Parliamentary Assembly
Assemblée parlementaire
http://assembly.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Déclassifié*
AS/Jur (2014) 02
23 janvier 2014
fjdoc02 2014

Commission des questions juridiques et des droits de l'homme

« Les opérations massives de surveillance en Europe » et « Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte »

Note introductive

Rapporteur : M. Pieter Omtzigt, Pays-Bas, Groupe du Parti populaire européen

1. Introduction

1. 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 massives de surveillance en Europe »[1] et le « Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte »[2]. Afin de commencer à travailler sur ces importants sujets le plus tôt possible, j'ai demandé à la commission, au cours de la même réunion, l'autorisation d'inviter à Strasbourg le donneur d'alerte qui a révélé l'existence d'opérations de surveillance à grande échelle, Edward Snowden, pour qu'il soit auditionné par la commission lors de la partie de session de janvier 2014 de l'Assemblée. À la suite d'un tour de table stimulant, la commission m'a invité à présenter tout d'abord l'habituelle « note introductive », qui expose l'étendue du/des futur(s) rapport(s), la situation actuelle et la méthode d'établissement des faits qui sera employée pour l'élaboration du rapport. La présente note vise à répondre à cette demande et à servir de socle à l'approfondissement de l'examen de la question. Je traiterai ici de la première phase de mes deux mandats de rapporteur, en présentant comment je conçois l'étendue de ces deux mandats, en procédant à un premier examen des travaux antérieurs et actuels réalisés hors du Conseil de l'Europe sur ce sujet et en proposant des activités d'investigation pertinentes. Compte tenu du nombre et de l'importance des questions qui relèvent de ces deux mandats, je souhaite proposer à la commission de présenter de manière distincte deux rapports finaux et deux projets de résolution et/ou de recommandation pour les deux sujets. En d'autres termes, je propose de consacrer un rapport à chaque sujet.

2. Les opérations massives de surveillance et les donneurs d'alerte, deux sujets réunis en une seule et même personne : Edward Snowden

2. L'action menée par M. Snowden a été à l'évidence importante pour ces deux sujets : il a divulgué des informations précises sur les opérations massives de surveillance menées par l'Agence nationale de sécurité (NSA) et d'autres organismes, provoquant ainsi un gigantesque débat public sur le respect de la vie privée à l'ère d'internet. Parallèlement, la manière dont il a divulgué ces informations a également ravivé le débat sur la protection des donneurs d'alerte. Cela dit, je partage le point de vue de la majorité des orateurs qui sont intervenus lors de notre premier tour de table le 6 novembre 2013 : aucun de ces deux sujets n'a vocation de donner lieu à un rapport consacré à la personne même de M. Snowden. Mais nous ne pouvons pas ignorer le fait que ce sont les révélations de M. Snowden qui ont provoqué le débat public sur la protection de la vie privée auquel nous avons

* Document déclassifié par la commission le 28 janvier 2014.
[1] Proposition de résolution, doc. 13288 du 6 août 2013.
[2] Proposition de résolution, doc. 13278 du 5 juillet 2013.

l'intention de participer dans le premier rapport et que son cas offre un exemple particulièrement intéressant de mise en balance des intérêts qui fondent les principes applicables à la protection des donneurs d'alerte, que nous examinerons dans le deuxième rapport.

3. La portée des futurs rapports

3.1. Les opérations massives de surveillance

3.1.1. Vue d'ensemble

3. Pour le titre de notre premier sujet je propose de garder le titre actuel en français : « opérations massives de surveillance ». Celui-ci décrit de manière neutre l'activité que nous avons l'intention d'examiner. [note du secrétariat : le Rapporteur propose, par contre, de changer le titre en anglais de « Massive Eavesdropping » à « Mass Surveillance » car le titre actuel a une connotation péjorative et polémique.]

4. À cet égard, j'aimerais tout d'abord présenter les informations disponibles sur l'étendue et la nature de la surveillance dont font l'objet tous les utilisateurs des moyens de communication modernes que nous sommes, comme les téléphones portables, les courriers électroniques et les réseaux sociaux. Une bonne partie de ces informations figure déjà dans le domaine public, à la suite des révélations de M. Snowden[3]. Des précisions supplémentaires, par exemple sur l'étendue de la coopération entre la NSA et ses homologues européens, continuent à être portées à notre connaissance[4].

5. J'aimerais ensuite examiner les conséquences de ces opérations massives de surveillance, de deux points de vue :

(1) du point de vue des droits de l'homme : l'incidence des opérations massives de surveillance sur les droits et libertés protégés par la Convention européenne des droits de l'homme
(2) du point de vue de la coopération internationale (notamment le partenariat transatlantique entre les États-Unis et ses alliés européens).

6. Enfin et surtout, j'aimerais réfléchir aux solutions qui permettraient de minimiser les conséquences négatives des opérations massives de surveillance et à la contribution que le Conseil de l'Europe serait en mesure d'apporter à cet effet.

7. Il s'agit d'un projet ambitieux et, compte tenu des ressources limitées dont dispose l'Assemblée, j'ai l'intention de faire le meilleur usage possible de l'expertise disponible et des travaux déjà réalisés, notamment à l'échelon de l'Union européenne (Parlement européen et Commission européenne).

3.1.2. Informations sur la nature et l'étendue des opérations massives de surveillance

8. La surveillance, envisagée comme un outil répressif et un instrument de renseignement, a été utilisée pour déceler et mettre en lumière les criminels ordinaires et les menaces qui pèsent sur la sécurité nationale. Ces menaces sont bien réelles et l'interception des communications (SIGINT, selon l'abréviation de l'OTAN) est un instrument précieux dont disposent les services répressifs et de sécurité. Mais au fil du temps, la nature de cette surveillance a évolué : la surveillance des communications visait au départ des suspects précis. Sa mise en place exigeait la prise d'une ordonnance judiciaire, fondée sur des motifs concrets et personnalisés de soupçon ; elle était uniquement utilisée lorsqu'il s'avérait indispensable de mettre un suspect en pleine lumière et à condition que l'atteinte au respect de la vie privée soit proportionnée à la gravité de l'infraction supposée ou du but poursuivi par l'activité de renseignement. Elle ne concernait que les tiers qui communiquaient avec le suspect. Aujourd'hui, dans les pratiques concrètes révélées par M. Snowden, d'énormes quantités de communications émises par des millions de personnes sont interceptées et conservées ; ce n'est qu'ensuite que la base de données ainsi constituée donne lieu à une recherche

