que les accords secrets passés entre les services de renseignement ne sauraient fonder juridiquement une atteinte à ces droits. Cela signifierait par conséquent que ce type de coopération à des fins de surveillance entre le BND et la NSA serait inconstitutionnel[33].

32. Au vu des allégations de M. Snowden à ce sujet lors de notre audition de juin 2014, j'ai adressé aux autorités allemandes, britanniques et américaines les questions suivantes:

> *1. Est-il vrai que les services américains compétents (notamment la NSA) aient obtenu des informations relatives à des ressortissants américains, collectées par leurs homologues en Allemagne [au Royaume-Uni], qu'ils n'étaient pas juridiquement autorisés à collecter eux-mêmes?*
>
> *2. Est-il vrai que, de leur côté, les services américains compétents aient fourni à leurs homologues allemands [britanniques] des informations relatives à des ressortissants allemands [britanniques] que les services allemands n'étaient pas juridiquement autorisés à collecter eux-mêmes?*

33. Les autorités allemandes ont répondu de façon brève et sèche que «les services de renseignement allemands respectent la législation. Les données à caractère personnel sont transmises aux services de renseignement étrangers, conformément aux dispositions légales pertinentes. Ces dispositions ne sont contournées d'aucune manière»[34].

34. La réponse des autorités britanniques comporte une présentation fort utile de la législation applicable et des mécanismes de contrôle[35] et souligne que «la collecte d'informations par les services de renseignement de l'Etat doit être effectuée de façon proportionnée et non arbitraire, à des fins légitimes, conformément à l'Etat de droit et soumise à un contrôle effectif». A propos de la question, la lettre précise: «Vous nous avez demandé si les relations de travail approfondies entre le GCHQ du Royaume-Uni et la NSA des Etats-Unis ont servi à contourner les dispositions légales nationales relatives à la collecte d'informations. La réponse est non, en aucun cas.»

35. Les autorités américaines n'ont pas répondu à ma lettre, ni à mon courrier de rappel envoyé le 18 décembre 2014.

36. Le libellé très strict de la réponse allemande concerne uniquement la transmission des données à caractère personnel aux services de renseignement étrangers. Les données à caractère personnel des ressortissants allemands sont bien protégées par le droit et rien ne permet de douter de l'application de cette protection, comme l'indique la lettre. Les auditions publiques auxquelles a procédé la commission d'enquête du Bundestag au sujet de «la série de questions relatives à Bad Aibling» démontrent même dans quelques cas isolés que la coopération entre le BND et la NSA à l'aide des installations américaines et allemandes présentes dans cette ville, qui reposait sur un mémorandum d'accord d'avril 2002, a pris fin en 2012 à l'initiative des Etats-Unis, contrariés par l'insistance de leurs partenaires allemands à expurger (de manière fastidieuse) toutes les données relatives à des ressortissants allemands en raison des obligations légales nées de l'article 10 de la Constitution allemande (*Grundgesetz*). Mais la réponse des autorités allemandes ne mentionne pas, du moins pas expressément, les données relatives aux ressortissants allemands communiquées par leurs partenaires étrangers dans le cadre de cette coopération; la protection des données allemandes fondée sur l'article 10 n'est pas applicable aux ressortissants étrangers, par exemple aux citoyens américains, dont les données ont par conséquent pu être transmises aux services de renseignement de leur pays d'origine. D'après ce qui ressort, selon moi, de la lecture des comptes rendus des auditions publiques, les objections légales soulevées par les partenaires allemands, qui ont tant «contrarié» leurs collègues de la NSA, concernaient uniquement les données allemandes.

37. La réponse britannique à la question du contournement de la législation est si catégorique que je ne me permettrais pas de la remettre en question. Mais il me semble que depuis l'adoption en (extrême) urgence de la loi relative à la conservation des données et aux pouvoirs d'investigation (Data Retention and Investigatory Powers Act – DRIPA) en juillet 2014[36] et le rejet de la loi américaine relative aux libertés (USA Freedom Act) en septembre 2014, la véritable question qui se pose est de savoir si les dispositions légales nationales pertinentes (au Royaume-Uni et aux Etats-Unis) qui régissent la conservation et l'utilisation des données à caractère personnel sont libellées de façon suffisamment précise et assorties d'un contrôle suffisamment efficace pour protéger le respect de la vie privée des ressortissants britanniques et américains. D'après mes déductions, la nouvelle loi, combinée avec la loi relative à la régulation des pouvoirs d'investigation (Regulation of Investigatory Powers Act – RIPA) adoptée en 2000 et l'interprétation donnée par la NSA des

33. *Der Spiegel*, 18 juin 2014 (note 29).
34. Réponse du 26 septembre 2014 (traduction du secrétariat).
35. Disponible auprès du secrétariat.
36. Paragraphe 74.

dispositions en vigueur aux Etats-Unis[37] permet la collecte, l'utilisation et la transmission à grande échelle des données à caractère personnel, notamment des métadonnées, de sorte qu'il semble peu utile de chercher encore à contourner la législation. C'est ce que confirme la décision rendue par le tribunal des pouvoirs d'investigation (Investigatory Powers Tribunal – IPT) le 5 décembre 2014[38], qui a conclu, en se fondant sur les politiques gouvernementales secrètes, que l'échange d'informations des services de renseignement avec la NSA ou l'accès aux informations obtenues à l'aide du programme PRISM de la NSA ne posait aucun problème[39].

2.3. Une surveillance qui n'épargne rien ni personne

38. Malgré des partenariats et une collaboration solides, voire une connivence entre la NSA et les services de renseignement de certains pays alliés, les fichiers Snowden montrent qu'aucun Etat, aucune personne ni aucune organisation – quels que soient ses liens avec les Etats-Unis – n'échappe à cette surveillance.

2.3.1. L'approbation par les Etats-Unis d'une surveillance exercée sur le monde entier, à l'exception de quatre pays

39. En juin 2014, le *Washington Post* a révélé que la Foreign Intelligence Surveillance Court (FISC – juridiction de contrôle du service de renseignement extérieur) avait autorisé la NSA à intercepter des informations «concernant» tous les pays du monde, à l'exception de quatre d'entre eux (c'est-à-dire les quatre autres Etats de l'alliance Five Eyes, sauf leurs territoires souverains, comme les îles Vierges britanniques) et d'organisations internationales comme la Banque mondiale, le Fonds monétaire international et l'Agence de l'énergie atomique[40]. La NSA ne prend pas nécessairement pour cible toutes les cibles recensées dans cette certification à tout moment, mais elle a le pouvoir de le faire.

2.3.2. Le refus de conclure des «accords de non-espionnage» avec un quelconque pays

40. En dépit des relations exclusives qu'entretiennent les cinq membres de l'alliance Five Eyes, il semble que les Etats-Unis et les quatre autres Etats ne se fassent pas une idée identique de l'existence ou non d'un «accord de non-espionnage» entre eux. Les documents classifiés indiquent que «la NSA ne prend pas pour cible ses partenaires et ne leur demande pas de faire ce qui est fondamentalement illégal pour elle», ce qui met en avant les relations privilégiées que les Etats-Unis entretiennent avec les membres de Five Eyes[41]. Pourtant, les Etats-Unis ont souligné à plusieurs reprises qu'ils n'avaient conclu aucun «accord de non-espionnage» avec un quelconque pays, pas même avec leurs partenaires de l'alliance Five Eyes; de fait, le texte de l'accord Royaume-Uni-Etats-Unis ne mentionne pas expressément un tel accord. L'administration américaine a au contraire précisé sa position, en expliquant que, bien qu'il n'existe «aucun accord officiel de ce type (…), des ententes ou des accords bilatéraux sont prévus avec un tout petit nombre de gouvernements (qui précisent, le cas échéant, les intentions, les restrictions et les limites de la collecte des informations). Ces relations bilatérales reposent sur des décennies d'habitudes, de transparence et de pratiques communes d'une politique et d'activités de renseignement pertinentes»[42].

41. Cela dit, un projet (distinct) de note communiqué par M. Snowden, intitulé «Collecte, traitement et diffusion des communications alliées» (Collection, Processing and Dissemination of Allied Communications), révèle que ces relations de confiance anciennes ont elles-mêmes leurs limites. La note dévoilée présente différents niveaux de classification pour chacun de ses paragraphes. Un paragraphe dont la mise en commun avec les membres de l'alliance Five-Eyes (les pays «partenaires») a été autorisée mentionne le fait que les gouvernements ont convenu qu'aucun d'eux ne prendra pour cible les ressortissants de l'autre. Mais le paragraphe suivant, dont la classification ne prévoit pas la communication aux partenaires étrangers («*noforn*») précise que les gouvernements «se réservent le droit» d'effectuer des opérations de renseignement contre les ressortissants de leurs partenaires «dans l'intérêt supérieur de chaque pays». Le projet de note ajoute que, «dans certaines situations, il peut être conseillé et permis de cibler unilatéralement les ressortissants d'un partenaire et les systèmes de communication d'un partenaire, lorsque l'intérêt supérieur des Etats-Unis et leur sécurité nationale le commande».

---

37. Paragraphes 44 à 52.
38. Paragraphe 75.
39. Jennifer Baker, «Nothing illegal to see here: Tribunal says TEMPORA spying is OK», *The Register*, 5 décembre 2014.
40. *The Washington Post*, 30 juin 2014, «Court gave NSA broad leeway in surveillance, documents show».
41. *Der Spiegel*, 1er juillet 2013, «How the NSA Targets Germany and Europe».
42. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (12 décembre 2013), p. 175.

2.3.3. Le «bazar européen» ou les espions espionnés

42. Les pays européens, y compris ceux qui participent étroitement aux activités de la NSA, ne sont pas épargnés par la surveillance des Etats-Unis. Grâce au programme RAMPART-A, la NSA recourt à ses partenaires étrangers, qui lui permettent d'accéder aux réseaux câblés de communications et qui accueillent le matériel américain, pour transporter, traiter et analyser les données interceptées. Lorsque le pays partenaire met sous surveillance un réseau câblé international à partir d'un point d'accès situé sur son territoire, il envoie les données à un centre de traitement équipé par la NSA, puis les transmet à un site de la NSA installé aux Etats-Unis. Les Etats collaborent par conséquent à la collecte et au traitement des contenus des appels téléphoniques, des fax, des courriers électroniques, des messageries instantanées, des données provenant de réseaux privés virtuels et des appels vidéo en ligne. Selon certaines sources, il existerait 13 sites RAMPART-A, dont neuf qui étaient en activité en 2013. Les révélations ont fait apparaître 33 pays tiers, dont l'Autriche, la Belgique, la Croatie, la République tchèque, le Danemark, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Italie, «l'ex-République yougoslave de Macédoine», les Pays-Bas, la Norvège, la Pologne, la Roumanie, l'Espagne, la Suède et la Turquie[43]. Le fonctionnement de ces partenariats est soumis à la condition que le pays d'accueil n'utilise pas la technologie d'espionnage de la NSA pour collecter des données sur les ressortissants américains. En contrepartie, la NSA accepte de son côté de ne pas collecter de données sur les ressortissants des pays d'accueil, à certaines exceptions près, qui ne sont pas précisées dans les documents divulgués. Néanmoins, les accords bilatéraux de non-espionnage réciproque passés entre les Etats-Unis et les Etats tiers sont insignifiants et faciles à contourner, ce qui donne lieu à ce que M. Snowden appelait un «bazar européen». Selon ses explications, les Etats-Unis peuvent tout simplement se contenter d'accéder aux communications du pays A qui transitent par le pays B, ce qui leur permet techniquement de ne pas violer l'accord de non-espionnage des communications qu'ils ont passé avec le pays A. De fait, la NSA s'est vantée dans sa propre documentation de présentation interne d'être «capable de prendre pour cible les signaux de la plupart des partenaires étrangers tiers, ce qu'elle fait bien souvent», malgré le fait que ces pays lui apportent leur soutien et qu'elle collabore avec eux.

43. Les récentes révélations sur la surveillance répétée et constante de l'Allemagne par la NSA montrent l'étendue de la surveillance secrète que pratique la NSA à l'égard de ses propres alliés, dont les activités et les données semblent, dans le meilleur des cas, fort peu en rapport avec les initiatives prises par les Etats-Unis pour protéger leurs propres citoyens du terrorisme ou des autres menaces qui pèsent sur la sécurité nationale. La chancelière Angela Merkel figurait ainsi, avec 121 autres chefs d'Etat et de gouvernement, dans la base de données centrale «Target Knowledge Base» de l'Agence, qui regroupe les cibles individuelles afin de permettre à ses employés d'analyser les «profils complets» des personnes ciblées. En mars 2013, la NSA a également obtenu qu'une ordonnance judiciaire top secret soit rendue contre l'Allemagne dans le cadre des mesures prises par le Gouvernement américain pour surveiller les communications en rapport avec ce pays; le GCHQ a pris pour cible trois sociétés allemandes dans une opération clandestine, qui consistait à infiltrer les serveurs informatiques des entreprises et à mettre sur écoute les communications de leur personnel. A la suite du scandale de l'écoute du téléphone de la chancelière Merkel par la NSA, un étudiant du nom de Sebastian Hahn a été identifié comme le deuxième citoyen allemand connu à être placé sous surveillance par l'Agence américaine. M. Hahn, domicilié en Bavière, est devenu la cible des Etats-Unis parce qu'il utilisait légalement un serveur dans le cadre du réseau Tor, auquel recourent les usagers qui cherchent à préserver la confidentialité de leurs activités sur internet. Deux des principales chaînes allemandes de service public, NDR et WDR, ont annoncé simultanément que la NSA espionnait tout particulièrement les personnes qui utilisent des systèmes de cryptage et d'anonymisation pour dissimuler les flux de données. Le simple fait de rechercher sur internet un logiciel de cryptage et de renforcement de la sécurité des données amène la NSA à relever et à surveiller l'adresse IP de l'auteur de la recherche, quel que soit le pays où il se trouve. Depuis le 10 juillet 2014, les services répressifs fédéraux allemands ont ouvert une enquête sur deux personnes soupçonnées d'espionnage pour le compte des Etats-Unis, l'une au Service de renseignement fédéral (BND) et l'autre au ministère de la Défense à Berlin. La première aurait été arrêtée au moment où elle tentait de vendre aux services de renseignement russes une partie des informations qu'elle avait recueillies depuis deux ans pour le compte des Etats-Unis[44]. Dans un pays où la question de la surveillance est particulièrement sensible en raison du souvenir de la surveillance abusive pratiquée par la Gestapo (police secrète nazie) et la Stasi (police de la sécurité d'Etat est-allemande), ces révélations ont contribué à refroidir considérablement les relations avec les Etats-Unis.

---

43. Les autres pays tiers étaient l'Algérie, l'Ethiopie, l'Inde, Israël, le Japon, la Jordanie, La Corée, le Pakistan, l'Arabie saoudite, Singapour, Taïwan, la Thaïlande, la Tunisie et les Emirats arabes unis, *Russia Today*, 19 juin 2014, «NSA uses 33 countries to intercept web traffic – Snowden Files».

44. *Russia Today*, 7 juillet 2014, «Merkel's mad: German leader indignant over "serious" US spying allegations».