[3] Voir : http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[4] Selon Alan Rusbridger, rédacteur en chef du Guardian, seul 1 % des 58 000 dossiers communiqués par M. Snowden ont été publiés à ce jour. Interrogé par la commission restreinte des affaires intérieures de la Chambre des communes du Royaume-Uni, qui lui demandait si 1 % des dossiers avait été publié, M. Rusbridger aurait répondu : « Ce chiffre est à peu près exact. Nous continuons à publier ces documents, qui représentent environ 1 % des informations qui nous ont été communiquées » (cf. http://uk.news.yahoo.com/mps-quiz-guardian-editor-snowden-030446879.html).

d'informations liées à un suspect particulier, sans que soient mis en balance, d'une part, les avantages que cette méthode présente pour les buts légitimes poursuivis et, d'autre part, les inconvénients qu'elle entraîne sous la forme d'une atteinte à la vie privée de millions de personnes innocentes. Cette évolution s'est produite dans la plupart des pays[5] sans qu'un véritable débat public n'ait eu lieu.

9. En résumé, les informations suivantes sur l'étendue des opérations massives de surveillance figurent désormais dans le domaine public :

3.1.2.1. Les « métadonnées »

10. 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[6] 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 ». Les « métadonnées » sont une présentation concise et condensée des communications interceptées ; elles comportent 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.

3.1.2.2. La collecte de données d'amont : BLARNEY, FAIRVIEW, OAKSTAR et STORMBREW

11. Une bonne part du flux des communications passe par les États-Unis ou par le Royaume-Uni, leur fidèle allié. La NSA, forte de l'avantage que lui procure la possibilité d'agir sur son propre terrain, peut ainsi intercepter le flux des communications qui aboutissent aux États-Unis ou les traversent. Les documents communiqués par M. Snowden montrent que les programmes de surveillance respectifs (dont les noms de code sont énumérés ci-dessus) fonctionnent au moyen de « partenariats » mis en place avec les principales sociétés américaines de télécoms et d'internet, dont certains ont été conclus il y a plusieurs dizaines d'années. Au sein de la NSA, la division chargée des programmes de collecte de données par l'intermédiaire de sociétés privées est la Special Source Operations (SSO), qui est qualifiée de « joyaux de la couronne » de la NSA dans les documents divulgués par M. Snowden.

3.1.2.3. Au Royaume-Uni également : le programme TEMPORA du GCHQ

12. Les documents Snowden ont également révélé l'existence du programme TEMPORA, mis en place en 2011 par le GCHQ (Government Communications Headquarters – Direction gouvernementale des communications), qui intercepte une très grande quantité de communications internet et téléphoniques en accédant au réseau câblé de fibres optiques. Le GCHQ partage la plupart de ces informations avec la NSA.

---

[5] À l'exception notamment de l'Allemagne, où une loi qui élargissait le champ d'application de la surveillance (« Grosser Lauschangriff ») a entraîné la démission en 1995 de la ministre fédérale de la Justice de l'époque, Sabine Leutheusser-Schnarrenberger ; cette dernière a ensuite contesté ce texte devant la Cour constitutionnelle fédérale, qui lui a donné raison (lien vers l'arrêt en allemand : https://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html). Mme Leutheusser-Schnarrenberger est devenue une nouvelle fois ministre fédérale de la Justice en 2009 et a entravé, grâce à ses nouvelles fonctions, la transposition par l'Allemagne de la directive sur la conservation des données des communications sans motif de soupçon. Le scandale de la NSA a également représenté l'un des grands thèmes abordés à l'occasion de la récente campagne électorale en Allemagne ; la révélation de la surveillance, par la NSA, du propre téléphone portable de la chancelière a indigné l'opinion publique et jusqu'aux responsables politiques conservateurs et aux commentateurs, qui avaient jusqu'ici montré peu d'intérêt pour les questions relatives à la protection des données (voir par exemple http://www.washingtonpost.com/blogs/worldviews/wp/2013/10/23/obamas-phone-call-with-angela-merkel-sounds-like-it-was-horribly-awkward/; http://www.spiegel.de/politik/deutschland/merkel-verlangt-von-usa-aufklaerung-der-nsa-affaere-a-934229.html; http://www.focus.de/politik/ausland/spaehaffaere-merkel-weitet-sich-aus-nsa-dementiert-obama-sprach-mit-nsa-chef-alexander-nie-ueber-merkel-ausspaehung_aid_1141205.html).

[6] Par exemple la sénatrice américaine Dianne Feinstein, présidente de la commission du renseignement du Sénat (citée par USA Today http://www.usatoday.com/story/opinion/2013/10/20/nsa-call-records-program-sen-dianne-feinstein-editorials-debates/3112715/).

3.1.2.4. « Five Eyes » et au-delà : un partenariat de confiance pour la mise en commun des activités de renseignement

13. L'alliance de mise en commun des activités de renseignement, « Five-Eyes » (qui regroupe les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et le Canada), fondée sur l'accord de renseignement sur les transmissions Royaume-Uni-États-Unis de 1946, prévoit que les services de renseignement alliés n'espionnent pas les citoyens de l'un de leur partenaire sans son autorisation. Celle-ci se limite en règle générale aux personnes soupçonnées d'avoir commis des actes répréhensibles. Un accord secret passé en 2007 entre les États-Unis et le Royaume-Uni (d'après les documents divulgués par M. Snowden[7]) a modifié ce principe : il autorise la NSA à analyser et à conserver tout numéro de téléphone mobile et de fax, tout courrier électronique et toute adresse IP pris dans ses « filets ». La NSA a la possibilité de rechercher des informations en remontant jusqu'à une distance de trois correspondants successifs depuis la cible visée, c'est-à-dire d'examiner les communications d'un ami d'un ami d'un ami[8]. Auparavant, ce type de prise accessoire (c'est-à-dire la collecte fortuite de données relatives à des personnes qui n'étaient pas au départ la cible de l'opération de surveillance et n'étaient par conséquent pas soupçonnées d'avoir commis des actes répréhensibles) devait être supprimée des bases de données de la NSA (« réduite »).

14. Un projet (distinct) de note communiqué par M. Snowden, intitulé « Collecte, traitement et diffusion des communications alliées » (*Collection, Processing and Dissemination of Allied Communications*), présente différents niveaux de classification pour chaque paragraphe. 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 États-Unis et leur sécurité nationale le commande ». Le document divulgué n'indique pas, et les hauts responsables contactés par « The Guardian » n'ont pas davantage précisé, si ce projet de note avait été effectivement mis en œuvre. Mais les révélations de M. Snowden ont permis d'apprendre que les communications des dirigeants de pays traditionnellement alliés des Américains, comme la chancelière Angela Merkel, étaient bel et bien interceptées[9].

3.1.2.5. Collecte des données descendantes : le programme PRISM de la NSA

15. PRISM, d'après les documents transmis par M. Snowden, est le plus gros contributeur individuel des rapports de renseignement de la NSA ; il s'agit d'un programme de collecte des « données descendantes », ce qui signifie que la NSA recueille les données provenant des sociétés internet américaines comme Google, Facebook, Apple, Yahoo et d'autres encore. Lorsque « The Guardian » et le « Washington Post » ont révélé l'existence de PRISM, les sociétés concernées ont nié avoir la moindre connaissance de ce programme et ont insisté sur le fait qu'elles étaient tenues par la législation de coopérer avec les services de renseignements. Le site Web précité du « Guardian »[10] comporte un document divulgué, qui révèle le nombre de dossiers de renseignement générés par chaque société (Yahoo y occupe la première place, suivie par Microsoft et Google, pour la période de juin à juillet 2010).

[7] Voir James Ball, "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data", The Guardian, 20 novembre 2013.

[8] Selon l'analyse du Guardian, cette extension de la collecte d'informations à une distance de trois correspondants successifs d'un usager classique de Facebook permettrait de récolter les données de plus de 5 millions de personnes.

[9] Voir plus haut la note de bas de page n° 5.

[10] Voir plus haut la note de bas de page n° 3.

3.1.2.6. « Force brute », « trappes », « cheval de Troie » et matériel informatique trafiqué : comment la NSA et le GCHQ font fi du respect de la vie privée et de la sécurité sur internet[11]

16. D'après les documents transmis par M. Snowden et révélés par « The Guardian » et d'autres organes de presse, la NSA et le GCHQ sont parvenus à contourner les systèmes de cryptage auxquels les utilisateurs d'internet ont recours pour protéger leurs données à caractère personnel, leurs transactions en ligne et leurs échanges de courriers électroniques. Pour ce faire, 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 superordinateurs 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. D'après les documents divulgués, un programme anti-cryptage de la NSA a fait en 2010 une découverte capitale, qui lui a permis d'exploiter une « immense quantité » de données collectées par l'intermédiaire des prises de distribution internet. Le document divulgué qualifie les consommateurs « d'adversaires » : il fait remarquer que « les modifications apportées sur le plan de la conception rendent les systèmes en question exploitables, grâce à la collecte opérée par les activités de renseignement sur les transmissions […]. Mais la sécurité du système demeure intacte pour le consommateur et les autres adversaires ». Les sociétés expertes en technologie insistent sur le fait qu'elles collaborent avec les services de renseignements uniquement lorsqu'elles y sont contraintes par la législation[12]. D'après les informations transmises à « The Guardian », le montant total des dépenses occasionnées depuis 2011 par les activités de renseignement sur les transmissions atteint 800 millions USD. En comparaison, PRISM s'avère économique, puisqu'il coûte 20 millions USD par an.

17. M. Snowden a également révélé (par l'intermédiaire du « Washington Post »[13]) un autre programme de la NSA, intitulé GENIUS et géré par une de ses unités, la TAO (Tailored Access Operations) : il consiste à implanter un logiciel dirigé de l'extérieur pour copier des données ou infecter un système informatique. Il pourrait être utilisé, par exemple, pour télécharger des documents compromettants sur l'ordinateur d'une cible, sans laisser la moindre trace. D'après le « Washington Post », au moins 85 000 systèmes informatiques du monde entier seront convertis pour constituer une sorte de « réseau de robots » au service de la NSA, pilotés par un système automatisé, qui a pour nom de code TURBINE. Selon les documents divulgués, « seuls 8448 » des 60 000 systèmes informatiques infiltrés en 2011 ont pu être pleinement exploités, en raison des effectifs limités dont dispose la NSA, bien que 1870 personnes aient été affectées à ce projet à l'époque.

18. Enfin et surtout, les révélations ont permis d'apprendre fin 2013 que la NSA interceptait également le matériel informatique expédié par les fabricants à des « cibles » et qu'elle le trafiquait pendant ce transit, en y incorporant des logiciels malveillants. Il s'agit d'une menace particulièrement grave pour la vie privée et la sécurité des données, puisque, comme me l'a indiqué un expert en la matière, il n'existe aujourd'hui aucun outil permettant de déceler ces modifications.

3.1.2.7. La géolocalisation de centaines de millions de téléphones portables

19. D'après les documents divulgués par M. Snowden et publiés par le Washington Post le 4 décembre 2013[14], la NSA conserve les données relatives à des centaines de millions de téléphones portables dans le monde entier et stocke environ 5 milliards de séries de données de localisation par jour. Ce système fonctionne même lorsque le GPS d'un smart phone est éteint, en suivant le déplacement du téléphone d'une station cellulaire (l'émetteur local) à une autre. La NSA collecte ces données relatives à la localisation et aux habitudes de déplacement pour « exploiter les cibles », c'est-à-dire pour découvrir les acolytes encore inconnus de « cibles » qu'elle connaît déjà (ceux qui les accompagnent dans leurs déplacements). Selon le Washington Post, les autorités ont déclaré qu'elles ne collectaient pas délibérément les données de géolocalisation des téléphones portables américains en vrac ; celles-ci sont recueillies de manière incidente. La collecte en vrac des données de géolocalisation des utilisateurs de téléphone portable s'effectue en amont (voir plus haut le point

[11] Voir The Guardian du 6 septembre 2013, "Revealed: how US and UK spy agencies defeat internet privacy and security".
[12] Microsoft chercherait à présent à échapper à cette « obligation de coopération » en saisissant à cet effet les juridictions américaines (voir DIE WELT du 5 décembre 2013, *Microsoft zieht gegen die NSA vor Gericht*).
[13] Voir le Washington Post du 30 août 2013, "US spy agencies mounted 231 offensive cyber operations in 2011 documents show".
[14] Voir le Washington Post du 4 décembre 2013, "NSA tracking cellphone locations worldwide Snowden documents show"

3.1.2.2.), en mettant sur écoute les réseaux téléphoniques des grands fournisseurs de télécommunications.