2.3.4. Les ressortissants américains également placés sous surveillance

44. Le Gouvernement américain a souligné à plusieurs reprises qu'il réservait un traitement distinct aux ressortissants américains et aux ressortissants étrangers dans ses programmes de surveillance. Pour obtenir une ordonnance judiciaire de mise sur écoute d'un ressortissant américain, le gouvernement doit par exemple convaincre un juge qu'il existe des «motifs raisonnables et suffisants» de croire que la cible commet une infraction pour le compte d'une puissance étrangère; quant aux ressortissants non américains, il suffit qu'ils soient «soupçonnés» d'être des agents étrangers. Pour autant, les ressortissants américains ne sont pas épargnés par la surveillance de leur propre gouvernement. Quelques jours après l'approbation par la Commission de surveillance du respect de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board) des programmes utilisés au titre de l'article 702 principalement à l'encontre des ressortissants étrangers[45], le *Washington Post* a indiqué que neuf communications sur dix interceptées dans le cadre de ces programmes n'étaient pas directement visées par les mesures de surveillance de la NSA et que les utilisateurs ordinaires d'internet, qu'ils soient Américains ou non, étaient très supérieurs en nombre aux ressortissants étrangers ciblés par décision judiciaire[46]. Pendant quatre mois, le quotidien a enquêté sur des rapports de surveillance, dont le nombre est estimé à 22 000, réunis par la NSA entre 2009 et 2012, c'est-à-dire au cours du premier mandat d'Obama, pendant lequel la collecte nationale de données effectuée par la NSA a augmenté de manière exponentielle. Les fichiers divulgués par M. Snowden comportent un très grand nombre de courriers électroniques, de messages, de photos et de documents, dont le précieux contenu concernait un projet nucléaire secret à l'étranger, les identités de pirates informatiques particulièrement agressifs à l'égard des réseaux informatiques américains et les déboires militaires d'une puissance hostile. Mais ces données comportaient également des communications «à caractère étonnamment intime, voire voyeuriste» entre plus de 10 000 titulaires de comptes qui n'étaient pas ciblés, mais dont les informations ont été néanmoins enregistrées. Dans cet échantillon, environ neuf communications sur dix n'étaient pas directement ciblées par la surveillance de la NSA; selon les chiffres communiqués dans un «rapport sur la transparence» du 26 juin 2014 de la Direction du renseignement national, 89 238 personnes ont été la cible de la collecte de données effectuée l'année précédente au titre de l'article 702 de la loi relative à la surveillance des services de renseignement extérieur (Foreign Intelligence Surveillance Act, loi fédérale américaine qui autorise la surveillance des «informations des services de renseignement extérieur» échangées entre les «puissances étrangères» et les «agents de puissances étrangères»). Sur la base du ratio établi pour l'échantillon de M. Snowden, les chiffres de la Direction équivaudraient à près de 900 000 comptes, ciblés ou non, placés sous surveillance. En outre, la moitié environ de ces fichiers de surveillance contenaient des noms, des adresses électroniques ou d'autres précisions concernant, selon la NSA, des ressortissants ou résidents américains.

45. La NSA a justifié ses pratiques en insistant sur le fait qu'elles visaient uniquement des cibles valables du renseignent extérieur et la seule conclusion qui pouvait être tirée à la lecture du *Washington Post* était que les cibles en question étaient en contact avec neuf personnes en moyenne. La NSA affirme que la collecte fortuite d'informations relatives à des personnes non ciblées est inévitable et que, dans d'autres situations, le Gouvernement américain s'efforce de limiter et d'écarter les données dépourvues de pertinence (par exemple, en cas de mise sur écoute dans le cadre d'affaires criminelles, le FBI est censé cesser d'écouter un appel lorsque la femme ou l'enfant d'un suspect est au téléphone. Il convient cependant de noter que si certaines données ont été collectées de manière fortuite parce que des personnes communiquaient directement avec une cible, d'autres données avaient un lien plus ténu avec la cible en question. Ainsi, la NSA a recueilli les propos et les identités de toute personne qui, quel que soit le sujet, postait sur un forum de discussion ou se contentait de le lire au moment où la cible y participait. Le fait de présumer que les auteurs de courriers électroniques rédigés dans une langue étrangère ou que toute personne figurant sur la «liste d'amis» d'un ressortissant étranger présent sur un forum de discussion soient également des ressortissants étrangers, ou le fait qu'une personne se connecte sur une adresse informatique qui semble étrangère (bien que des outils extrêmement simples, de type proxy, puissent permettre de rediriger le flux de données d'un utilisateur dans le monde entier) ont été, pour les analystes, autant de «motifs raisonnables et suffisants» de croire que les cibles détenaient de précieuses informations sur un gouvernement étranger, une organisation terroriste ou sur la diffusion d'armes non conventionnelles au titre des dispositions applicables aux programmes PRISM et Upstream.

46. Cette révélation est intervenue quelques jours à peine après la conclusion, par la Commission de surveillance du respect de la vie privée et des libertés civiles, que la politique d'interception des communications appliquée par la NSA, que l'agence affirmait fondée sur l'article 702, s'était efforcée de

45. Pour de plus amples précisions, la partie 2.6.

46. *The Washington Post*, 5 juillet 2014, «In NSA-intercepted data, those not targeted far outnumber the foreigners who are».

«réduire au minimum» cette prise accessoire de données, ce que la Commission avait jugé dans l'ensemble efficace[47]. L'échantillon de M. Snowden montre qu'un grand nombre de communications de cibles non visées continuent à être prises dans les filets de l'agence. Cette révélation est par ailleurs importante, car le général Keith Alexander a nié à plusieurs reprises que M. Snowden puisse avoir transmis le contenu même des communications interceptées à un journaliste – ce qu'il a pourtant bel et bien fait – puisqu'il n'avait pas accès à ces données. M. Snowden affirme que sa fonction d'agent contractuel pour le compte de Booz Allen au centre d'opération de la NSA à Hawaii lui a donné «un libre accès, d'une étendue inhabituelle, à des données de transmission brutes des services de renseignement (SIGINT) à l'occasion des fonctions particulières qu'il exerçait pour le compte de deux autorités».

47. Les fichiers Snowden révèlent par ailleurs que les services de renseignement américains ont surveillé des militants, avocats et responsables politiques musulmans de premier plan en se fondant sur une législation qui visait les terroristes et les espions étrangers[48]. D'après les documents divulgués, la NSA et le FBI ont surveillé secrètement les courriers électroniques de musulmans américains en vue, dont les noms étaient inscrits sur une liste de 7 485 adresses électroniques surveillées de 2002 à 2008, parallèlement à des ressortissants étrangers accusés depuis longtemps de mener des activités terroristes. Parmi eux figurait M. Faisal Gill, avocat et ancien conseiller politique des services de renseignement au Département de la sécurité intérieure, qui était autorisé à accéder aux informations classées sensibles, c'est-à-dire auxquelles était attribué un niveau de classification réservé aux secrets les plus étroitement gardés. Il avait servi dans l'armée américaine et travaillé pour le compte de l'administration de George W. Bush de fin 2001 à 2005. La NSA a pourtant commencé à surveiller son compte en 2006, lorsqu'il a quitté son emploi dans l'administration pour devenir le cofondateur d'une étude d'avocats en compagnie d'Asim Ghafoor, avocat spécialisé dans la défense des droits des musulmans, qui représentait des gouvernements étrangers et des organisations du Moyen-Orient devant les juridictions américaines et qui, selon le rapport, était également la cible des activités des services de renseignement américains. Il a été surveillé une nouvelle fois par la NSA de mars 2005 à au moins mars 2008, au moment où il intentait une action en justice contre le gouvernement en raison de la surveillance illégale antérieure de ses communications à caractère personnel.

48. Pour pouvoir placer un ressortissant américain sous surveillance, les agences de renseignement doivent démontrer l'existence de motifs raisonnables et suffisants de croire que les cibles américaines sont les agents d'une puissance étrangère ou d'une organisation terroriste internationale et qu'elles «prennent part ou peuvent prendre part» à la commission ou la complicité d'actes d'espionnage, de sabotage ou de terrorisme. Les responsables américains insistent sur le fait que les vérifications internes prévues dans la procédure en vigueur écartent tout risque d'abus. La Direction du renseignement du Département de la Justice possède divers «garde-fous» qui rejettent fréquemment des demandes (au moins dans la moitié des cas) ou les renvoient à leurs auteurs pour qu'elles soient réexaminées. Enfin, l'agent désireux de placer sous surveillance un citoyen américain doit démontrer, devant la Foreign Intelligence Surveillance Court (FISC – juridiction de contrôle du service de renseignement extérieur), l'existence de «motifs raisonnables et suffisants» de penser que l'intéressé est un agent d'une puissance étrangère et prend part ou est sur le point de prendre part à l'une des «trois infractions» prévues par la loi relative à la surveillance des services de renseignement extérieur (FISA), c'est-à-dire à un attentat avéré ou possible, ou à un autre acte grave hostile, de sabotage ou de terrorisme international, ou encore à des activités clandestines de renseignement. Dans la quasi-totalité des affaires dont est elle saisie, la FISC accorde l'autorisation de procéder à une surveillance, mais les agents des services de renseignement affirment que seules les demandes les plus fondées sont déposées devant cette juridiction.

49. Pourtant, d'après *The Intercept*, la procédure devant la FISC n'est pas contradictoire et les critères de la démonstration de l'existence de «motifs raisonnables et suffisants» ne sont pas précisés. Un ancien agent des services répressifs a indiqué dans une interview que les juges se contentent bien souvent des assertions des agents auteurs de la demande d'autorisation et qu'il a lui-même obtenu de nombreux mandats signés à deux heures du matin par un juge en pyjama dans son salon.

50. Ces révélations rappellent de façon dérangeante les anciennes pratiques employées pour la surveillance des militants des droits civiques tels que Martin Luther King – voire de manière plus troublante encore compte tenu de l'efficacité accrue des outils de surveillance dont dispose désormais le gouvernement. L'un des documents divulgués de la NSA décrivait une cible potentielle à surveiller d'après la FISA comme un «enturbanné[49]» et certains agents des services répressifs qui participaient aux activités de lutte contre le terrorisme avaient considéré des ressortissants américains de confession musulmane comme des gens

47. *New York Times*, 6 juillet 2014, «Officials Defend NSA After New Privacy Details Are Reported».
48. *The Intercept*, 9 juillet 2014, «Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On».
49. Insulte raciste utilisée à l'égard des personnes qui portent un couvre-chef islamique.

sectaires et des conspirateurs. *The Intercept* a cité les propos de M. John Guandolo, ancien agent de lutte contre le terrorisme, qui a sans complexe qualifié un avocat musulman de «principal protagoniste des Frères musulmans aux Etats-Unis» ou de «djihadiste» «directement lié à des membres d'Al-Qaïda», pour la simple raison qu'il représentait des fondations ou des gouvernements du Moyen-Orient. Les points de vue anti-islamiques de M. Guandolo ont même été insérés dans les principaux documents de formation utilisés par l'agence. Cette démarche montre que des personnes peuvent être victimes d'une surveillance intrusive sur la base de clichés et de preuves discutables.

51. Une réponse conjointe de la Direction du renseignement national et du Département de la Justice précise qu'il «est totalement faux que les services de renseignement américains procèdent à une surveillance électronique de personnalités politiques et religieuses ou de militants pour l'unique raison qu'ils sont en désaccord avec la politique nationale, critiquent le gouvernement ou exercent leurs droits constitutionnels»[50]. Il est difficile de porter une appréciation sur cette réponse, qui n'exclut de toute façon pas que la religion ou des critiques soient utilisés comme des facteurs décisifs déterminant des mises sous surveillance, compte tenu du manque de transparence qui règne à propos des critères retenus par l'administration pour initier une surveillance.

52. Un nouveau donneur d'alerte a entretemps fait son apparition: John Napier Tye, ancien chef de l'unité Liberté d'internet du Bureau de la démocratie, des droits de l'homme et du travail du Département d'Etat de janvier 2011 à avril 2014, où il était habilité à recevoir des informations top secret et «classées sensibles». Le 18 juillet 2014, M. Tye a révélé dans les colonnes du *Washington Post* que, bien que le débat sur les opérations de surveillance massive se soit focalisé sur la collecte de données effectuée au titre de l'article 215 du «Patriot Act», ces activités ne représentent qu'une faible portion des opérations de surveillance et «n'englobent pas l'intégralité de la collecte et de la conservation des communications des ressortissants américains, autorisées par le décret d'application 12333», dont les répercussions sur les citoyens américains posent davantage problème que l'article 215[51]. Le décret d'application 12333, pris en 1981 par le Président Reagan, n'offre aucune garantie aux ressortissants américains eux-mêmes lorsque la collecte de données est pratiquée hors du territoire américain. Le texte impose aux agents d'obtenir une ordonnance judiciaire pour procéder à la surveillance d'une personne précise, mais en cas de collecte «fortuite» du contenu des communications d'un ressortissant américain (aussi bien le contenu que les métadonnées) à l'occasion de la surveillance légale d'un autre ressortissant étranger, l'article 2.3.*c* du décret 12333 autorise expressément la conservation de ces données, sans condition ni limite. M. Tye a précisé que le propre Groupe d'étude du Président Obama sur les technologies de renseignement et de communication (Review Group on Intelligence and Communication Technologies) avait à l'esprit le décret 12333 lorsqu'il a préconisé dans la Recommandation 12 de son rapport public que le Gouvernement expurge immédiatement les communications américaines collectées de manière «fortuite», ce que la Maison Blanche a refusé de faire.

2.4. Le recours abusif à des opérations de surveillance massive motivé par des considérations politiques avérées et/ou possibles

53. Les récentes révélations montrent que les opérations de surveillance massive ont servi à entraver l'activité des opposants politiques, des militants de la défense des droits de l'homme ou des journalistes. Comme je l'ai indiqué dans ma note introductive, la NSA a surveillé la navigation, sur des sites pornographiques, de six musulmans considérés comme des islamistes dont le discours incite à la haine, pour nuire à leur crédibilité et à leur réputation[52]. M. Snowden a confirmé lors de son audition devant notre commission que la NSA avait même eu recours à la surveillance d'organisations de défense des droits de l'homme. Il est difficile d'imaginer en quoi espionnage d'organisations comme Amnesty International ou Human Rights Watch peut se justifier «dans l'intérêt de la sécurité nationale». Les activités de ces organisations, extrêmement précieuses en raison de leur contribution à la promotion de nos valeurs communes, sont en revanche gravement compromises lorsque les victimes et les témoins d'actes de violation des droits de l'homme n'osent plus communiquer librement avec ceux qui cherchent à les aider parce qu'ils craignent d'être surveillés.

---

50. Joint Statement by the Office of the Director of National Intelligence and the Department of Justice on Court-ordered Legal Surveillance of U.S. Persons, 9 juillet 2014.
51. *The Washington Post*, 18 juillet 2014, «Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans».
52. Document AS/Jur (2014) 02, 23 janvier 2014, paragraphe 20.

2.4.1. L'espionnage ciblé à des fins politiques et économiques

54. Les fichiers Snowden ont confirmé que les Etats s'espionnaient les uns les autres ou procédaient à une surveillance qui, dans le meilleur des cas, avait un rapport très limité avec la lutte contre le terrorisme. *Le Monde* a indiqué que grâce à son programme de collecte des données Upstream, la NSA était en mesure d'intercepter les communications de diverses cibles, dont deux dirigeants philippins, Jejomar Binay et Manuel Roxas, qui ne sont pas connus pour leurs positions anti-américaines, un complexe hôtelier situé au Honduras qui accueille des conférences internationales, le Centre international de physique théorique en Italie, AT&T, la Société saoudienne des télécommunications (Saudi Telecom Company), la société internet autrichienne Chello, la société pakistanaise de sécurité en ligne Tranchulas et la société libyenne de télécommunications Libyan International Telecom Company[53].

55. Une présentation interne de la NSA de 2010 donne d'autres exemples de la surveillance ciblée effectuée par l'agence. Ce document montre que l'opération «Royal Concierge» menée par le GCHQ a consisté à surveiller au moins 350 hôtels de luxe à travers le monde pendant plus de trois ans «pour cibler, rechercher et analyser les réservations, afin de déceler la présence de diplomates et de haut responsables de gouvernements». L'agence a mis sur écoute les appels téléphoniques et a surveillé les ordinateurs des hôtels, tout en envoyant des agents de renseignement observer en personne les cibles dans les hôtels en question[54]. *The Guardian* a également révélé que la NSA utilisait un programme baptisé Dropmire pour intercepter les faxes à sécurité renforcée et accéder aux documents transmis par des faxes cryptés depuis des ambassades étrangères situées dans d'autres pays[55].

56. L'agence de renseignement britannique a collaboré avec son homologue américain pour extraire des informations à partir des applications non sécurisées pour smartphones, comme le jeu Angry Birds. Ces opérations leur ont permis d'obtenir l'âge, le sexe, la géolocalisation, le modèle de téléphone, la taille de l'écran et, dans certains cas, des informations sensibles telles que l'orientation sexuelle des intéressés, grâce à leurs instruments de surveillance massive.

57. Le New York Times a révélé que la NSA surveillait une étude d'avocats américaine qui représentait les intérêts d'un gouvernement étranger dans les litiges commerciaux avec les Etats-Unis[56], ainsi que les préparatifs d'autres pays en vue du Sommet sur le climat de Copenhague, y compris ceux du pays hôte, le Danemark[57]. La NSA a également procédé à la surveillance ciblée des Nations Unies, de l'Union européenne et d'autres organisations internationales de diverses manières, notamment en interceptant les communications téléphoniques et les faxes des ambassades, en copiant les disques durs et en surveillant le réseau câblé informatique interne utilisé par les agents[58]. Pour donner quelques exemples des nombreux cas révélés, précisons que la NSA a recueilli à l'occasion de l'opération Blackfoot les données des services diplomatiques français présents au siège des Nations Unies à New York[59]. L'opération Perdido a ciblé les bureaux de l'Union européenne à New York et à Washington, tandis que le système mis en place par la NSA sous le nom de code Powell a permis la surveillance des bureaux de la représentation grecque auprès des Nations Unies à New York. Le document interne de la NSA indique que cet espionnage a eu une influence déterminante sur «la tactique de négociation des Etats-Unis aux Nations Unies» dans le cadre de la guerre en Irak. Grâce aux conversations interceptées, la NSA aurait été en mesure d'informer le Département d'Etat américain et l'ambassadeur américain auprès des Nations Unies avec un degré de certitude élevé que la majorité requise était acquise avant le vote sur la résolution correspondante des Nations Unies[60]. Alors qu'on pouvait s'attendre à ce que cette surveillance vise les adversaires idéologiques classiques des Etats-Unis et les pays sensibles du Moyen-Orient et qu'elle était plus facile à justifier dans le cadre de la lutte contre le terrorisme, le fait qu'elle ait inclus des alliés traditionnels discrédite la thèse d'une surveillance visant à protéger la sécurité nationale.

53. *Le Monde*, 8 mai 2014, «Révélations sur les écoutes sous-marines de la NSA».
54. *Der Spiegel*, 17 novembre 2013, «'Royal Concierge': GCHQ Monitors Diplomats' Hotel Bookings».
55. *The Guardian*, 30 juin 2013, «New NSA leaks show how US is bugging its European allies».
56. *The New York Times*, 15 février 2014, «Spying by N.S.A. Ally Entangled in Law Firm».
57. *The Guardian*, 30 janvier 2014, «Snowden revelations of NSA spying on Copenhagen climate talks spark anger».
58. *The Guardian*, 30 juin 2014, «New NSA leaks show how US is bugging its European allies».
59. *Der Spiegel*, 1er septembre 2013, «'Success Story': NSA Targeted French Foreign Ministry».
60. *Der Spiegel*, 26 août 2013, «Codename 'Apalachee': How America Spies on Europe and the UN».

2.4.2. Des opérations de propagande flagrantes

58. Les révélations ont par ailleurs montré que les Etats-Unis et le Royaume-Uni recourraient à des opérations de propagande pour appuyer leurs desseins. L'Agence américaine de développement international (Agency for International Development) a utilisé un programme secret, baptisé ZunZuneo, pour recueillir des données à caractère privé des utilisateurs cubains d'internet, afin de les manipuler et de fomenter une dissidence contre le Gouvernement cubain[61].

59. D'autres révélations ont permis de constater que le Royaume-Uni avait pris des mesures similaires choquantes sans rapport avec le terrorisme ou des menaces sur la sécurité nationale. Les documents divulgués montrent que les services britanniques ont publié de faux documents sur internet pour porter atteinte à la réputation des personnes et des sociétés ciblées, tout en cherchant à manipuler le discours et le militantisme en ligne pour obtenir les résultats qu'ils jugeaient souhaitables. Ils ont procédé à des opérations de fausses attributions de documents (en publiant des documents en ligne faussement attribués à quelqu'un d'autre) et ont posté de faux commentaires sur des blogs, en prétendant être la victime de la personne dont ils cherchaient à salir la réputation[62]. *The Intercept* a également révélé que le GCHQ avait mis au point de nombreux instruments de couverture en vue de manipuler et de déformer le discours politique en ligne et de diffuser une propagande d'Etat. Parmi ces instruments figuraient des programmes destinés à manipuler les résultats de sondages en ligne, à gonfler artificiellement les chiffres du nombre de visiteurs de certains sites web, à «amplifier» les messages approuvés sur YouTube, à censurer les messages vidéo jugés «extrémistes», à surveiller l'utilisation du site d'enchères britannique eBay et même à connecter ensemble deux téléphones placés sur écoute au cours d'un appel[63].

60. Il ne fait aucun doute que ces techniques de manipulation représentent une grave menace pour l'Etat de droit, car elles permettent la fabrication de toute pièce d'éléments de preuve dans les affaires pénales, par exemple à l'encontre de journalistes ou de militants des droits de l'homme accusés de complicité d'activités terroristes[64]. Parallèlement, l'existence de ces manipulations rend plus difficile, sinon impossible, l'utilisation de véritables preuves numériques devant les tribunaux à l'encontre de vrais criminels.

2.4.3. L'absence de responsabilité interne au sein des agences de renseignement

61. Dans une interview parue dans *The Guardian* en juillet 2014, M. Snowden a indiqué que les atteintes à la vie privée commises par les agents de la NSA qui avaient accès à des communications privées interceptées étaient «assez habituelles»[65]:

> *«L'agence a recruté de jeunes types de 18 à 22 ans. Ils se voient subitement confier des fonctions assorties de responsabilités extraordinaires, qui leur permettent d'avoir accès à l'ensemble des enregistrements de vos données à caractère privé. Au cours de leur travail quotidien, ils tombent sur des éléments sans le moindre rapport avec leur activité, par exemple la photo intime d'une personne nue dans une situation sexuellement compromettante, mais extrêmement attirante. Qu'en font-ils? Ils font pivoter leur fauteuil et montrent cette photo à leur collègue, qui s'extasie: "C'est génial, envoie ça à Bill". Bill l'envoie alors à Georges, qui l'envoie à Tom et tôt ou tard, la vie de cette personne sera connue de tous ces employés.»*[66]

62. Une accusation similaire a été lancée en 2008, lorsqu'on a fait état de l'échange, entre les agents de la NSA au sein même de l'agence, de communications téléphoniques à caractère sexuellement explicite qu'ils avaient interceptées[67]; mais ces abus n'ont pour une bonne part pas été détectés ni signalés en raison de la faiblesse des contrôles internes. Selon certaines sources, des agents de la NSA utilisent les techniques de surveillance de l'agence pour mettre le nez dans des histoires sentimentales, «une pratique suffisamment répandue pour se voir affublée d'un nom de code aux accents d'espionnage: LOVEINT»[68].

---

61. *The Guardian*, 3 avril 2014, «US secretly created 'Cuban Twitter' to stir unrest and undermine government».
62. *The Intercept*, 24 février 2014, «How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations».
63. *The Intercept*, 14 juillet 2014, «Hacking Online Polls and Other Ways British Spies Seek to Control the Internet».
64. Il ne s'agit en aucun cas d'un risque hypothétique. Dans plusieurs actions en justice récemment engagées à l'encontre de journalistes en Turquie, les avocats affirment que de faux courriers électroniques ont été insérés dans l'ordinateur de leurs clients par les autorités (voir par exemple Dexter Filkins, Showtrials on the Bosphorus, *The New Yorker*, 13 août 2013.
65. *The Guardian*, 17 juillet 2014, «Edward Snowden urges professionals to encrypt client communications».
66. *The Washington Post*, 17 juillet 2014, «Snowden: NSA employees share sexts».
67. ABC News, 9 octobre 2008, «Exclusive: Inside Account of U.S. Eavesdropping on Americans».
68. *The Washington Post*, *ibid*. (note 66).

2.5. La mise en place de «trappes», le décryptage et l'envoi de logiciels malveillants: comment la NSA et ses partenaires compromettent le respect de la vie privée et la sécurité sur internet

63. La quasi-totalité des communications en ligne sont cryptées d'une manière ou d'une autre pour protéger nos vies privées, nos communications et nos comptes bancaires contre les cyberattaques, le vol ou des voisins trop curieux. La NSA reconnaît ouvertement qu'il est primordial pour elle de neutraliser le cryptage utilisé par ses adversaires. Mais pour ce faire, l'agence recourt à des méthodes dont les conséquences contreproductives donnent lieu aux mises en garde des experts, car elles compromettent la sécurité en ligne et rendent les utilisateurs vulnérables aux intrusions dans leur vie privée et leurs données à caractère personnel. La NSA utilise divers moyens: elle s'assure la maîtrise des normes internationales de cryptage, recourt à la technique de la «force brute» en confiant des missions de décryptage à de super-ordinateurs et collabore avec des sociétés expertes en technologie et des fournisseurs de services internet qui mettent à sa disposition les «trappes», c'est-à-dire les failles secrètes du système, ce qui lui permet de contourner les logiciels de cryptage commerciaux.

64. La NSA a rémunéré des sociétés pour qu'elles définissent délibérément des normes de cryptage plus fragiles comme choix par défaut des logiciels de sécurité de leurs clients. Grâce à «l'interdiction de la chaîne logistique», l'agence a pu intercepter des produits américains, comme les routeurs et les serveurs fabriqués par des sociétés américaines telles que Cisco, et y implanter des balises avant de les reconditionner et de les expédier aux consommateurs dans le monde entier sans qu'ils en soient informés.

65. Selon un document budgétaire des services de renseignement divulgué par M. Snowden, la NSA consacre plus de $US 250 millions par an à son programme «Sigint Enabling Project»[69] visant à saboter les protocoles de sécurité et leur application.

66. La NSA a par ailleurs fortement accéléré le recours aux opérations de piratage qu'elle n'avait cessé de critiquer lorsque les Etats-Unis en étaient la cible. Grâce aux logiciels «malveillants», l'agence peut maîtriser totalement un ordinateur infecté, ce qui permet à ses agents de prendre le contrôle du microphone de l'ordinateur ciblé et d'enregistrer les conversations à proximité de l'appareil, de prendre secrètement le contrôle de la webcam de l'ordinateur pour réaliser des clichés ou d'enregistrer l'historique de la consultation d'internet et de recueillir des précisions sur les connexions et les mots de passe utilisés pour accéder aux sites Web et aux boîtes aux lettres électroniques. La NSA a également informatisé des processus de diffusion à grande échelle de ces logiciels malveillants et a partagé avec les membres de l'alliance Five Eyes un grand nombre de ses fichiers consacrés à l'utilisation des logiciels implantés. Le système TURBINE, par exemple, qui assure l'exécution des logiciels malveillants automatisés qui ont été implantés, a été utilisé avec l'aide d'autres gouvernements qui en étaient informés et qui ont parfois participé à des attaques de logiciels malveillants. Le GCHQ a joué un rôle particulièrement important dans la mise au point de tactiques d'utilisation des logiciels malveillants: il gérait le centre de surveillance par satellite de Menwith Hill (la plate-forme européenne de la NSA située dans le nord du Yorkshire) et a lui-même appliqué certaines de ces tactiques, par exemple, selon certaines sources, en piratant les ordinateurs des ingénieurs de réseau de Belgacom, opérateur belge des télécommunications, qui compte parmi ses clients plusieurs institutions de l'Union européenne[70]. De nouvelles révélations faites par *The Intercept* le 4 décembre 2014 à partir des fichiers Snowden montrent qu'à l'occasion d'une opération répondant au nom de code «AURORAGOLD», la NSA a piraté les réseaux des opérateurs de téléphonie mobile du monde entier[71]. Un autre programme de logiciel espion, apparemment mis au point conjointement par la NSA et le GCHQ, a été dénommé «REGIN» lorsqu'il a été découvert par des entreprises spécialisées dans la sécurité sur internet, qui seraient parvenues à mettre au point des moyens de contrer ce système[72].

67. Le programme phare de surveillance planétaire d'internet semble être «TREASUREMAP», mis au point conjointement par la NSA et le GCHQ, dont l'existence a été révélée en septembre 2014[73] grâce aux documents divulgués par M. Snowden. Il s'agit d'une vaste campagne lancée par la NSA pour procéder à une cartographie mondiale d'internet, en cherchant à recenser et à localiser chaque appareil (ordinateur, tablette, smartphone) connecté à internet quelque part dans le monde – «partout, en permanence» selon les termes des documents de la NSA divulgués. Des cartes extraites de TREASUREMAP montrent que les agences ont

---

69. ProPublica, 5 septembre 2013, «Revealed: the NSA's Secret Campaign to Crack, Undermine Internet Security».
70. Voir par exemple *SPIEGELonline* (édition en anglais), 11 novembre 2013, GCHQ targets engineers with fax LinkedIn pages.
71. *The Intercept*, «Operation Auroragold – How the NSA Hacks Cellphone Networks Worldwide«.
72. Une description du fonctionnement du «super-cheval de Troie» Regin est donnée par C. Stöcker et M. Rosenbach, «Super-Trojaner Regin ist eine NSA-Geheimwaffe», *SPIEGELonline*, 25 novembre 2014.
73. Certains éléments de Treasure Map ont été dévoilés en novembre 2013 par le *New York Times* («NSA Report outlined Goals for More Power»).

pénétré les systèmes informatiques de sociétés privées de gestion de satellites, comme la société Stellar établie en Allemagne. Ces atteintes à la sécurité peuvent avoir d'énormes conséquences, notamment la capacité de priver d'internet des pays entiers[74].

68. La mise en place de trappes, l'implantation de logiciels malveillants et l'affaiblissement délibéré des systèmes de cryptage entraînent l'apparition de nouvelles failles dans les systèmes ciblés; or, celles-ci peuvent être découvertes et exploitées par des tiers qui ne sont pas animés de bonnes intentions. Les ordinateurs et les informations de leurs utilisateurs ainsi visés se retrouvent sans défense, non seulement face à la surveillance des pouvoirs publics, mais également face aux autres pirates, malfaiteurs ou dangers dont les utilisateurs sont censés être protégés par les systèmes de cryptage. Je suis par conséquent quelque peu surpris que le responsable du Centre européen de lutte contre la cybercriminalité d'Europol[75] ait demandé que le cryptage soit autorisé à la seule condition que des trappes soient installées au profit de ses services[76].

69. En outre, ces programmes ne sont pas seulement utilisés contre les individus qui représentent une menace pour la sécurité nationale ou pour les personnes que la NSA considère comme des «extrémistes». Parmi les cibles visées figuraient des administrateurs de systèmes informatiques qui travaillaient pour le compte de fournisseurs étrangers de services téléphoniques et internet, alors qu'aucun d'eux n'avait un lien avec des activités terroristes ou d'autres activités criminelles. Ils ont simplement été ciblés parce que le piratage de l'ordinateur d'un administrateur permettait à la NSA d'accéder secrètement aux communications traitées par la société de l'administrateur concerné. Enfin, la NSA a répété à plusieurs reprises que M. Snowden n'avait pas pu avoir accès aux données brutes collectées dans le cadre des activités de surveillance de l'agence. Pourtant, l'agence elle-même s'est révélée incapable de protéger les données extrêmement sensibles qu'elle avait recueillies[77]. Que se serait-il passé si Edward Snowden avait été un terroriste? Que se passerait-il si ces données tombaient aux mains d'un régime totalitaire? La fragilisation délibérée du cryptage et des autres normes de sécurité d'internet par la NSA et ses alliés pour faciliter les opérations de surveillance massive présente un grave danger pour la sécurité nationale. Ces failles peuvent en effet être décelées et exploitées par des Etats voyous, des terroristes, des cyberterroristes, voire des délinquants de droit commun, et mêmes des chercheurs indépendants qui ont découvert de telles faiblesses et publié leurs exploits en guise de mise en garde. Ils peuvent tous tirer parti des dispositifs mis en place par les personnes chargées d'assurer notre sécurité pour causer des dommages considérables à nos sociétés.