3.1.2.8. L'observation, par la NSA, de la fréquentation des sites Web pornographiques par les islamistes

20. Un document d'octobre 2012 divulgué par M. Snowden[15] évoque la surveillance de six musulmans, considérés par la NSA comme des islamistes dont le discours incite à la haine ; il explique de quelle manière les « faiblesses personnelles » d'un individu peuvent être décelées par sa mise sous surveillance numérique et utilisées pour nuire à sa crédibilité et à sa réputation.

21. Ce qui m'inquiète le plus, c'est le fait que ces outils (ou ceux que le programme GENIUS permet d'utiliser[16]) peuvent également servir à nuire, par exemple, à des opposants politiques, à des militants des droits de l'homme ou à des journalistes. Jusqu'à ces derniers temps, le caractère acceptable ou non des opérations massives de surveillance et leur étendue n'avaient guère fait l'objet d'un débat public dans un quelconque pays. Ce débat est désormais plus qu'indispensable et il devrait se tenir sur la base des informations publiquement disponibles.

3.1.2.9. L'infiltration par la NSA des jeux vidéo en ligne

22. D'après les documents révélés par M. Snowden[17], des agents américains et britanniques ont infiltré des jeux en ligne tels que « World of Warcraft » et « Second Life ». Dans un document de 2008 intitulé « L'exploitation de l'utilisation par les terroristes des jeux et des environnements virtuels », la NSA présente les jeux en ligne comme des « réseaux de communication qui regorgent de cibles » et que fréquentent les terroristes et les criminels. Ces listes peuvent fournir des métadonnées potentiellement intéressantes, comme des « listes d'amis », des photos et des données de géolocalisation. Mais sur quelles personnes ? Des adolescents passionnés de jeux vidéo ? Doivent-ils redouter à présent que l'elfe ou l'ork qu'ils combattent à l'écran soit en réalité un agent secret chargé de recueillir des données ou de recruter des informateurs[18] ? Je n'étais pas sûr de devoir faire figurer ces informations dans le présent document, car elles risquaient de faire oublier l'extrême gravité des autres atteintes à la vie privée de chacun d'entre nous. Mais cet exemple témoigne de la détermination de la NSA à tout infiltrer de manière systématique.

3.1.3. Quelques réactions provoquées à ce jour par les révélations sur les opérations massives de surveillance

23. Le débat provoqué par ces révélations se poursuit. Elles ont entraîné un grand nombre de réactions négatives de la part des citoyens et des hauts responsables politiques. Ces derniers ont été particulièrement indignés d'apprendre qu'ils faisaient eux aussi l'objet de cette surveillance. La déception causée par cet « espionnage entre amis », qui a été formulée de la façon la plus mordante par Angela Merkel[19], a profondément affecté les rapports de confiance mutuelle.

24. Le 10 juillet 2013, la commission des libertés civiles (LIBE) du Parlement européen a lancé une vaste « enquête approfondie sur les programmes de surveillance américains »[20]. Elle a procédé à ce jour à 11 auditions d'experts et de militants et aurait également[21] décidé d'auditionner M. Snowden lui-

[15] Voir le Huffington Post du 26 novembre 2013 : "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'" ; BBC news du 27 novembre 2013, « NSA planned to discredit radicals over web-porn use »; Spiegel online 27 novembre 2013 : « NSA beobachtet Porno-Nutzung islamischer Zielpersonen ».

[16] Voir plus haut le point 3.1.2.6.

[17] Voir http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life (publiés simultanément le 9 décembre 2013 par « The Guardian » et le « New York Times »).

[18] Je simplifie sans doute à outrance la situation, car il est peu probable que des agents participant à ce type de surveillance se mettent réellement à « jouer » ou à utiliser l'interface normale des jeux, car la surveillance de l'historique des échanges et des dialogues en ligne n'exige aucune interaction graphique. Un expert que j'ai consulté m'a par ailleurs indiqué que la surveillance des échanges effectués sur des jeux de type « SecondLife » par les services répressifs pouvait fort bien représenter un moyen justifié et efficace de restreindre le blanchiment de capitaux réalisé par la criminalité organisée grâce à l'échange de biens virtuels.

[19] Voir par exemple le communiqué de l'AFP du 18 novembre 2013, « Merkel urges explanation over 'grave' US spy claims ».

[20] Voir http://www.europarl.europa.eu/news/fr/news-room/content/20130701IPR14770/html/Une-engu%C3%AAte-approfondie-sur-les-programmes-de-surveillance-am%C3%A9ricains.

[21] The Guardian du 8 décembre 2013, "Edward Snowden to give evidence to EU parliament, says MEP". Mais aucun accord n'a encore été trouvé sur la forme que pourrait prendre cette audition, ce qui explique pourquoi elle

même. Le 18 décembre 2013, la commission LIBE a présenté ses conclusions préliminaires, rédigées par Claude Moraes (Royaume-Uni, S&D)[22]. Ses conclusions préliminaires préconisent de consentir à un accord commercial avec les États-Unis uniquement si celui-ci ne mentionne pas la protection des données, en suspendant l'accord sur la sphère de sécurité (les normes relatives à la protection des données que les sociétés américaines sont tenues de respecter lors du transfert des données relatives aux citoyens de l'UE) et le programme de surveillance du financement du terrorisme (Terrorist Finance Tracking Programme – TFTP), en vue de renégocier des normes plus adaptées en matière de protection des données ; elles invitent également à la création d'un espace de stockage en ligne (« cloud ») des données de l'UE. En parallèle, la Commission européenne a également entamé un dialogue avec les autorités américaines[23].

25. Un projet de résolution de l'Assemblée générale des Nations Unies, qui critiquait les opérations de surveillance à grande échelle des communications en ligne, a été déposé conjointement par l'Allemagne et le Brésil et adopté à l'unanimité par la commission compétente le 26 novembre 2013[24], non sans avoir été au préalable considérablement édulcoré sous la pression des États-Unis et des autres membres de l'alliance « Five Eyes ». Il est intéressant de constater qu'à ce jour

> « la plupart des gouvernements ont réagi en se montrant critique à l'égard de Washington et de Londres et ont demandé qu'il soit mis fin à leur surveillance. Mais rares sont ceux qui ont cité en exemple leur propre système »[25].