2.6. Les réactions législatives, judiciaires et politiques aux Etats-Unis et au Royaume-Uni à la suite des révélations d'Edward Snowden

70. A la suite des révélations d'Edward Snowden, le Gouvernement américain a réexaminé ses pratiques de surveillance et leur a apporté quelques modifications. En janvier 2014, la Commission de surveillance du respect de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board)[78] a critiqué les programmes d'enregistrement des communications téléphoniques appliqués au titre de l'article 215 de la loi «USA PATRIOT» («loi visant à l'unité et au renforcement des Etats-Unis par la fourniture des outils adéquats indispensables pour déceler et réprimer le terrorisme») et le fonctionnement de la Foreign Intelligence Surveillance Court (FISC – juridiction de contrôle des services de renseignement extérieur). Elle a conclu que la collecte en vrac d'enregistrements de conversations téléphoniques n'avait présenté qu'un intérêt «minime» pour la lutte contre le terrorisme[79], qu'elle était illégale et qu'elle devait prendre fin. La Commission n'a constaté «aucun exemple de situation dans laquelle le programme a directement contribué à découvrir un

---

74. Pour une description détaillée de Treasure Map et de ses implications, voir Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer et Christian Grothoff, «Map of the Stars, the NSA and GCHQ campaign against German Satellite Companies», *The Intercept*, 14 septembre 2014.

75. https://www.europol.europa.eu/ec3.

76. *SPIEGELonline*, 13 octobre 2014, «Cybercrime – Europäische Internetpolizei fordert Hintertüren»; ironie du sort, un virus malveillant baptisé «European Cybercrime Centre» utilisé à des fins d'extorsion de fonds exige le versement «d'amendes» élevées pour obtenir le déblocage de l'ordinateur infecté par le virus (voir par exemple http://pcviruskiller.blogspot.fr/2013/07/removing-european-cybercrime-centre.html).

77. *The Atlantic*, 7 juillet 2014, «The Latest Snowden Leak Is Devastating to NSA Defenders».

78. Une instance bipartite du pouvoir exécutif américain, chargée notamment de passer en revue les mesures de lutte contre le terrorisme prises par l'exécutif, afin de vérifier qu'elles sont conformes aux exigences de respect de la vie privée et des libertés civiles.

79. Cette conclusion formulée par une instance de contrôle officielle des Etats-Unis a été confirmée par une étude approfondie réalisée sous les auspices de l'Union européenne (SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act, FP7-SEC-2011-284725), publiée le 29 mai 2014. Cette étude, dont les auteurs sont entre autres Martin Scheinin et Douwe Korff, conclut que, par rapport aux techniques classiques de surveillance, les opérations de surveillance massive d'internet sont d'une maigre utilité pour les enquêtes menées dans le cadre de la lutte contre le

complot terroriste inconnu auparavant ou à déjouer un attentat terroriste»[80]. Dans son premier rapport, la Commission a également recommandé au gouvernement de restreindre l'accès des analystes aux enregistrements des communications téléphoniques aux personnes en contact avec une personne liée à un suspect, c'est-à-dire dans la limite de deux contacts en cascade (au lieu de trois actuellement), de créer un groupe d'experts composé de juristes externes, chargé d'assurer la défense des intérêts des citoyens dans les principales affaires portant sur les programmes secrets de surveillance et de veiller à la suppression plus rapide des données. Le Président Obama a finalement décidé, dans son instruction présidentielle générale du 17 janvier 2014[81] de cesser la collecte administrative en vrac des données téléphoniques et a soumis l'accès de la NSA aux données dorénavant collectées par les sociétés de téléphonie à l'obtention d'un mandat délivré par la FISC[82]. Il a également interdit la mise sur écoute des dirigeants des pays alliés, sauf lorsque la sécurité nationale le commande. Mais la question de l'opportunité d'un espionnage des autres hauts responsables de ces pays n'a pas été abordée. Enfin, l'examen minutieux des appels téléphoniques a été limité à deux contacts en cascade associés à un numéro de téléphone en rapport avec une personne soupçonnée d'activités terroristes. Le Président Obama n'a pas donné suite à certaines recommandations de plus ample portée préconisées par sa commission consultative en matière de surveillance (par exemple l'exigence de l'approbation par un juge des lettres de sécurité nationale, une sorte de réquisition permettant au FBI d'obtenir des informations relatives à certaines personnes auprès de leur banque, de leur opérateur de téléphone portable et d'autres entreprises)[83].

71. En revanche, en juillet 2014, le deuxième rapport de la Commission de surveillance du respect de la vie privée et des libertés civiles a reconnu le bien-fondé des programmes de surveillance d'internet mis en place par la NSA en vertu de l'article 702 de la loi relative à la surveillance des services de renseignement extérieur. Le programme PRISM, dans le cadre duquel la NSA collecte des données de renseignement extérieur auprès de Google, Facebook, Microsoft, Apple et la quasi-totalité des autres grandes entreprises américaines de technologie, tombe en effet sous le coup de l'article 702. Selon la Commission, cet article a permis au gouvernement de «réunir un plus large éventail de données de renseignement extérieur qu'il ne lui aurait été possible d'en obtenir – aussi rapidement et aussi efficacement – sans cette disposition» à des fins telles que la recherche de la prolifération nucléaire et la surveillance des réseaux terroristes dans le but de comprendre leur mode de fonctionnement[84]. La Commission conclut dans son rapport que, par certains aspects, ces programmes «sont à la limite du raisonnable sur le plan constitutionnel» en raison de «l'étendue imprécise, qui peut être considérable, de la collecte fortuite des communications des ressortissants américains» et présente quelques propositions politiques destinées à rendre les programmes plus «rassurants dans le domaine du raisonnable»[85].

72. En juillet 2014, la commission du renseignement du Sénat a adopté une nouvelle proposition de loi sur la cybersécurité, intitulée loi relative à la mise en commun des informations en matière de cybersécurité (Cybersecurity Information Sharing Act – CISA), à laquelle les détracteurs de la NSA ont reproché d'étendre davantage l'accès de l'agence aux données relatives aux ressortissants américains[86]. Si ce texte est adopté par le Sénat, les services de l'administration seront autorisés à conserver et à mettre en commun leurs données «à des fins de cybersécurité» et les entreprises privées pourront partager leurs informations relatives aux cyberattaques «en temps réel» et seront par ailleurs protégées contre les actions en justice intentées par des particuliers pour le partage de leurs données avec d'autres entreprises et l'administration américaine[87].

---

terrorisme: «Les techniques de surveillance d'Internet, à l'exception de l'analyse ciblée des réseaux sociaux, représentent, d'une part, une ingérence inadmissible dans les droits fondamentaux au respect de la vie privée et à la protection des données, d'autre part, le pire risque, du point de vue éthique, d'effet dissuasif et de perte de confiance et, enfin, une intrusion et une discrimination, tout en portant atteinte aux normes morales de la proportionnalité des moyens et du consentement des personnes soumises à cette surveillance. En attendant, ces dégâts importants sur le plan moral et juridique sont pour l'essentiel moyennement, voire peu utiles, puisqu'ils produisent des résultats très inférieurs en matière de coûts, d'efficacité et de respect de la vie privée dès la conception d'un programme que d'autres solutions techniques de moindre envergure. Les arguments en faveur du recours à un système de surveillance massive d'internet sont faibles» (p. 50).

80. *The New York Times*, 23 janvier 2014, «Watchdog report says N.S.A. Program is Illegal and Should End».
81. PPD28: www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.
82. *The New York Times*, 30 juin 2014, «Sky Isn't Falling After Leaks by Snowden».
83. *The New York Times*, 17 janvier 2014, «Obama Outlines Calibrated Curbs on Phone Spying».
84. *The New York Times*, 2 juillet 2014, «U.S. Privacy Panel Backs N.S.A.'s Internet Tapping».
85. *Ibid*.
86. *The Guardian*, 12 juillet 2014, «The Senate is giving more power to the NSA, in secret. Everyone should fight it».
87. Le Président Obama a menacé de faire usage de son droit de veto contre une proposition similaire (CISPA) en 2013 et son administration a indiqué que le projet CISA devait être renforcé sur le plan de la protection de la vie privée pour obtenir le soutien du Président; www.bankinfosecurity.com/white-house-hasnt-backed-cisa-a-7126.

73. Une tentative législative visant à contenir quelque peu la NSA – la proposition de loi relative aux libertés (USA Freedom Act) déposée en 2013 pour mettre fin à la collecte des données téléphoniques des ressortissants américains par la NSA – a échoué devant le Sénat américain en novembre 2014. Cette proposition avait reçu le soutien du Président, des principaux membres du Congrès des deux partis et, mais avec davantage de réticences, de la plupart des groupes de défense des libertés civiles et de la NSA. Le Sénat y a fait obstacle à la suite de critiques qui présentaient ce texte comme un «cadeau fait aux terroristes»; la proposition de loi n'est pas non plus parvenue à obtenir le soutien des défenseurs des libertés civiles (y compris des donneurs d'alerte de la NSA Thomas Drake et Bill Binney), qui craignaient que le libellé du texte soit si imprécis qu'il permette par mégarde à la NSA d'étendre son emprise, compte tenu de l'interprétation extensive des dispositions légales à laquelle la NSA avait déjà procédé par le passé, alors que celles-ci visaient à restreindre ses pouvoirs[88]. Le dernier espoir des défenseurs des libertés civiles réside dans le fait que l'article 215 de la loi «USA Patriot», sur lequel repose une bonne partie de la collecte des métadonnées, ne sera plus en vigueur à compter de juin 2015, ce qui donnera lieu à de nouveaux débats[89].

74. Au Royaume-Uni, en juillet 2014, le gouvernement a fait adopter par la Chambre des communes une loi d'urgence controversée, qui a franchi en un seul jour toutes les étapes de la procédure législative, afin de pouvoir continuer à contraindre les entreprises de services de communications et d'internet à conserver les données relatives à l'utilisation et la géolocalisation de leurs clients pendant une durée maximale d'un an, ainsi qu'à les transmettre aux services répressifs à leur demande. Le gouvernement affirmait que cette législation était indispensable à la protection de la sécurité nationale, compte tenu des événements survenus en Irak et en Syrie. Cette adoption dans l'urgence faisait également suite à la décision rendue par la Cour de justice de l'Union européenne (CJUE) en avril 2014[90], qui avait conclu au caractère disproportionné, au regard du droit au respect de la vie privée des citoyens, de la directive de l'Union européenne sur la conservation des données des communications, qui imposait aux prestataires de services de communications de conserver les données de communication et de géolocalisation (mais pas les contenus) de leurs clients pendant une période maximale de deux ans. Le nouveau texte de loi met également en place des dispositifs de contrôle, notamment une Commission de surveillance du respect de la vie privée et des libertés civiles, et impose au gouvernement la publication annuelle de «rapports sur la transparence». La Commissaire aux droits de l'homme des Nations Unies, Navi Pillay, a critiqué le recours à une procédure simplifiée pour l'adoption du projet de loi d'urgence sur la surveillance et a fait écho aux inquiétudes des groupes de défenses des libertés civiles, qui redoutaient que la procédure accélérée ne permette pas d'aborder les préoccupations soulevées par la CJUE lorsqu'elle a annulé la directive de l'Union européenne[91].

75. La contestation en justice des activités de surveillance du GCHQ devant le tribunal des pouvoirs d'investigation (Investigatory Powers Tribunal – IPT) par Amnesty International, l'American Civil Liberties Union, Privacy International and Liberty, entre autres, a viré à la «pure farce», selon les termes d'Amnesty International[92]. Au cours de la procédure, le gouvernement a insisté sur le fait qu'il ne confirmerait ni ne nierait aucune de ses activités de surveillance[93], ce qui illustre la difficulté de la contestation en justice des programmes secrets de surveillance de l'administration. Dans sa décision du 5 décembre 2014[94], l'IPT a rejeté la demande qui lui était faite, notamment à propos du programme TEMPORA révélé par M. Snowden, en concluant que ce programme, pour autant qu'il existe, était conforme à la législation. La partie demanderesse a annoncé son intention de porter l'affaire devant la Cour européenne des droits de l'homme.

76. En revanche, les juridictions constitutionnelles d'Allemagne, d'Autriche, de Bulgarie, de Chypre, de République tchèque, de Roumanie et de Slovénie, à l'instar de la CJUE, ont toutes conclu au caractère inconstitutionnel de la conservation générale des données[95].

---

88. Spencer Ackermann, «Senate Republicans block landmark NSA surveillance reform bill», *The Guardian*, 19 novembre 2014.
89. Sebastian Fischer, Republikaner stoppen NSA-Reform, *SPIEGELonline*, 19 novembre 2014.
90. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf.
91. *The Guardian*, 15 juillet 2014, «UN commissioner criticizes decision to fast-track emergency surveillance bill».
92. Amnesty International, 18 juillet 2014, «UK hearing on mass government surveillance wraps up after "farcical" week».
93. BBC News, 14 juillet 2014, «Tribunal hearing legal challenge over GCHQ surveillance claims».
94. https://www.privacyinternational.org/temporaipt.pdf.
95. BBC News (note 93).

77. En Allemagne, le *Bundestag* a créé une commission d'enquête sur l'affaire de la NSA le 20 mars 2014[96]. Les travaux de la commission étant toujours en cours, j'aimerais me limiter aux quelques observations suivantes, qui reposent sur des informations publiquement disponibles:

i. Je tiens tout d'abord à féliciter le Bundestag d'avoir constitué cette commission d'enquête. Je n'ai pas connaissance d'un autre parlement d'un Etat membre du Conseil de l'Europe qui ait pris une mesure similaire.

ii. Deuxièmement, je trouve un peu inquiétant que les parlementaires aient accepté trop rapidement, comme cela avait déjà été le cas par le passé, la tactique employée par l'exécutif, qui consiste à refuser de fournir des informations à la commission au motif qu'elles doivent rester secrètes pour des raisons de sécurité nationale. Dans son rapport sur «Les recours abusifs au secret d'Etat et à la sécurité nationale: obstacles au contrôle parlementaire et judiciaire des violations des droits de l'homme»[97], notre collègue Dick Marty avait déjà fait une remarque similaire à propos de la commission d'enquête sur le rôle joué par le BND dans le programme de restitutions de la CIA. L'arrêt rendu par la Cour constitutionnelle fédérale allemande[98] à la demande de membres de l'opposition a précisé l'étendue du droit à l'information du parlement dans un esprit d'ouverture, en soulignant que la protection de la sécurité d'Etat n'était pas un monopole de l'exécutif, mais une prérogative qu'il partageait avec le parlement. Cet arrêt a été rendu trop tard pour la commission d'enquête sur le BND/CIA, mais la commission d'enquête sur la NSA pourrait se fonder sur cette décision pour affirmer de manière plus énergique son droit à l'information.

iii. Troisièmement, je regrette que la commission ne soit pas parvenue à s'entendre sur l'invitation de M. Snowden à Berlin. Il est clair qu'il s'agit d'un témoin important et on peut douter de sa capacité à s'exprimer librement à Moscou[99].

3. Les répercussions des opérations de surveillance massive sur les droits de l'homme

78. Les révélations de M. Snowden soulèvent inévitablement la question des répercussions sur les droits de l'homme de la collecte à grande échelle des données à caractère privé. L'ancien chef du BND, Hansjörg Geiger, a bien résumé la situation devant notre commission: «Pour parler sans détour, la surveillance massive et sans entrave des données par les services de renseignement est tout simplement incompatible avec la protection des droits de l'homme»[100]. De la même manière, le Commissaire aux droits de l'homme du Conseil de l'Europe a déclaré que «la conservation en masse et sans suspicion de données de communication est fondamentalement contraire à la prééminence du droit, incompatible avec les principes fondamentaux de protection des données et inefficace»[101].

3.1. Le droit au respect de la vie privée

3.1.1. Les normes du Conseil de l'Europe

79. Les opérations de surveillance massive constituent a priori une atteinte à l'article 8 de la Convention européenne des droits de l'homme (STE n° 5, «la Convention»), qui lie l'ensemble des Etats membres du Conseil de l'Europe. La Cour européenne des droits de l'homme («la Cour») s'est prononcée sur une série d'affaires relatives à la protection des données et à la surveillance, et notamment sur des requêtes qui concernaient l'interception des communications[102], diverses formes de surveillance[103] et la protection contre la conservation des données à caractère personnel par les pouvoirs publics[104].

---

96. www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss.
97. Doc. 12714, paragraphe 32.
98. Décision du 17 juin 2009 (2 BvE 3/07), disponible (en allemand) sur: www.bundesverfassungsgericht.de/entscheidungen/es20090617_2bve000307.html.
99. Les membres de l'opposition ont saisi la Cour constitutionnelle fédérale d'une demande d'annulation du refus de la majorité d'inviter M. Snowden à témoigner à Berlin. La Cour a rejeté cette demande pour vice de forme: en vertu de la législation qui régit les travaux des commissions d'enquête, c'est la Cour suprême fédérale (de Leipzig), et non la Cour constitutionnelle fédérale (de Karlsruhe) qui est compétente en l'espèce, puisque l'affaire concerne «uniquement» les modalités de la mise en œuvre d'une décision de procéder à l'audition d'un témoin.
100. Témoignage de M. Geiger devant la commission du 8 avril 2014.
101. «La prééminence du droit sur l'internet» (note 10), recommandation II.6 (p. 22).
102. *Malone c. Royaume-Uni* (Requête n° 8691/79, arrêt du 2 août 1984).
103. *Klass et autres c. Allemagne* (Requête n° 5029/71, arrêt du 6 septembre 1978).
104. *Leander c. Suède* (Requête n° 9248/81, arrêt du 26 mars 1987), *S. et Marper c. Royaume-Uni* (Requêtes nos 30562 et 30566/04, arrêt du 4 décembre 2008).

80. L'article 8.1 («Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance») affirme le droit au respect de la vie privée, qui est également consacré par d'autres conventions relatives aux droits de l'homme, comme l'article 12 de la Déclaration universelle des droits de l'homme et l'article 17 du Pacte international relatif aux droits civils et politiques[105]. Les communications interceptées et conservées dans le cadre de programmes de surveillance massive sans le consentement des personnes visées entrent bien évidemment dans le champ d'application de la «correspondance» et de la «vie privée» de l'article 8[106]. Même lorsque l'ingérence concerne des informations tombées dans le domaine public, la Cour a conclu dans les affaires *Segerstedt-Wiberg et autres c. Suède*[107] et *Rotaru c. Roumanie*[108], puis réaffirmé dans l'affaire *Shimovolos c. Russie*[109] que «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»[110]. Selon la Cour, «le terme vie privé a un sens très large, qui n'est pas susceptible de faire l'objet d'une définition exhaustive» et peut englober des activités à caractère professionnel ou commercial[111]. Comme la protection des données à caractère personnel revêt une importance capitale pour le droit au respect de la vie privée d'une personne, la Cour a constamment conclu que «la collecte et la conservation systématiques des données relatives à une personne précise par les services de sécurité constitue une ingérence dans la vie privée de cette personne, même si ces données sont collectées dans un lieu public ou concernent exclusivement les activités professionnelles ou publiques de l'intéressé»[112].

81. L'article 8.2 prévoit quelques exceptions limitées, pour lesquelles la Cour a énoncé une série de principes que les gouvernements doivent respecter lorsqu'ils prennent des mesures qui ont une incidence sur la vie privée des citoyens, garantie par l'article 8.1. Deux conditions doivent être réunies, qui sont précisées ci-dessous.

82. La première condition est que cette ingérence soit conforme à la loi. La loi doit être accessible aux justiciables et l'intéressé doit pouvoir prévoir les conséquences qu'elle aura pour lui; autrement dit, la loi doit être formulée de façon suffisamment claire et précise pour indiquer de manière adéquate aux citoyens les conditions et les situations dans lesquelles les autorités ont le droit de porter atteinte au droit au respect de la vie privée. La loi doit prévoir un minimum de garanties pour l'exercice du pouvoir d'appréciation des pouvoirs publics, c'est-à-dire comporter des dispositions suffisamment précises et claires sur la nature des infractions susceptibles de donner lieu à une ordonnance d'interception. Il importe que les autorités compétentes assurent une surveillance et un contrôle effectifs, afin de prévenir tout abus. La Cour souligne que «la «loi» irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ne connaissait pas de limites», surtout si l'on considère que le risque d'arbitraire se présente avec une netteté singulière lorsqu'il s'agit d'une forme de pouvoir que l'exécutif exerce en secret[113].

83. Dans les affaires *Khan c. Royaume-Uni*[114] et *PG. et J.H. c. Royaume-Uni*[115], la Cour européenne des droits de l'homme a conclu que les appareils d'écoute secrète installés par la police dans un domicile privé violaient l'article 8. Au moment des faits, ces mesures étaient uniquement régies par les lignes directrices du Home Office, qui n'étaient ni juridiquement contraignantes ni directement accessibles par les citoyens. De même, dans l'affaire *Copland c. Royaume-Uni*, la Cour a estimé que l'utilisation d'appareils d'écoute secrète

---

105. Le PIRDCP interdit toute ingérence arbitraire ou illégale dans la vie privée ou la correspondance d'une personne; il impose à chaque Etat partie l'obligation positive de créer un cadre juridique assurant la protection effective du droit au respect de la vie privée contre toute ingérence ou atteinte, que cette ingérence ou atteinte provienne ou non de l'Etat lui-même, d'Etats étrangers ou d'acteurs privés; il protège des domaines particuliers de la vie privée, comme le corps, la famille, le domicile et la correspondance d'une personne, et restreint la collecte, l'utilisation et l'échange de données à caractère personnel, que l'on qualifie bien souvent d'informations confidentielles.

106. «(…) les conversations téléphoniques (…) se trouvent comprises dans les notions de "vie privée" et de "correspondance", visées par [l'article 8]», *Klass et autres c. Allemagne*, Requête n° 5029/71, arrêt du 6 septembre 1978.

107. Requête n° 62332/00, arrêt du 6 septembre 2006.

108. Requête n° 28341/95, arrêt du 4 mai 2000 (Grande Chambre).

109. Requête n° 30194/09, arrêt du 28 novembre 2011.

110. *Rotaru c. Roumanie* (note 108 *supra*), paragraphe 43.

111. *Shimovolos c. Russie* (note 109 *supra*), paragraphe 64, à propos de *Niemietz c. Allemagne*, Requête n° 13710/88, arrêt du 16 décembre 1992, paragraphe 29, et *Halford c. Royaume-Uni*, Requête n° 20605/92, arrêt du 25 juin 1997, paragraphes 42-46.

112. *Shimovolos c. Russie* (note 109 *supra*), paragraphe 64; voir également *S. et Marper c. Royaume-Uni*, Requêtes n° 30562/04 et 30566/04, arrêt du 4 décembre 2008.

113. *Segerstedt-Wiberg et autres c. Suède*, Requête n° 62332/00, arrêt du 6 septembre 2006, paragraphe 76.

114. Requête n° 35394/97, arrêt du 4 octobre 2000.

115. Requête n° 44787/98, arrêt du 25 décembre 2001.

et la collecte et la conservation d'informations relatives à l'utilisation par la requérante de son téléphone, de ses courriers électroniques et d'internet n'étaient pas «prévues par la loi», dans la mesure où il n'existait aucune législation interne régissant cette surveillance au moment des faits[116].

84. Dans l'affaire *Kruslin c. France*, la Cour a conclu à la violation de l'article 8 par la mise sur écoute de lignes téléphoniques ordonnée par un juge d'instruction dans une affaire de meurtre, parce que le droit français n'indiquait pas suffisamment clairement l'étendue et le mode d'exercice du pouvoir discrétionnaire des autorités dans ce domaine[117]. Dans l'affaire *Amann c. Suisse*, la Cour a également conclu à la violation de l'article 8 en raison de l'interception, par le ministère public, d'un appel téléphonique reçu par le requérant, qui avait été passé depuis l'ancienne ambassade soviétique (pour commander un appareil dépilatoire pour lequel le requérant avait fait de la publicité), dans la mesure où le droit suisse ne précisait pas si les autorités avaient le pouvoir discrétionnaire de créer et de conserver des dossiers de renseignement dans la forme retenue pour le requérant[118]. La Cour a conclu à des violations similaires pour le manque de clarté des dispositions légales autorisant l'enregistrement systématique des conversations dans la salle des visites d'une prison à des fins autres que celles de la sécurité de l'établissement dans l'affaire *Wisse c. France*[119] et l'utilisation d'appareils d'enregistrement à l'encontre de personnes soupçonnées de meurtre dans l'affaire *Vetter c. France*[120]*.* Dans l'affaire *A. c. France*, la Cour a conclu à la violation de l'article 8 parce que l'enregistrement d'une personne privée dans le cadre d'une enquête préliminaire de police n'avait pas été effectué conformément à la procédure judiciaire et n'avait pas été ordonné par un juge d'instruction[121].

85. La deuxième condition requise pour qu'une ingérence corresponde à l'exception prévue à l'article 8.2 est que cette ingérence dans le droit au respect de la vie privée soit «nécessaire dans une société démocratique» pour poursuivre l'un des buts énoncés dans le deuxième alinéa (sécurité nationale, sûreté publique, bien-être économique, etc.). Dans l'affaire *Segerstedt-Wiberg et autres c. Suède*[122], les requérants s'étaient plaints de la conservation d'informations à leur sujet dans les dossiers de la police de sécurité de Suède et du refus de cette dernière de leur révéler l'étendue des informations conservées. La Cour a conclu en 2006 que, pour l'un des requérants, il était légitime que le gouvernement conserve des informations relatives aux menaces d'attentats à la bombe dont l'intéressé et certaines autres personnalités avaient fait l'objet, puisque cela se justifiait par l'objectif de prévention des troubles à l'ordre public ou des infractions pénales poursuivi par la police. En revanche, elle a estimé qu'il n'existait aucun but légitime pour les autres requérants, qui avaient été affiliés à certains partis politiques de gauche et au Parti communiste. L'un d'eux aurait préconisé de résister par la violence à la police lors de manifestations en 1969, tandis que les autres étaient membres du parti KPLM(r), qui professait la domination d'une classe sociale sur une autre en ne respectant pas la loi. Comme ces informations concernaient des faits anciens, la Cour a toutefois estimé que cette conservation ne pouvait avoir poursuivi un but légitime de sécurité nationale.

86. L'affaire *Klass et autres c. Allemagne*, bien qu'elle soit de 1978, montre précisément les différents avantages et risques des dispositifs de surveillance équivalents à ceux dont les fichiers de la NSA ont révélé l'existence. La Cour reconnaît que:

> *«Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'Etat doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales[123].»*

116. Requête n° 62617/00, arrêt du 3 avril 2007.
117. Requête n° 11801/85, arrêt du 24 avril 1990.
118. Requête n° 27798/95, arrêt du 16 février 2000.
119. Requête n° 71611/01, arrêt du 20 décembre 2005.
120. Requête n° 59842/00, arrêt du 31 mai 2005.
121. Requête n° 14838/89, arrêt du 23 novembre 1992.
122. Requête n° 62332/00, arrêt du 6 septembre 2006.
123. Requête n° 5029/71, arrêt du 6 septembre 1978, paragraphe 48.

87. Mais cette affaire met également l'accent sur le fait que les progrès techniques ont rendu l'espionnage et la surveillance plus complexes; la Cour souligne que, malgré la menace terroriste,

> *«les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée»*[124].

88. Les lignes directrices et les exigences énoncées dans l'affaire *Shimovolos c. Russie* donnent des indications sur les garanties légales que tous les Etats doivent prévoir pour protéger le respect de la vie privée au titre de l'article 8. Selon la Cour,

> *«le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'application de mesures secrètes de surveillance apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit user de termes assez clairs pour indiquer aux citoyens de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre des mesures secrètes de surveillance et de collecte des données. En outre, puisque l'application de mesures secrètes de surveillance des communications échappe au contrôle du public et le risque d'abus est inhérent à tout système de surveillance secrète, la loi doit prévoir les garanties minimales suivantes contre les abus de pouvoir: la nature, l'étendue et la durée des mesures éventuelles, les motifs requis pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours prévu par le droit interne»*[125].

89. Cette affaire est particulièrement emblématique des types d'opérations de surveillance massive dont il est question dans le présent rapport: le requérant, militant de la défense de droits de l'homme, figurait dans une base de données des services de sécurité à des fins de surveillance secrète, constituée en vertu d'un arrêté ministériel qui n'avait pas été publié et n'était pas accessible au public; ses déplacements avaient été par la suite surveillés, ce qui avait conduit à son arrestation. Les citoyens ne pouvaient donc pas savoir pour quelles raisons des personnes figuraient dans cette base de données, quel type d'informations elle comportait, pendant combien de temps, comment ces informations étaient conservées et utilisées ni qui en avait la maîtrise. Dans une autre affaire, *Association «21 décembre 1989» et autres c. Roumanie*[126], le président d'une association de défense des intérêts des participants et des victimes des événements de 1989 (la répression des manifestations antigouvernementales en Roumanie) avait fait l'objet de mesures de surveillance de la part des services secrets, principalement sous la forme d'une mise sur écoute de son téléphone. Les services de renseignement avaient réuni des informations à son sujet en 1990, qu'ils avaient conservé pendant 16 ans. La Cour a conclu à la violation de l'article 8.

90. L'appréciation par la Cour de la qualité de la loi et des garanties contre les abus des programmes de surveillance dépend des circonstances de chaque affaire, y compris «la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne»[127]. Dans l'affaire *Klass et autres c. Allemagne*, la Cour n'a pas conclu à la violation de l'article 8, car elle a jugé les mesures de surveillance en question nécessaires dans une société démocratique dans l'intérêt de la sécurité nationale et pour la défense de l'ordre ou la prévention des infractions pénales; elle a estimé que des garanties suffisantes assuraient le contrôle de ces mesures avant, pendant et après la surveillance. Elle a conclu que les instances de contrôle prévues par la loi étaient indépendantes des autorités qui effectuaient la surveillance et qu'elles étaient investies de compétences suffisantes pour pouvoir exercer un contrôle effectif et constant sur le processus de surveillance.

91. Par ailleurs, la Cour a également admis, dans l'affaire *Association «21 décembre 1989» et autres c. Roumanie*[128], qu'une personne pouvait, sous certaines conditions, se prétendre victime d'une violation en raison de la simple possibilité que des mesures secrètes soient prises sur le fondement d'une législation qui le permettait, sans avoir à démontrer que de telles mesures lui avaient été effectivement appliquées. En l'absence d'une telle faculté, l'article 8 pourrait «être réduit à néant». Une telle situation serait également contraire à l'article 13 de la Convention européenne des droits de l'homme, qui garantit que «toute personne

---

124. *Ibid*., paragraphe 49.
125. Requête n° 30194/09, arrêt du 28 novembre 2011, paragraphe 68.
126. Requêtes n^{os} 33810/07 et 18817/08, arrêt du 24 mai 2011.
127. *Klass et autres c. Allemagne,* Requête n° 5029/71, arrêt du 6 septembre 1978, paragraphe 50.
128. Requêtes n^{os} 33810/07 et 18817/08, arrêt du 24 mai 2011.

dont les droits et libertés reconnus dans la présente Convention ont été violés a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles».