26. Une partie de la société civile s'est également mobilisée. Pour les militants de la liberté d'internet et les donneurs d'alerte, Edward Snowden est un héros. Dans une « lettre ouverte aux agents des services de renseignements qui recherchent Snowden »[26], de célèbres donneurs d'alerte invitent instamment les fonctionnaires à écouter leur conscience et à rejoindre Edward Snowden, en œuvrant pour que « les responsables politiques qui se conduisent en escrocs aient à répondre de leurs actes ». Parmi les signataires figurent Daniel Ellsberg, qui, après avoir divulgué les « documents du Pentagone », a été poursuivi sans succès pour trahison et passe généralement aujourd'hui pour avoir contribué à écourter la guerre du Vietnam[27]. Par ailleurs, le 10 décembre 2013, 560 auteurs du monde entier, dont cinq lauréats du prix Nobel, ont lancé un appel contre les opérations de surveillance à grande échelle d'internet et en faveur d'une « Charte des droits numériques »[28].

27. Le scandale de la NSA a également porté atteinte à la réputation des géants d'internet dont le siège est aux États-Unis, comme Microsoft, Cisco et Google. Les révélations de M. Snowden montrent en effet leur connivence volontaire ou contrainte avec la NSA, à laquelle ils ont permis d'accéder aux données relatives à leurs clients, voire de porter atteinte aux mesures de sécurité des données commerciales. D'après une étude réalisée par l'Information Technology & Innovation Foundation de Washington, D.C., les révélations de M. Snowden pourraient coûter jusqu'à 35 milliards USD de perte de chiffre d'affaires aux sociétés américaines[29]. Les sociétés américaines de technologie n'ont peut-être pas été trop concernées par les problèmes d'atteinte à la vie privée relatifs à leurs données commerciales, mais leur image publique en Europe et dans le reste du monde a considérablement souffert des révélations de M. Snowden[30]. Lorsque les autorités de Washington cherchent à justifier les programmes de la NSA, en expliquant que ceux-ci visent uniquement les pays étrangers, cela ne rend pas service aux multinationales, qui font à présent pression pour obtenir une réforme des services secrets[31]. Leurs concurrents étrangers encouragent le nationalisme économique pour tirer

---

n'aura pas lieu avant la fin 2013, comme cela avait été initialement prévu (voir http://www.welt.de/politik/ausland/article122863850/Snowden-Anhoerung-vor-EU-Parlament-geplatzt.html?config=print#).

[22] Voir le communiqué de presse du 18 décembre 2000 : Enquête sur la NSA: présentation des premières conclusions.

[23] Voir par exemple l'article du magazine Le Point du 19 novembre 2013 : « Surveillance de la NSA : rencontre "constructive" entre UE et Etats-Unis ».

[24] Voir par exemple l'article du « Süddeutsche Zeitung » du 26 novembre 2013 : « Deutsche UN-Resolution gegen Spionage einstimmig verabschiedet ».

[25] 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 (page 9).

[26] « The Guardian », 11 décembre 2013 : Former whistleblowers: open letter to intelligence employees after Snowden.

[27] Voir par exemple la description détaillée disponible sur : http://law2.umkc.edu/faculty/projects/ftrials/ellsberg/ellsberghome.html.

[28] Voir http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3.

[29] Voir DIE WELT du 27 novembre 2013, "NSA-Skandal kostet die USA bis zu 35 Milliarden Dollar".

[30] Voir Mascolo et Scott (ibid.), page 11.

[31] Voir DIE WELT du 18 décembre 2013 : "Internet-Bosse fordern Reform der Geheimdienste".

profit des craintes de l'opinion publique à l'égard des sociétés technologiques qui ont leur siège aux États-Unis et qui représentent une menace pour la vie privée de leurs clients[32]. Comme nous le verrons, cette situation risque fort d'être préjudiciable non seulement aux acteurs américains, mais également à la viabilité future d'internet tel que nous le connaissons aujourd'hui, rien de moins !

28. Après avoir passé en revue les premières réactions du monde politique, de la société civile et des milieux économiques aux révélations résumées plus haut, j'aimerais à présent commencer à réfléchir à la réponse que le Conseil de l'Europe pourrait donner à ces opérations de surveillance à grande échelle.

3.1.4. Contribution à une réponse du Conseil aux opérations massives de surveillance

29. En sa qualité de « première organisation européenne de protection des droits de l'homme »[33], le Conseil de l'Europe devrait aborder les opérations massives de surveillance sous l'angle des droits de l'homme. Cette plate-forme de dialogue et de coopération en Europe devrait également se soucier de l'incidence des opérations de surveillance à grande échelle sur la coopération internationale à l'ère d'internet.

3.1.4.1. Les opérations massives de surveillance envisagée sous l'angle des droits de l'homme

30. Toute surveillance des communications constitue a priori une atteinte à l'article 8 de la Convention européenne des droits de l'homme :

> « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » (article 8, paragraphe 1, de la Convention européenne des droits de l'homme).

31. Il ne fait guère de doute que le terme « correspondance » englobe également les moyens électroniques de communication, dont l'interception peut porter atteinte au respect de la « vie privée » de la même manière que l'interception du courrier, dont la confidentialité jouit d'une protection minutieuse, y compris dans les constitutions et les codes pénaux nationaux. L'évolution de la technologie de la transmission des messages ne saurait avoir pour conséquence légale de restreindre la protection de la vie privée.

32. L'article 8, paragraphe 2, prévoit une importante exception à la protection de la vie privée :

> « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

33. Cette exception prend évidemment en compte la forme originale de la surveillance, c'est-à-dire une surveillance autorisée par une ordonnance judiciaire, fondée sur des éléments de preuve et prise à l'encontre d'un suspect. Mais dans quelle mesure autorise-t-elle également les opérations massives de surveillance, décidées sans ordonnance judiciaire et même sans motif de soupçon à l'égard de « cibles » multiples ?

34. La jurisprudence de la Cour européenne des droits de l'homme (« la Cour ») semble jusqu'ici s'être montrée relativement protectrice des droits relatifs à la vie privée. Dans l'affaire de référence *Klass et autres c. Allemagne*[34], la Cour a estimé que

> « Caractéristique de l'États policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques. […] En évaluant l'étendue de la sauvegarde offerte par l'article 8 la Cour ne peut que constater deux faits importants : les progrès techniques réalisés en matière d'espionnage et parallèlement de surveillance ; en second lieu, le développement du terrorisme en Europe au cours des dernières années. Les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que

[32] Voir par exemple DIE ZEIT en ligne, 11 novembre 2013, "Ein Schlandnet würde nur der Telekom nützen",
[33] Voir le Washington Post du 4 novembre 2005 "US faces scrutiny over secret prisons",
[34] Requête n° 5029/71, arrêt de la Cour plénière du 6 septembre 1978.

> l'États 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 (§42, 48).

35. S'agissant des conditions de cette surveillance, la Cour accorde aux États membres une marge d'appréciation étendue. Mais la Cour souligne que

> « les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. […] Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple 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 (§49, 50).