92. L'affaire pendante *Big Brother Watch et autres c. Royaume-Uni* et d'autres affaires introduites après les révélations d'Edward Snowden[129] permettront de connaître la position de la Cour sur les programmes de surveillance massive du GCHQ[130]. Les requérants de l'affaire *Big Brother Watch* soutiennent qu'il est possible qu'ils aient fait l'objet d'une surveillance générale de la part des services de sécurité du Royaume-Uni, qui peuvent avoir reçu des données interceptées à l'étranger en rapport avec leurs communications électroniques. Ils prétendent que ces ingérences ne sont pas «prévues par la loi» comme l'exige l'article 8, car le droit interne ne prévoit pas la réception d'informations communiquées par les services de renseignement étrangers; la loi ne prévoit par ailleurs aucun contrôle ni garantie à propos des circonstances dans lesquelles les services de renseignement britanniques peuvent demander aux services de renseignement étrangers d'intercepter des communications et de leur permettre d'accéder aux données ainsi obtenues, ni à propos de l'éventuelle utilisation, analyse, diffusion, conservation et destruction des données demandées à des services de renseignement étrangers et/ou obtenues d'eux. Dans une autre affaire pendante depuis 2006, *Roman Zakharov c. Russie*[131], un éditeur russe fait grief de l'absence de garanties légales contre la surveillance des communications passées sur son téléphone portable. En vertu d'un décret d'application qui n'avait pas été publié, l'opérateur de son téléphone mobile avait installé un matériel permettant au Service fédéral de sécurité (FSB) d'intercepter toute communication téléphonique sans l'autorisation préalable d'un juge.

93. En attendant, la Cour de justice de l'Union européenne s'est penchée sur la question de la confidentialité des données et a conclu, dans l'affaire *Google Spain c. Gonzalez*[132], qu'un opérateur de moteur de recherche internet était responsable du traitement par ses soins des données à caractère personnel présentes sur les pages web publiées par des tiers. La Cour de justice a principalement reconnu aux citoyens le droit de demander la suppression de ces données à caractère personnel indexées.

94. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) accorde une protection supplémentaire pour tout traitement des données effectué par le secteur privé et le secteur public, y compris le traitement des données réalisé par les autorités judiciaires et autres autorités répressives. La convention définit les «données à caractère personnel» comme «toute information concernant une personne physique identifiée ou identifiable», ce qui englobe les communications interceptées par les programmes de surveillance de l'administration. En avril 2014, cette convention avait été ratifiée par l'ensemble des Etats membres de l'Union européenne; elle avait été modifiée en 1999 pour permettre l'adhésion de l'Union européenne. Il s'agit du seul instrument international juridiquement contraignant dans le domaine de la protection des données. La convention autorise même le traitement des données «sensibles», comme les informations relatives à l'origine raciale, aux opinions politiques, à la santé, aux convictions religieuses, à la vie sexuelle ou aux condamnations pénales d'une personne, sous réserve de l'existence de certaines garanties légales. La convention prévoit le libre flux des données entre les Etats Parties, mais impose également des restrictions aux flux en direction des Etats dans lesquels les dispositions légales ne prévoient pas de protection équivalente. La convention est actuellement en cours de modernisation. Je partage pleinement la recommandation du Commissaire aux droits de l'homme du Conseil de l'Europe, selon qui «la révision en cours de la Convention n° 108 ne devrait pas aboutir à un abaissement des niveaux d'exigence en matière de protection des données à l'échelle européenne ou mondiale. Bien au contraire, elle devrait permettre de préciser les règles et d'en renforcer l'application, en particulier en ce qui concerne (…) la surveillance à des fins de renseignement et de sécurité nationale»[133].

---

129. MTI-EcoNews/Hungary, 29 novembre 2013, «NGO to turn to Strasbourg court over security services' secret surveillance».
130. Requête n° 58170/13, affaire communiquée le 7 janvier 2014.
131. Requête n° 47143/06 (voir le communiqué de presse de la Cour européenne des droits de l'homme, qui présente un résumé des faits et de l'état actuel de la procédure, en annonçant l'audience orale du 24 septembre 2014, CEDH 241 (2014) du 29 août 2014; voir également l'analyse de Philip Leach, citée par *The Guardian*, 25 septembre 2014 («Russia's eavesdropping on phone calls examined by Strasbourg Court»).
132. Affaire C-131/12, arrêt du 13 mai 2014 (Grande Chambre).
133. «La prééminence du droit sur l'internet» (note 10), recommandation II.4 (p. 22).

3.1.2. Le débat au sein des Nations Unies

95. Les fichiers Snowden ont également fait naître un débat au sein des Nations Unies. En décembre 2013, l'Assemblée générale des Nations Unies a adopté la Résolution 68/167, qui proclame que les droits des personnes protégés hors ligne devraient également être protégés en ligne et appelle l'ensemble des Etats à respecter et à protéger le droit au respect de la vie privée dans les communications numériques. Le 30 juin 2014, le Haut-Commissariat des Nations Unies aux droits de l'homme a présenté un rapport[134] sur les graves répercussions des programmes de surveillance massive sur les droits de l'homme dans le cadre du Pacte international relatif aux droits civils et politiques (PIRDCP), qui a été ratifié par 167 Etats et dont l'article 17 comporte des garanties similaires à celles de la Convention européenne des droits de l'homme en matière de droit au respect de la vie privée. Ce rapport soulevait plusieurs points importants auxquels les Etats devront remédier pour que la législation et la politique restent adaptées à la nature évolutive des communications numériques. Premièrement, il préconisait que les mesures de surveillance soient «légales» (c'est-à-dire que l'ingérence autorisée par les Etats ait un fondement légal, lui-même conforme au Pacte), qu'elles ne soient pas «arbitraires» et soient par ailleurs «raisonnables» (proportionnées au but poursuivi et nécessaires dans les circonstances en question). Le rapport affirme que la conservation obligatoire des données relatives aux tiers (par exemple lorsque les Etats imposent aux sociétés de services de communications de conserver les données sur les communications de leurs clients) n'était ni nécessaire ni proportionnée et que la collecte des données dans un but légitime et leur utilisation ultérieure dans un autre but légitime n'étaient pas davantage conformes au principe de proportionnalité. Il soulignait le fait que les dispositions secrètes et leur interprétation secrète – voire l'interprétation secrète de la législation par un juge – [auxquelles certains Etats se réfèrent pour justifier leurs programmes de surveillance] ne satisfaisaient pas aux critères indispensables de la «loi», puisqu'elles n'étaient pas suffisamment précises et accessibles pour permettre aux personnes susceptibles d'être concernées de régler leur conduite en prévision des conséquences qu'un acte donné pouvait avoir. Afin de combler le vide juridique qui permet l'existence d'une «coopération à des fins de collusion», le rapport concluait que l'obligation de protection de la vie privée faite à l'Etat naissait dès que la surveillance impliquait «l'exercice du pouvoir ou le contrôle effectif dudit Etat à l'échelle de l'infrastructure des communications numériques».

96. Le rapport des Nations Unies faisait en outre observer que le traitement différent réservé aux cibles étrangères et non étrangères contrevenait au principe de non-discrimination énoncé par le PIRDCP – un problème crucial également à mes yeux. Il soulignait la nécessité de l'existence d'un contrôle effectif des programmes de surveillance, sous la forme d'une combinaison de mécanismes de contrôle administratifs, judiciaires et parlementaires véritablement impartiaux, indépendants et transparents. Enfin, le rapport proposait que les Etats mettent à la disposition des victimes d'une violation de la vie privée des recours effectifs et que le secteur privé, dans la mesure où il a fait l'objet d'une «délégation de la force publique et des responsabilités quasi judiciaires aux intermédiaires internet sous couvert d'"autorégulation" ou de "coopération"»[135] s'engage expressément à respecter et à protéger les droits de l'homme.

3.2. Liberté d'expression, droit à l'information et liberté d'association

97. Indépendamment du fait que les particuliers soient conscients d'être la cible d'opérations de surveillance massive, l'interception et la collecte indistinctes des données ont d'importantes ramifications à l'égard de liberté d'expression, d'information et d'association. Le fait de savoir que les Etats opèrent une surveillance massive a un effet dissuasif sur l'exercice de ces libertés. Selon un rapport de novembre 2013 sur les effets de la surveillance de la NSA, rédigé par PEN International[136], les écrivains ne sont pas seulement inquiets à une très large majorité de la surveillance des gouvernements, ils pratiquent également de ce fait l'autocensure. 85 % des 520 écrivains américains qui ont répondu à cette enquête ont déclaré être inquiets de la surveillance du gouvernement[137]. 28 % ont réduit ou évité les activités des médias sociaux, 24 % ont délibérément évité d'aborder certains sujets au téléphone ou dans leurs courriers électroniques et 16 % ont évité d'écrire ou de s'exprimer à propos d'un sujet particulier. Lorsque les auteurs, les journalistes ou les militants de la société civile se montrent réticents à écrire, s'exprimer ou faire des recherches sur certains sujets (par exemple le Moyen-Orient, les critiques à l'égard du Gouvernement après le 11 septembre, le mouvement Occupy, les questions militaires, etc.) ou à communiquer avec des sources ou des amis à l'étranger de peur de mettre en danger leurs homologues, cela ne nuit pas seulement à leur liberté d'expression, mais également à la liberté d'information de tous les autres citoyens.

---

134. «Le droit à la vie privée à l'ère du numérique», Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme.
135. *Ibid*., p. 14.
136. Une association d'écrivains qui promeut la littérature et la liberté d'expression dans le monde.
137. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

98. Comme nous l'avons indiqué plus haut, la NSA a ciblé des personnes qui avaient simplement fait une recherche sur certains mots en indiquant leur souhait de protéger leurs données, avaient consulté certains sites web ou avaient lu passivement un forum en ligne sur lequel d'autres personnes soupçonnées échangeaient des messages instantanés. Le fait d'avoir conscience que les gouvernements peuvent cibler les personnes qui se réunissent sur certains sites web nuit à la liberté de toute personne de naviguer sur internet ou de communiquer avec des individus dont elle craint qu'ils puissent éveiller les soupçons des autorités pour une raison ou une autre.

99. En octobre 2014, le Président Poutine a annoncé le renforcement de la surveillance sur internet en Russie, dans le but de se protéger contre les attaques des pirates informatiques et la propagande en faveur de la violence et de l'extrémisme[138]. Sachant que ce dernier terme est interprété très largement par les autorités répressives russes, cette annonce ne présage rien de bon, même si le Président jure de respecter les principes démocratiques de la liberté d'expression et d'information.

3.3. Démocratie

100. Les opérations de surveillance massive indistincte présentent également un risque essentiel pour la démocratie, dès lors que les services de renseignement contournent les voies politiques démocratiques et juridiques pour mettre en œuvre des programmes qui interceptent une quantité considérable de communications privées. Les fichiers divulgués par M. Snowden montrent que les Etats ont faussement prétendu ignorer la coopération de leurs services de renseignement avec la NSA pour mener diverses formes d'opérations de surveillance massive, à l'échelon tant national qu'international. Au Royaume-Uni, des ministres ont affirmé ignorer totalement l'existence de TEMPORA, le plus important programme d'espionnage du GCHQ, tandis que le Président Obama a prétendu qu'il n'avait pas été informé de la surveillance par la NSA du téléphone portable personnel de la chancelière Merkel. Les responsables politiques allemands de haut rang ont fait part de leur indignation après les révélations sur la surveillance massive de la population allemande[139]. Or, la coopération approfondie des services de renseignement allemands dans cette surveillance a été révélée par la suite[140].

101. Cette ignorance réelle ou supposée laisse penser que certaines parties du gouvernement, sans parler des citoyens directement touchés par les programmes de surveillance, n'avaient pas été consultées comme elles auraient dû l'être. De fait, un document de la NSA divulgué a montré que: «Un agent SIGINT ['données de transmission des services de renseignement'] auquel on demandait si les changements politiques au sein de ces pays avaient une incidence sur les relations de la NSA a expliqué en quoi ces changements étaient en général sans conséquence: seule une poignée de responsables militaires de ces pays sont informés des activités d'espionnage. Peu d'élus, pour autant qu'il y en ait, ont connaissance de cette surveillance[141].» Bien qu'il ne soit naturellement pas souhaitable, ni même possible, de placer l'ensemble des activités de renseignement sous le contrôle intégral des citoyens, le processus politique constitutionnel, qui garantit la responsabilité des services devant des dirigeants démocratiquement élus, ne doit pas être contourné. Les instances parlementaires de contrôle doivent avoir un accès suffisant aux informations et aux documents pour pouvoir exercer leur mandat de manière constructive. Une réflexion entendue à Bruxelles au début du mois me paraît tout à fait censée: pour que les instances parlementaires de contrôle se montrent plus mordantes, il faudrait qu'elles aient leur mot à dire dans les affectations budgétaires des services qu'elles contrôlent. D'après ce que j'ai pu constater, la responsabilité budgétaire est réellement une forme extrêmement efficace de responsabilité politique.

102. Comme je l'ai fait remarquer dans ma note introductive[142], l'emballement de cette machine de surveillance est dû au fait que les dirigeants politiques ont perdu le contrôle des activités des services de renseignement, que la plupart des responsables politiques ne parviennent plus à comprendre. James Clapper, directeur du Service national de renseignement, a ainsi donné une réponse célèbre au sénateur Ron Wyden, membre de la commission du renseignement du Sénat, qui lui demandait lors d'une audience publique organisée par le Congrès le 12 mars 2013 si la NSA collectait les données de centaines de millions de personnes ou de centaines de millions d'Américains qui n'étaient soupçonnés d'aucune infraction: «Non Monsieur, pas en connaissance de cause[143].» Je ne veux toujours pas croire qu'il ait menti. Mais il n'avait, à tout le moins, pas été correctement informé de la situation par ses collaborateurs, qui avaient eux-mêmes

138. *SPIEGELonline,* 1er octobre 2014, Internetüberwachung – Putin klagt über Hacker-Angriffe.
139. Voir les références dans la note introductive (AS/Jur (2014) 02), paragraphe 23.
140. Voir plus haut paragraphe 29 et note 31 *supra*.
141. *The Intercept*, 13 mars 2014, «Foreign Officials In the Dark About Their Own Spy Agencies' Cooperation with NSA».
142. Document AS/Jur (2014) 02, paragraphe 52.
143. Fred Kaplan, «James Clapper lied to Congress about NSA surveillance», 11 juin 2013.

peut-être perdu le contrôle des activités des entreprises privées au profit desquelles une bonne part des opérations de surveillance avaient été externalisées (comme l'employeur de M. Snowden). La privatisation des opérations de surveillance risque fort de générer elle-même l'augmentation de ses activités, alimentée par l'intérêt qu'y trouvent les prestataires. Les «besoins» toujours croissants en dépenses de surveillance sont si faciles à justifier: le fait d'avoir pu prévenir une tentative d'attentat grâce aux opérations de surveillance rend l'augmentation de ces activités de surveillance indispensable pour éviter davantage d'attentats[144]; lorsqu'un attentat n'a pu être évité, cela tient au fait que les opérations de surveillance étaient insuffisantes… Le parallèle qui peut être établi avec la privatisation des prisons aux Etats-Unis est inquiétant: depuis les débuts de la privatisation dans les années 1980, la population carcérale américaine a au moins triplé, en dépit de la diminution du taux de criminalité au cours de la même période[145]. La croissance «du complexe industriel de la surveillance» pourrait bien égaler, voire dépasser la «croissance du complexe carcéro-industriel»[146].

3.4. L'application extraterritoriale des droits de l'homme et l'égalité de traitement des résidents nationaux et étrangers

103. Comme nous l'avons vu, le droit interne offre une protection juridique plus ou moins solide du droit au respect de la vie privée des résidents: elle est assez solide en Allemagne, et un peu moins aux Etats-Unis[147] ou au Royaume-Uni, dont les populations ne bénéficient pas de la méfiance de leurs services de renseignement respectifs que les Allemands doivent aux ravages de la Gestapo et de la Stasi. Mais cette protection (et même son renforcement actuellement examiné aux Etats-Unis et dans d'autres pays) n'est tout simplement pas applicable aux ressortissants étrangers, qui sont traités comme une cible: seuls les «Américains» (ressortissants et résidents) bénéficient du Premier Amendement (liberté d'expression et liberté d'association), du Quatrième Amendement (protection contre les «perquisitions excessives») et de la plupart des garanties (limitées) que prévoit la législation relative à la sécurité nationale[148]. Le rapport de décembre 2014 du Commissaire aux droits de l'homme du Conseil de l'Europe résume très justement en quoi cette situation va à l'encontre de la tendance générale du droit international des droits de l'homme à l'élargissement du champ de l'application extraterritoriale des obligations des Etats en matière de droits de l'homme (y compris les obligations nées du PIRDCP, que les Etats-Unis ont ratifié) et pourquoi elle constitue une violation du principe de l'égalité de traitement[149]. Aux fins du présent rapport, la situation sans équivalent dans laquelle se trouvent les Etats-Unis (et le Royaume-Uni) par rapport à l'infrastructure matérielle d'internet et le fait que les sociétés privées établies aux Etats-Unis collectent et conservent d'énormes quantités de données relatives à des personnes qui résident n'importe où dans le monde rendent l'exclusion des «non Américains (et Britanniques)» de toute protection légale contre les opérations de surveillance massive tout simplement intolérable; cette situation pourrait bien conduire à la destruction d'internet tel que nous le connaissons, comme nous le verrons plus loin.

---

144. Mais la NSA a intensifié ses activités de surveillance bien avant le 11 septembre 2001 et, malgré le niveau de surveillance actuel, elle n'a pas mis un terme au terrorisme. Un rapport du 12 décembre 2013, rédigé par un groupe d'experts du Sénat américain («Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies») conclut que la collecte des métadonnées n'a pas joué de rôle déterminant dans la prévention des attentats terroristes (p. 104).

145. Voir par exemple www.globalresearch.ca/the-prison-industry-in-the-united-states-big-business-or-a-new-form-of-slavery/8289.

146. John W. Whitehead, «Jailing Americans for profit: the rise of the prison industrial complex»,*Huffington Post*, 4 octobre 2012.

147. Le rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail ad hoc UE-USA sur la protection des données (Report on Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection) du 27 novembre 2013 donne un excellent aperçu des fondements juridiques des activités de surveillance aux Etats-Unis au titre de l'article 702 de la loi FISA, de l'article 215 de la loi «USA Patriot» et du décret d'application 12333. Ce document souligne notamment la différence fondamentale qui existe entre la définition par l'Union européenne de la collecte et du traitement des données et la définition retenue par les Etats-Unis, qui, contrairement au droit de l'Union européenne, ne considèrent pas généralement l'acquisition initiale des données à caractère personnel comme un «traitement» des données à caractère personnel au sens des garanties accordées par la loi. Le document démontre également que le principal problème n'est pas celui de l'illégalité en droit américain des activités de surveillance de la NSA, mais celui de la faiblesse des dispositions légales en vigueur, qui semblent prendre en compte la plupart des pratiques révélées par M. Snowden.

148. «La prééminence du droit sur l'internet» (note 10), p. 11, et la recommandation I.1 du Commissaire (p. 21).

149. «La prééminence du droit sur l'internet» (note10), p. 48-50.

4. Les répercussions des opérations de surveillance massive sur la coopération internationale et l'avenir d'internet

104. En premier lieu, le fait que les révélations aient montré que la NSA espionnait même ses alliés les plus proches a nui aux relations interétatiques. Au Brésil, la Présidente Rousseff a vivement condamné les activités de surveillance de la NSA, en déclarant dans une allocution prononcée devant l'Assemblée générale des Nations Unies en septembre 2013: «Nous sommes confrontés (…) à une situation de graves violations des droits de l'homme et des libertés civiles, à une invasion et à une interception d'informations confidentielles relatives aux activités des entreprises, et surtout à un manque de respect envers la souveraineté nationale de mon pays»[150]. M[me] Rousseff est allée jusqu'à annuler une visite aux Etats-Unis après des révélations selon lesquelles la NSA avait intercepté ses propres courriers électroniques et messages, ainsi que ceux de l'entreprise pétrolière publique Petrobras[151]. Le Brésil a, depuis, cherché à acheminer les communications Internet en contournant les Etats-Unis afin d'éviter toute surveillance. Le 2 juillet 2014, l'Inde a convoqué un haut diplomate américain après avoir appris que les Etats-Unis avaient autorisé la NSA à espionner le parti au pouvoir, le BJP, lorsqu'il était dans l'opposition en 2010[152].

105. Les relations entre les Etats-Unis et l'Allemagne se sont elles aussi considérablement dégradées à cause de cette affaire de surveillance. Le Gouvernement allemand a mis fin à son contrat de services de communications avec la société américaine Verizon Communications Inc. pour les services administratifs à partir de 2015[153]. La révélation de l'espionnage par la NSA de la chancelière Merkel et d'autres personnalités allemandes de premier plan a suscité un tollé général. *Der Spiegel* a accusé la NSA de «transformer internet en un système d'armes», tandis que le *New York Times* a indiqué que M[me] Merkel comparait la mise sur écoute de son téléphone par la NSA aux écoutes de la Stasi. La ministre allemande de la Justice, Sabine Leutheusser-Schnarrenberger, qui avait vivement critiqué les Etats-Unis depuis le scandale PRISM, a qualifié les méthodes américaines de surveillance de «réminiscence des méthodes utilisées par les ennemis pendant la guerre froide». Les négociations sur un accord de non-espionnage entre l'Allemagne et les Etats-Unis se sont achevées au bout de plusieurs mois sans avoir abouti, car les deux parties ne sont pas parvenues à s'entendre sur sa portée[154]. Bien que M[me] Merkel ait déconseillé d'inviter M. Snowden à témoigner devant la commission d'enquête précitée constituée par le Parlement allemand, pour éviter de nuire davantage aux relations entre les Etats-Unis et l'Allemagne, ces relations se sont tendues une nouvelle fois après l'annonce de deux doubles agents supposés qui espionnaient en Allemagne pour le compte des Etats-Unis. Ces révélations ont été faites lorsque la commission d'enquête du Bundestag a entendu le témoignage de deux anciens collaborateurs de la NSA, Thomas Drake et William Binney, sur les programmes de surveillance massive de la NSA et la coopération alléguée du BND allemand. Après avoir prudemment demandé des explications à Washington, surtout depuis que le Président Obama avait ordonné un bilan complet de l'espionnage des pays alliés et des autres partenaires à la suite de la divulgation de la mise sur écoute de M[me] Merkel, l'Allemagne a non seulement convoqué l'ambassadeur américain John B. Emerson au ministère des Affaires étrangères le 4 juillet 2014, juste avant la réception donnée à l'ambassade américaine pour des centaines d'invités à l'occasion de la fête nationale des Etats-Unis[155], mais a également invité le chef du bureau de la CIA à quitter Berlin, en manquant de peu de l'expulser officiellement du pays[156]. Certains bureaux du Bundestag auraient même sérieusement envisagé de revenir à l'utilisation des machines à écrire pour les communications particulièrement sensibles, afin de déjouer désormais toute surveillance de la NSA[157].

106. Pourtant, d'aucuns ont jugé «étonnamment modérée» la réaction initiale des gouvernements face aux révélations des programmes de surveillance massive de la NSA, considérant que les dirigeants avaient généralement eu connaissance des activités de surveillance habituellement pratiquées par les services de renseignement étrangers – et leurs propres services nationaux[158]. Le Royaume-Uni en offre un exemple représentatif. Après la destruction d'ordinateurs et des fichiers que les journalistes du *Guardian* avaient reçus

---

150. *USA Today*, 20 octobre 2013, «Global reaction to NSA spying reports» pour un échantillon de réaction des dirigeants à travers le monde après les révélations sur la NSA.
151. BBC News, 17 septembre 2013, «Brazilian President Dilma Rousseff calls off US trip».
152. Harmeet Shah Singh et Ben Brumfield, «India summons U.S. diplomat over report of NSA spying.» CNN.com, 2 juillet 2014.
153. Anton Troianovski et Danny Yadron, «German Government Ends Verizon Contract: Interior Ministry Cites Security Concerns Amid U.S. Spying Disclosures», *Wall Street Journal*, 26 juin 2014.
154. *The New York Times*, 2 mai 2014, «Merkel Signals That Tension Persists Over U.S. Spying».
155. *The New York Times*, 6 juillet 2014, «Ties Strained, Germans Press U.S. to Answer Spy Allegation».
156. *The Telegraph*, 10 juillet 2014, «Germany asks CIA station chief in Berlin to leave country over US spying row».
157. *Forbes*, 19 juillet 2014, «German NSA Inquiry Chief Proposes Ultimate Cybersecurity Move… Use a Typewriter».
158. Karen Kornbluh, attachée supérieure de recherches en politique numérique, Council on Foreign Relations, «Global Responses to NSA Surveillance: 3 things to know».

d'Edward Snowden, le Premier ministre Cameron a même déclaré publiquement que «[s]i elle [la presse] ne faisait pas preuve d'un minimum de responsabilité sociale, il sera extrêmement difficile pour le gouvernement de se tenir en retrait et de ne pas agir», mettant ainsi principalement en garde la presse britannique contre la publication de reportages sur le contenu des fichiers Snowden. En août 2013, David Miranda, le compagnon de M. Greenwald qui avait eu accès aux fichiers Snowden, a même été détenu au titre de la législation antiterroriste à l'aéroport de Heathrow pendant neuf heures alors qu'il se rendait à Rio de Janeiro. Le téléphone portable, l'ordinateur portable, les DVD et d'autres objets appartenant au ressortissant brésilien auraient été saisis. Comme l'a déclaré Jonathan Marcus sur BBC news,

> *«les gouvernements européens amis des Etats-Unis sont quelque peu vexés et l'Administration Obama est quelque peu embarrassée. Je dis "quelque peu" parce que, d'après ce qu'indique une bonne partie des commentaires formulés après ces révélations, on assiste à une sorte de jeu d'ombres chinoises. Cela ressemble un peu à ce passage d'un classique du cinéma, "Casablanca", où le chef de la police se dit choqué de voir qu'on pratique le jeu dans un établissement dont il sait parfaitement qu'il s'agit d'un casino, quelques instants à peine avant qu'un croupier lui remette ses gains»*[159].

107. Comme le secrétaire d'Etat à la Défense Donald Rumsfeld l'avait un jour déclaré, «c'est des choses qui arrivent». Mais la confirmation que de proches alliés s'espionnent mutuellement met en jeu la coopération politique et économique dans d'autres domaines. La confiance des citoyens à l'égard de leur gouvernement et des entreprises de leur propre pays en a été ébranlée, parce que les révélations ont montré que les acteurs du secteur public et du secteur privé étaient de connivence avec la NSA. Les utilisateurs d'internet en Europe se sont de plus en plus plaints de la domination des sociétés américaines de technologie, notamment pour le traitement des données, bien qu'ils continuent à recourir massivement aux services de ces entreprises[160]. Google conserve 85 % des parts de marché de la recherche sur internet dans les cinq principales puissances économiques européennes, y compris au Royaume-Uni, en France et en Allemagne, contre 65 % sur le marché américain. Facebook a plus que doublé le nombre de ses utilisateurs européens, qui ont dépassé les 150 millions, au cours des cinq dernières années; selon les statistiques comScore, les entreprises américaines de technologie exploitent sept des 10 sites web les plus visités.

108. Face au mécontentement croissant qu'a suscité la surveillance des Etats-Unis, les responsables politiques ont réagi en demandant un renforcement de la «souveraineté technologique» et une «nationalisation des données». Les révélations de M. Snowden ont donc eu de graves répercussions sur le développement d'internet et ont accéléré la tendance à la «balkanisation» d'internet, au détriment du développement d'un immense réseau en ligne facilement accessible. Internet tel que nous le connaissons (ou tel que nous pensions le connaître) est une plate-forme mondiale d'échange d'informations, de débat ouvert et libre et de commerce. Mais le Brésil et l'Union européenne, par exemple, ont annoncé un projet de pose d'un câble sous-marin en fibre optique de $US 185 millions pour contrecarrer la surveillance des Etats-Unis. Les responsables politiques allemands ont également appelé à la mise au point d'un «internet allemand» permettant aux données des consommateurs allemands de contourner les serveurs étrangers et aux informations de demeurer dans des réseaux intégralement contrôlés par l'Allemagne[161]. La Russie a adopté une loi qui impose aux entreprises d'internet de conserver les données des utilisateurs russes sur des serveurs installés en Russie[162]. Après une enquête de six mois menée à la suite des révélations de M. Snowden, le Parlement européen a adopté un rapport sur le programme de surveillance de la NSA en février 2014[163], qui affirme que l'Union européenne devrait suspendre les accords conclus avec les Etats-Unis sur les données bancaires et la sphère de sécurité relatifs à la confidentialité des données (normes volontaires de protection des données que les sociétés non-Union européenne sont tenues de respecter lors du transfert aux Etats-Unis des données à caractère personnel des citoyens de l'Union européenne). Les parlementaires européens ont ajouté que le Parlement européen devait uniquement donner son accord au Partenariat transatlantique de commerce et d'investissement (TTIP) entre l'Union européenne et les Etats-Unis, qui est en cours de négociation, si les Etats-Unis respectaient pleinement les droits fondamentaux des citoyens de l'Union européenne. Le Parlement européen réfléchit à de nouvelles dispositions rigoureuses en matière de protection des données, qui placeraient les entreprises américaines dans la difficile situation d'être soumises à une vérification préalable des autorités de l'Union européenne avant de se conformer aux

---

159. BBC News, 26 octobre 2013, «NSA spying allegations: Are US allies really shocked?».
160. *The New York Times*, 6 juillet 2014, «Principles Are No Match for Europe's Love of US Web Titans».
161. Reuters, 25 octobre 2013, «Germany wants German Internet as spying scandal rankles».
162. Hogan Lovells, Chronicle of Data Protection, «Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect« (posté le 18 juillet 2014).
163. Voir le rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).

demandes contraignantes faites par les autorités américaines. La commission des libertés civiles (LIBE) du Parlement européen a également préconisé la création d'un espace de stockage en ligne («cloud») des données de l'Union européenne, qui imposerait le stockage ou le traitement de l'ensemble des données des consommateurs européens en Europe, voire dans le pays du consommateur concerné. D'après deux professeurs de droit, certains Etats, comme l'Australie, la France, la Corée du Sud et l'Inde, ont déjà mis en œuvre une constellation d'exigences relatives à la géolocalisation des données[164].

109. Selon moi, la proposition faite par le Parlement européen, qui préconise d'utiliser tous les instruments dont l'Union européenne dispose dans ses relations avec les Etats-Unis pour faire pression en faveur de la protection de la vie privée des citoyens européens mérite un soutien sans réserve. Dans leurs négociations sur les nouveaux accords, tels que le Partenariat transatlantique de commerce et d'investissement (TTIP), et dans la mise en œuvre de ceux qui existent déjà, comme le Programme de surveillance du financement du terrorisme (Terrorist Finance Tracking Programme – TFTP) ou l'accord sur les données des dossiers passagers (Passenger Name Records – PNR) et la décision sur la sphère de sécurité[165], les négociateurs de l'Union européenne devraient indiquer clairement que l'Europe n'accepte pas d'être espionnée par son partenaire transatlantique. La législation et la pratique devraient assurer aux citoyens européens et américains une protection égale de leur droit au respect de la vie privée, qui devrait faire partie intégrante d'un partenariat fondé sur le respect et la confiance mutuels[166].

110. En revanche, la proposition de «nationaliser» les communications internet présente de multiples dangers: la structure d'internet n'est pas conçue pour un «routage national» et le fait d'apporter d'importants changements au mode de routage pourrait diminuer la fonctionnalité globale du réseau[167]. En outre, les experts considèrent que l'important en matière de sécurité des communications n'est pas la géolocalisation des données, mais la complexité des mesures de protection[168]. Qui plus est, ces mesures de renationalisation pourraient bien s'avérer contre-productives du point de vue des principes défendus par le Conseil de l'Europe. Le routage national ne protège habituellement pas les droits fondamentaux, bien au contrair. La Chine ou l'Iran, par exemple, où les gouvernements cherchent à restreindre les informations mises à la disposition de leurs citoyens, en font un usage abusif: «La géolocalisation des échanges sur internet renforcera les possibilités de surveillance et de censure nationales et la forme de persécution politique des dissidents sur internet que l'Occident combat depuis des années[169].» Certains Etats membres du Conseil de l'Europe pourraient également être tentés par cette solution[170].