36. Lorsqu'elle a rendu cet arrêt en 1978, la Cour ne pouvait pas même imaginer les progrès technologiques qui permettraient un jour de parvenir à l'étendue actuelle de la surveillance qui nous occupe ici. Entre-temps, elle a eu l'occasion de préciser plus en détail les conditions dans lesquelles elle juge les mesures de surveillance acceptables au regard de la Convention.

37. Dans l'arrêt *Kruslin c. France*[35], la Cour a conclu à la violation de l'article 8 parce que la législation française qui régissait la mise sur écoute des lignes téléphoniques n'était pas suffisamment « prévisible », dans la mesure où elle ne définissait pas les catégories de personnes susceptibles de voir leur téléphone placé sur écoute par ordonnance judiciaire ni la nature des infractions qui pouvaient donner lieu à ce type d'ordonnance.

38. Dans l'arrêt *Halford c. Royaume-Uni*[36], la Cour a réaffirmé que les notions de « vie privée » et de « correspondance » de l'article 8 pouvaient englober les appels téléphoniques effectués depuis les locaux professionnels et le domicile. Elle a conclu à une violation, considérant que les appels internes effectués au sein de la direction de la police avaient été interceptés sans fondement légal.

39. Dans l'arrêt *Lambert c. France*[37], la Cour a conclu à la violation de l'article 8 parce que le requérant s'était vu refuser la possibilité de contester la manière dont la durée de la surveillance de la ligne téléphonique d'un tiers avait été prolongée. L'argument de la Cour est particulièrement intéressant pour le domaine qui nous occupe :

> « [ce raisonnement] pourrait conduire à des décisions privant de la protection de la loi un nombre très important de personnes, à savoir toutes celles qui conversent sur une autre ligne téléphonique que la leur. Cela reviendrait d'ailleurs, en pratique, à vider le mécanisme protecteur d'une large partie de sa substance » (§38).

40. Cet argumentaire semble s'appliquer mieux encore aux opérations massives de surveillance divulguées par M. Snowden.

41. Dans l'arrêt *Amann c. Suisse*[38], la Cour a conclu à la violation de l'article 8 dans la mesure où, d'une part, l'interception d'un appel téléphonique n'était pas prévue par une loi qui satisfaisait à l'exigence de prévisibilité et, d'autre part, le gouvernement n'était pas en mesure de démontrer que les garanties prévues par la loi avaient été respectées. Cette affaire est, elle aussi, particulièrement intéressante pour nous, puisque le requérant a fait par hasard l'objet d'une surveillance : il avait été intégré dans une base de données destinée aux opérations de surveillance de la lutte contre l'espionnage parce qu'une femme de l'ambassade soviétique de Berne l'avait appelé pour commander un appareil qu'il mettait en vente. On peut dire qu'en matière d'opérations massives de surveillance, l'immense majorité des personnes dont les communications sont interceptées par les « filets » de surveillance actuels finissent par être intégrées dans une base de données de manière fortuite, de la même manière que M. Amann, sous forme de prise accessoire.

[35] Requête n° 11801/85, arrêt du 24 avril 1990.
[36] Requête n° 20605/92, arrêt du 25 juin 1997.
[37] Requête n° 23618/94, arrêt du 24 août 1998.
[38] Requête n° 27798/95, arrêt du 16 février 2000.

42. Dans l'arrêt *Copland c. Royaume-Uni*[39], la Cour a précisé que la correspondance électronique et l'utilisation d'internet relevaient du champ d'application de l'article 8, au même titre que les communications téléphoniques ou postales. La Cour a conclu à une violation sans juger pertinent que les données obtenues n'aient pas été communiquées à des tiers ni utilisées d'une quelconque façon contre la requérante. Il est intéressant de noter, pour ce qui nous occupe, que, selon la Cour, la simple

> « collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressée au respect de sa vie privée et de sa correspondance » (§ 44).

43. En l'absence de toute législation interne régissant la surveillance à l'époque des faits, cette ingérence n'était pas « prévue par la loi ».

44. L'affaire *Liberty et autres c. Royaume-Uni*[40] porte sur l'interception des communications à destination ou en provenance de l'étranger des organisations de défense des libertés civiles par le ministère de la Défense. La loi relative à l'interception des communications de 1985 autorise les mandats d'interception des communications (intérieures ou à destination ou en provenance de l'étranger) liées à une adresse ou à une personne précise ou des communications (à destination ou en provenance de l'étranger) en général, sans restriction à l'égard des personnes ou des locaux concernés. La loi impose au secrétaire d'État de prendre les mesures qu'il juge nécessaires pour assurer l'existence de garanties contre les abus de pouvoir et institue une commission spéciale habilitée à enquêter sur les plaintes en la matière et un commissaire chargé de signaler ce type de situation et doté de pouvoirs de contrôle. Le détail précis des « garanties » n'était pas divulgué pour des raisons de sécurité nationale. La Cour a conclu à la violation de l'article 8 parce que la loi accordait aux autorités britanniques une « latitude pratiquement illimitée pour capter des communications transmises entre le Royaume-Uni et une personne se trouvant à l'étranger » et que « n'importe quelle communication à destination ou en provenance de l'étranger pouvait en théorie faire l'objet d'une interception », tandis que la nature des « mesures » destinées à prévenir les abus « n'était pas précisé[e] par la loi ou rendu[e] public d'une autre manière ».

45. L'affaire ultérieure *Kennedy c. Royaume-Uni*[41] porte sur la proportionnalité et les garanties de la législation britannique en matière d'interception des communications intérieures (nationales). La Cour a conclu à l'absence de violation de la Convention parce que « la législation sur laquelle repose le régime prévoyait un certain nombre de garanties pour la protection de toute donnée obtenue » et que « le régime était soumis au contrôle d'une instance qui jouissait d'un degré d'indépendance satisfaisant et de compétences suffisantes ». Cet arrêt ou, plus précisément, le régime légal de surveillance des communications internes au en vigueur Royaume-Uni en 2005 peut tenir lieu d'exemple à suivre : la législation prévoyait en effet des garanties spécifiques contre les abus et la création d'une instance de contrôle indépendante dotée de pouvoirs suffisants. J'ai l'intention d'examiner plus attentivement ce que cela signifie en pratique, dans le cadre de l'exercice ultérieur de mon mandat de rapporteur.