5. Les solutions qui permettraient d'atténuer au maximum les conséquences négatives des opérations de surveillance massive et le rôle que le Conseil de l'Europe pourrait jouer en la matière

111. Les fichiers Snowden ont montré la nécessité d'établir un cadre juridique plus précis pour les activités de surveillance, à l'intérieur et à l'extérieur des frontières nationales. Le Conseil de l'Europe a un rôle important à jouer à cet égard, car il ne lui est pas interdit, contrairement à l'Union européenne, de traiter de la protection des droits de l'homme vue sous l'angle de la sécurité nationale.

5.1. Revoir la législation nationale en vue d'adapter la protection de la vie privée aux défis que représentent les progrès technologiques qui permettent d'opérer une surveillance massive

112. Depuis juillet 2014, plusieurs nouvelles affaires qui portent directement sur les programmes de surveillance massive révélés par les fichiers Snowden sont pendantes devant la Cour européenne des droits de l'homme. La jurisprudence de la Cour a déjà établi que les Etats devaient mettre en place un processus transparent pour s'assurer que seules les mesures de surveillance nécessaires soient prises dans le but d'atteindre un ensemble clairement défini d'objectifs, qui exigent et justifient une atteinte au droit au respect

---

164. *The Atlantic*, 25 juin 2014, «The End of the Internet?».
165. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (en anglais), 27 novembre 2013 (document de la Commission européenne COM(2013)847 final).
166. Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows (en anglais), 27 novembre 2013 (document de la Commission européenne COM(2013)846 final).
167. Georg Mascolo et Ben Scott, «Lessons from the summer of Snowden, the hard road back to trust», Open Technology Institute, Wilson Center, New America Foundation, octobre 2013 (p. 12).
168. *The Atlantic*, 25 juin 2014, «The End of the Internet?».
169. Mascolo et Scott, *op. cit*., p. 12.
170. Voir, par exemple, le rapport de Human Rights Watch: «Turkey: Internet Freedom Rights in Sharp Decline», 2 septembre 2014; pour l'Azerbaïdjan, voir l'aperçu général donné par Freedom House, «Freedom on the Net/Azerbaijan» (2013).

de la vie privée. Au lieu d'attendre la constatation par la Cour de violations, les Etats membres du Conseil de l'Europe devraient revoir préventivement leur législation, pour veiller à ce qu'elle reste adaptée aux défis que représentent les progrès technologiques qui permettent d'opérer une surveillance massive dans les proportions révélées par M. Snowden.

113. Le droit interne devrait uniquement permettre la collecte et l'analyse des données à caractère personnel (y compris des métadonnées) avec le consentement des intéressés ou à la suite d'une ordonnance judiciaire rendue sur la base du soupçon raisonnable que la cible prend part à des activités criminelles. Il importe que la collecte et le traitement illégaux des données soient pénalisés 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 encore à exploiter les failles existantes, devrait être rigoureusement interdite. Compte tenu du rôle particulièrement important que jouent les entreprises privées dans la collecte et le traitement des données à caractère personnel, il convient de soumettre l'ensemble des établissements et entreprises privés qui collectent ou conservent ces données à des normes de sécurité rigoureuses.

114. Afin de faire respecter ce cadre juridique, les Etats membres devraient également veiller à ce que leurs services de renseignement soient soumis à des dispositifs de contrôle judiciaire et parlementaire adéquats. Ces instances de contrôle doivent disposer d'un accès suffisant aux informations et aux connaissances expertes. Elles devraient également avoir le pouvoir d'examiner toute coopération internationale sans être tenues de respecter le principe de la maîtrise de l'information par son auteur (en vertu duquel le service dont provient l'information en question a le droit de déterminer avec qui cette information est partagée). Cela devra se faire sur une base mutuelle, étant entendu de part et d'autre que dans tous les Etats respectueux de la prééminence du droit, les services de renseignement sont soumis à un contrôle judiciaire ou parlementaire.

5.2. Un «Code du renseignement» international qui énonce des principes fondamentaux mutuellement admis

115. Les remous politiques causés par «l'espionnage des amis» et la possible collusion entre les services de renseignement en vue de contourner les restrictions nationales montrent qu'il est indispensable que les Etats s'entendent sur l'élaboration d'un «code» des services de renseignement admis par tous, qui mettrait un terme aux opérations de surveillance massive illimitée et confinerait les pratiques de surveillance aux mesures strictement indispensables à la poursuite de buts sécuritaires légitimes. Ce code définirait précisément ce qui est permis et ce qui est interdit entre alliés et partenaires; il préciserait ce que les services de renseignement sont autorisés à faire, de quelle manière ils peuvent coopérer et comment des alliés devraient s'abstenir de s'espionner les uns les autres. Comme l'a expliqué lors de l'audition de la commission du 4 avril 2014 M. Hansjörg Geiger, ancien chef du BND allemand et secrétaire d'Etat auprès du ministère de la Justice, ce code démontrerait la volonté des gouvernements d'instaurer un certain degré de transparence dans l'application de leurs programmes de surveillance et de garantir, dans la mesure du possible, le droit des citoyens au respect de leur vie privée[171].

116. M. Geiger a proposé quatre principes simples. Premièrement, toute forme d'espionnage politique ou économique mutuel doit être interdite, sans exception. La surveillance ou l'écoute des alliés altère la confiance entre les pays «amis» et le prix à payer est très supérieur aux avantages que peut procurer ce genre de pratique. Deuxièmement, l'activité d'un service de renseignement sur le territoire d'un autre Etat membre peut uniquement être exercée avec le consentement de ce dernier et dans le respect du cadre juridique qui y est applicable (par exemple dans le but spécifique de prévenir le terrorisme ou toute autre forme d'actes criminels extrêmement graves). Troisièmement, les données relatives aux ressortissants non soupçonnés d'Etats amis ne sauraient en aucun cas être recherchées, analysées ou conservées massivement. Seules les informations relatives à des personnes légitimement ciblées peuvent être collectées à titre exceptionnel et dans un but précis. Toute donnée relative à un particulier ou donnée économique conservée qui n'est pas indispensable à la poursuite de ce but clairement défini doit être supprimée ou détruite sans tarder. Quatrièmement, les sociétés de télécommunications et les fournisseurs de services internet ne peuvent être contraints par les services de renseignement de leur accorder un accès illimité à d'immenses bases de données à caractère personnel; seule une décision de justice peut ordonner cette mesure. Une telle restriction ne compromettrait pas la sécurité des Etats contractants, car cette décision de justice peut être obtenue en cas de menace réaliste particulière.

---

171. Audition du 8 avril 2014 de la commission des questions juridiques et des droits de l'homme sur «Les opérations de surveillance massive». La vidéo complète de cette audition est disponible sur: http://clients.dbee.com/coe/webcast/index.php?id=20140408-1&lang=en.

117. Même un code du renseignement adopté volontairement aurait de puissants effets, puisque les Etats qui refuseraient de le respecter pourraient être accusés par leurs alliés de pratiques illégales, ce qui altérerait leur crédibilité de partenaires de coopération. Mais un accord multilatéral contraignant serait plus efficace pour combler les vides juridiques que les Etats exploitent à l'heure actuelle pour contourner les restrictions légales imposées à leurs programmes de renseignement. Comme nous l'avons vu précédemment, la «collusion visant à se soustraire aux restrictions» permet encore aux services de renseignement de repousser les limites de leur pouvoir de collecte des données dans leur propre pays, en recourant aux données collectées par leurs alliés ou par des Etats tiers. Un code du renseignement offrirait une occasion de combler les vides juridiques et de protéger les citoyens, non seulement de la surveillance de leurs propres gouvernements, mais également de celle des autres Etats contractants.

118. Cette prouesse est bien entendue ambitieuse et soulèverait de nombreuses questions essentielles avant même que le processus de négociation ne soit engagé: il s'agira notamment de définir quels seront les Etats Parties à ce code, comment son application sera contrôlée et les termes précis de l'accord qui permettra aux services de renseignement d'assumer convenablement leurs missions légitimes, tout en protégeant les libertés civiles et les droits de l'homme. Mais ce défi vaut la peine d'être relevé, compte tenu des enjeux en présence, et il offre au Conseil de l'Europe une occasion de jouer un rôle important, conforme à sa mission de défense de l'Etat de droit, des droits de l'homme et de la démocratie.

5.3. Un cryptage généralisé destiné à renforcer le respect de la vie privée

119. En attendant que les Etats s'entendent sur les limites des programmes de surveillance massive de leurs services de renseignement, un cryptage généralisé destiné à renforcer le respect de la vie privée reste la riposte la plus efficace pour permettre aux citoyens de protéger leurs données. Comme l'a expliqué M. Snowden lors de l'audition de la commission en avril 2014, le recours à la «force brute» contre certains systèmes de cryptage n'est pas réellement envisageable, car il faudrait plus d'énergie que n'en contient l'univers tout entier pour procéder à une analyse cryptographique ou, en substance, trouver une solution de décryptage et décrypter des algorithmes de cryptage moderne convenablement mis en œuvre et renforcés par des clés totalement aléatoires et suffisamment longues». Les partisans du recours à un cryptage généralisé pour lutter contre les opérations de surveillance massive insistent par conséquent sur le fait qu'ils peuvent remporter cette «course aux armements» contre la NSA et les autres services de renseignement, en raison de «l'asymétrie» d'ordre technologique entre les modestes ressources nécessaires aux inventeurs de codes de cryptage et le coût considérable que suppose le décryptage d'un code relativement simple.

120. Certains experts techniques vont au-delà de cette proposition et préconisent la «décentralisation» d'internet (au lieu de sa «balkanisation»), c'est-à-dire encouragent chaque utilisateur à installer son propre serveur bien protégé, ce qui exclurait toute forme d'opérations de surveillance massive. Les cibles légitimes, comme les terroristes, les membres de la criminalité organisée et d'autres individus du même type (et leurs fournisseurs d'accès) devront faire l'objet d'une ordonnance judiciaire pour être contraints à renoncer à leurs clés de cryptage. Cette «clientèle» est précisément celle à laquelle la surveillance ciblée classique était autrefois réservée, autorisée par une ordonnance judiciaire prise sur la base de motifs de soupçon concrets.

5.4. Améliorer la protection des donneurs d'alerte

121. Les révélations de M. Snowden ont joué un rôle essentiel pour permettre aux citoyens – et aux responsables politiques – de prendre conscience des programmes de surveillance massive des services de renseignement et provoquer un débat indispensable sur l'étendue du sacrifice des droits civiques et de la vie privée des citoyens auquel il conviendrait de consentir au nom de la sécurité nationale.

122. Cependant, même lorsque des limites légales suffisantes et des mécanismes de contrôle auront été établis à l'échelon national, et sur le plan international au moyen d'un «code du renseignement» multilatéral, les donneurs d'alerte resteront indispensables, car ils sont le moyen le plus efficace de faire respecter les restrictions imposées à la surveillance. Les activités des services secrets sont par nature difficiles à contrôler par un mécanisme de contrôle judiciaire ou parlementaire classique. L'accès d'une instance de contrôle aux informations pertinentes et le problème de capacité que pose le volume colossal d'activités à contrôler rendront toujours ce contrôle difficilement efficace. L'épée de Damoclès que représente la divulgation de tout abus par des donneurs d'alerte présents au sein même des services de renseignement et bien protégés pourrait bien être le moyen de dissuasion le plus efficace contre les graves violations des limites légales qu'il convient, selon nous, d'imposer aux activités de surveillance. Cette appréciation fait d'autant plus autorité qu'elle est partagée par un ancien haut responsable des services de renseignement, M. Geiger, dont l'expérience à la tête du BND allemand confère un poids tout particulier.

123. Il est par conséquent indispensable de réévaluer les mesures de protection des donneurs d'alerte parallèlement à la formulation de nos recommandations relatives aux opérations de surveillance massive. Ces questions seront abordées prochainement dans un rapport distinct en cours d'élaboration consacré au thème «Améliorer la protection des donneurs d'alerte».

6. Conclusions

124. Les «fichiers Snowden» ont révélé l'étendue de la menace que la surveillance massive représente pour notre vie privée et pour les autres droits de l'homme dont l'exercice effectif dépend du respect de la vie privée, comme la liberté d'expression et d'information, voire la liberté de religion, le droit à un procès équitable et le droit à l'égalité de traitement. En résumé, rien ni personne ne peut espérer échapper à la surveillance des services de renseignement de nos propres pays et même de pays étrangers – à moins que nous réussissions à généraliser le recours à des technologies sûres[172]. Les progrès technologiques qui permettent aux services de renseignement de premier plan dans le monde de collecter et de conserver des quantités stupéfiantes de données, «partout, en permanence», s'accompagnent de bonds technologique équivalents dans la mise au point des outils de filtrage et d'analyse nécessaires à l'utilisation de ces données. Avant que le «complexe industriel de la surveillance» ne soit totalement hors de contrôle, nous devons agir, afin d'imposer à cette surveillance le respect de l'Etat de droit. Il faudra pour cela revoir complètement la législation nationale pertinente dans la plupart, si ce n'est la totalité, des Etats membres et observateurs. Par ailleurs, des principes fondamentaux devront être énoncés à l'échelon international. Pour être crédible, le respect du cadre juridique national et international devra être assuré par des mécanismes de contrôle convaincants, ainsi que par la protection des donneurs d'alerte qui révèlent les violations commises. Il convient également de donner aux organes de contrôle parlementaire la possibilité de se montrer suffisamment mordants, en leur permettant d'avoir leur mot à dire dans l'approbation des affectations budgétaires des services. En attendant que ce cadre juridique soit réellement en place et fonctionne, l'usage généralisé du cryptage «de bout en bout» (end-to-end) et la décentralisation semblent être les seuls moyens de protection disponibles contre les abus qui nuisent aujourd'hui déjà à l'intégrité d'internet.

125. Enfin, il convient de garder à l'esprit que les opérations de surveillance massive ont un coût sur le plan politique comme sur celui des droits de l'homme: elles menacent l'existence même d'internet tel que nous le connaissons, avec les avantages socio-économiques que nous en retirons à l'heure actuelle; elles altèrent la confiance entre les pays amis et partenaires sur la scène internationale; et elles portent atteinte à la vie privée et aux libertés civiques de nos concitoyens. Il importe que le Conseil de l'Europe saisisse cette occasion d'attirer l'attention sur les normes internationales indispensables à la protection des droits de l'homme fondamentaux, tout en veillant à ce que les services de renseignement continuent à assurer notre sécurité en utilisant des moyens efficaces et proportionnés. Une première étape positive pourrait consister, pour le Secrétaire Général du Conseil de l'Europe, à ouvrir une enquête au titre de l'article 52 de la Convention européenne des droits de l'homme, en demandant à tous les Etats membres d'expliquer de quelle manière leur droit interne assure l'application effective du droit au respect de la vie privée et familiale garanti par l'article 8.

126. Comme nous l'avons vu, les opérations de surveillance massive ne sont même pas un outil efficace pour la lutte contre le terrorisme et la criminalité organisée, par rapport à la surveillance ciblée classique[173]. Nous avons également vu que certains aspects des opérations de surveillance massive, comme la fragilisation délibérée du cryptage et d'autres normes de sécurité d'internet pour faciliter la collecte des données, représente un grave danger pour la sécurité nationale[174]. Ces failles peuvent être décelées et exploitées par des Etats voyous, des terroristes, des cyberterroristes et des criminels de droit commun pour causer d'énormes dommages à nos sociétés. Il s'ensuit que la protection de la vie privée et la protection de la sécurité nationale ne sont pas incompatibles, bien au contraire: la protection des données et la sécurité d'internet sont indispensables à notre sécurité!

127. Les projet de résolution et projet de recommandation reprennent les éléments essentiels de ces constatations et conclusions.

---

172. Telles que GnuPG ou OTR (*Der Spiegel*, 27 décembre 2014, révélation de documents de la NSA portant une évaluation de l'efficacité de différentes méthodes de cryptage).
173. Voir plus haut le paragraphe 70, qui mentionne des études américaines et de l'Union européenne qui parviennent à la même conclusion.
174. Voir plus haut les paragraphes 68 et 69.