46. La Cour aura l'occasion de continuer à préciser sa jurisprudence dans un proche avenir, puisqu'au moins deux nouvelles requêtes ont été introduites devant elle : une ONG hongroise conteste la législation hongroise qui autorise les opérations secrètes de surveillance et de collecte des données par les services nationaux de sécurité sur simple autorisation ministérielle[42] ; trois ONG britanniques ont par ailleurs saisi la Cour de Strasbourg d'une requête contre la collecte d'une gigantesque quantité de données par le GCHQ du Royaume-Uni[43]. Dans l'intervalle, M. Bosjan Zupancic, juge à la Cour européenne des droits de l'homme au titre de la Slovénie, aurait affirmé à l'occasion d'une audition organisée par la commission d'enquête du Parlement européen sur l'affaire de la NSA que les opérations massives de surveillance sont inacceptables de manière générale et qu'elles peuvent donner lieu à des recours devant les tribunaux[44].

---

[39] Requête n° 62617/00, arrêt du 3 avril 2007.
[40] Requête n° 58243/00, arrêt du 1er juillet 2008.
[41] Requête n° 26839/05, arrêt du 18 mai 2010.
[42] Voir MTI-EcoNews/Hungary du 29 novembre 2013 : « NGO to turn to Strasbourg court over security services' secret surveillance ».
[43] Voir le Guardian du 3 octobre 2013 : "GCHQ faces legal challenge in European court over online privacy".
[44] Voir Heise en ligne du 15 octobre 2013 : « Rechtsexperten im EU-Parlament: NSA und GCHQ verletzen Menschenrechte und Souveränität ».

47. La légalité des opérations massives de surveillance en droit international des droits de l'homme est également examinée par la Commission interaméricaine des droits de l'homme, qui, en octobre 2013, a tenu une audition thématique sur « la liberté d'expression et la surveillance des communications par les États-Unis »[45].

48. Les juridictions auront à trancher une question essentielle : l'atteinte à la vie privée survient-elle au moment de la collecte ou de l'interception des données à caractère personnel ou lors de leur traitement ou de leur utilisation ? La technologie pourrait bien façonner l'approche retenue par les décideurs politiques. Un expert m'a en effet expliqué qu'il était généralement plus facile de filtrer les données transmises en temps réel à propos de cibles précises et de se contenter de conserver les données pertinentes. Le filtrage des données est plus rapide que leur stockage et il est plus facile de les filtrer sur leur lieu d'interception que de transmettre dans un premier temps l'ensemble des données recueillies vers leur lieu de stockage. Mais il n'est pas techniquement possible aujourd'hui de remonter le temps (par exemple de retrouver ce que les auteurs de l'attentat à la bombe de Boston faisaient en 2011 ou avec qui ils communiquaient avant d'apparaître sur le « radar »). Cette opération peut uniquement être effectuée une fois les données interceptées, conservées et consultables[46]. Pour que l'interception et le stockage à grande échelle des données puissent se faire en toute légalité, certains affirment que la « surveillance » (envisagée comme une atteinte à la vie privée) ne signifie plus la simple interception des données, mais uniquement leur traitement et leur utilisation effectifs. Faut-il admettre cette évolution comme une nécessité technique, indispensable à la lutte contre le terrorisme ? Ou s'agit-il d'un pas supplémentaire inacceptable sur un terrain glissant, qui nous mènera vers l'univers de *1984* de George Orwell[47] ? Dans la mesure où cette « pêche au chalut » et ce stockage de gigantesques quantités de données relatives à des personnes non suspectes sont effectivement pratiqués, peut-on au moins garantir que les données recueillies sous forme de « prise accessoire », qu'il est techniquement impossible d'éviter, soient rapidement effacées (« réduites », pour reprendre la terminologie de la NSA) ?

3.1.4.2. La question vue sous l'angle de la coopération internationale : les opérations massives de surveillance menacent la viabilité d'internet, comment y remédier ?

49. 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, pourquoi pas, de relations. Cette situation pourrait bien changer après les révélations de M. Snowden. L'une des réponses qui pourraient être apportées au sentiment de surveillance généralisée pratiquée par la NSA et d'autres organismes est celle de la « souveraineté technologique », notamment par une réglementation imposant que toutes les données conservées et traitées relatives aux consommateurs européens soient conservées et traitées en Europe, voire dans chaque pays concerné[48]. Il s'agirait à la fois d'une réaction politique face aux abus et d'un outil de commercialisation pour les entreprises européennes, comme nous l'avons vu. Mais cette situation 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[49]. Qui plus est, du point de vue du Conseil de l'Europe,

> « les objectifs de routage national ne vont pas dans le sens de la protection des droits civiques, mais plutôt dans le sens contraire. La localisation 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 »[50].

[45] Voir le témoignage d'Emi MacLean de l'Open Society Justice Initiative et d'Alex Abdo pour le compte de l'American Civil Liberties Union (ACLU), ainsi que les conclusions d'un groupe d'autres ONG (disponibles auprès du Secrétariat).
[46] Voir 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 (page 7).
[47] Voir Mascolo et Scott, ibid., page 7.
[48] Selon certaines informations, le ministre allemand de l'Intérieur, M. Friedrich, aurait suggéré aux citoyens inquiets de l'espionnage américain d'éviter les services internet qui transmettent des données par l'intermédiaire des réseaux américains. La chancelière, Mme Merkel, a évoqué une solution de routage exclusivement allemande (voir Mascolo et Scott, ibid., page 10). Le projet de conclusions de la commission LIBE du Parlement européen (voir plus haut la note 21) préconise également la création d'un « espace de stockage européen en ligne (« cloud ») des données ».
[49] Voir Mascolo et Scott, ibid., page 12.
[50] Mascolo et Scott, ibid., page 12.

50. Je partage totalement cette inquiétude. La « balkanisation d'internet »[51] ne semble pas une bonne solution. Je fais mienne la conclusion de Mascolo et Scott :

> « Compte tenu des risques encourus, il serait sage de rechercher énergiquement une solution politique, avant de retomber dans un nationalisme économique et technologique déployé pour faire face à la surveillance étrangère »[52].

51. L'autre solution préconisée à la suite des révélations de M. Snowden est celle de la négociation, tout au moins entre pays amis et alliés, d'accords de « non-espionnage »[53] et plus généralement de la mise en place d'un cadre juridique plus précis applicable aux activités de surveillance, à l'intérieur et à l'extérieur des frontières nationales. Ces solutions exigent à l'évidence, y compris de la part des usagers d'internet, un degré conséquent de confiance dans le fait qu'il s'agit d'accords que les signataires entendent sincèrement respecter et que chacun d'entre eux respectera effectivement.

52. Mais les actes dévoilés par les révélations de M. Snowden, et non ses révélations elles-mêmes, ont entraîné une grave perte de confiance, même entre pays « amis ». L'emballement de cette machine de surveillance est également dû au fait que les dirigeants politiques ont perdu le contrôle des activités des services de renseignements, 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 »[54]. Je ne veux 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 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[55]. À l'inverse, 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 États-Unis est inquiétant : depuis les débuts de la privatisation dans les années 1980, la population carcérale américaine a au moins triplé, tandis que le taux de criminalité a diminué[56]. La croissance « du complexe industriel de la surveillance » pourrait bien égaler, voire dépasser la « croissance du complexe carcéro-industriel »[57].

53. Les partisans d'un cryptage massif des données, destiné à faire face aux opérations massives de surveillance, insistent sur le fait que leur solution permettra de remporter la « course aux armements » contre la NSA et les autres organismes de ce type, en raison de « l'asymétrie » d'ordre technologique entre les modestes ressources nécessaires aux inventeurs de codes de cryptage et le

---

[51] Voir Eugene Kaspersky, "What will happen if countries carve up the internet?", in : The Guardian, 17 décembre 2013.

[52] Mascolo et Scott, ibid., page 12.

[53] Voir DIE WELT du 17 décembre 2013 : "Ein Abkommen wird NSA-Spionage nicht verhindern". En résumé, le New York Times avait indiqué que les autorités américaines refusaient de conclure un accord de « non-espionnage » avec l'Allemagne, comme cette dernière l'avait proposé, d'après ce que l'on peut déduire d'une réponse du gouvernement à une question parlementaire posée par le groupe du Parti social-démocrate du Bundestag (lien : http://www.welt.de/themen/bundesregierung). Berlin a réaffirmé que les négociations se poursuivaient. L'auteur de l'article met en doute la valeur de l'éventuel futur « mémorandum d'accord ». Il rappelle que dans un « mémorandum d'accord » conclu entre la NSA et le BND allemand le 28 avril 2002, la NSA s'était dite prête à respecter la législation allemande en matière de surveillance téléphonique et autre, alors qu'il s'est avéré que même le téléphone portable de la chancelière, Mme Merkel, était surveillé depuis des années.

[54] Voir Fred Kaplan, "James Clapper lied to Congress about NSA surveillance", 11 juin 2013.

[55] 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 (page 104).

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

[57] Voir John W. Whitehead, "Jailing Americans for profit: the rise of the prison industrial complex", Huffington Post, 4 octobre 2012.

coût considérable que suppose le décryptage d'un code relativement simple. Les militants du cryptage proposent de décentraliser internet, en allant bien au-delà d'une « balkanisation » pays par pays. Ils considèrent que la solution réside dans « l'atomisation » d'internet, dans laquelle chaque usager posséderait son propre serveur crypté. Aucun code connu ne peut résister à la « force brute », c'est-à-dire à l'utilisation massive de superordinateurs capables d'épuiser toutes les combinaisons, mais cette « force brute » entraîne une très forte consommation de ressources et peut par conséquent uniquement être employée contre un nombre limité de cibles soigneusement choisies, comme les terroristes, les marchands d'armes, les parrains de la mafia et d'autres individus du même type. Cette clientèle est précisément celle à laquelle la surveillance était autrefois réservée, autorisée par une ordonnance judiciaire prise sur la base de motifs de soupçon concrets. Je dois reconnaître que cette option ne manque pas d'attraits, mais je tiens à en savoir davantage sur la faisabilité et les éventuelles conséquences de cette « solution de cryptage massif », et surtout sur ses incidences sur le maintien de l'ordre.

54. Les responsables politiques que nous sommes doivent, en tout état de cause, être conscients du prix politique des opérations massives de surveillance : elles menacent l'existence même d'internet tel que nous le connaissons, avec tous ses avantages sociaux et économiques, et entraînent une perte de confiance des pays amis et partenaires sur la scène internationale.

55. La confiance est le fondement de toute forme de coopération internationale et elle doit, par conséquent, être restaurée de toute urgence. La solution alternative, c'est-à-dire la « balkanisation » ou « l'atomisation » d'internet et une course aux armements cryptologiques, ne semble pas très attrayante, du moins à première vue. Même s'il est difficile d'espérer que le droit et les accords nationaux et internationaux seront respectés, il convient de ne pas les perdre de vue, comme certains « experts technologiques» ont tendance à le faire. Nous devons veiller à ce que la Convention et les législations internes soient mises à jour de manière à ce qu'elles puissent offrir une protection suffisante contre toute intrusion injustifiée dans la vie privée. L'existence d'un cadre juridique établi au terme d'un débat démocratique[58] confère une légitimité à des pratiques qui restent légales, tout en donnant des orientations à ceux qui combattent « au front ». Un cadre juridique adéquat offre en particulier une garantie importante aux donneurs d'alerte éventuels, dont l'action pourrait bien être le meilleur moyen de faire respecter tout cadre juridique actuel ou futur. Pour que des révélations soient protégées par des textes de loi et des principes pertinents, les révélations doivent concerner des pratiques abusives, c'est-à-dire, dans l'idéal, des pratiques qui violent un cadre juridique en vigueur[59].

56. Cette dernière considération nous conduit tout droit au prochain sujet qui nous occupe : la protection des donneurs d'alerte.

[58] Le rapport du Groupe d'étude du Président (note 54 ci-dessus) reconnaît le préjudice causé à la diplomatie et aux intérêts économiques américains par les excès de la NSA et propose une vaste réforme des pratiques de surveillance actuelles, notamment par une limitation de la collecte des métadonnées par la NSA, le rejet des « trappes » imposées aux systèmes de sécurité des données (dont les experts n'ont pas trouvé la preuve, contrairement aux allégations fondées sur les documents révélés par M. Snowden, voir page 217) et un traitement plus respectueux des ressortissants des pays étrangers (page 155). Le Groupe reproche également à la Foreign Intelligence Surveillance Court (FISC – juridiction de contrôle du service de renseignement extérieur) de se montrer trop complaisante à l'égard des services de renseignement (page 207). L'examen des recommandations du Groupe débutera en janvier.

[59] C'est ce qui explique que M. Snowden ait réagi de manière très positive à la récente décision rendue par un juge fédéral américain. Les militants conservateurs avaient contesté en justice la validité des programmes de surveillance de la NSA. Le juge du tribunal fédéral de grande instance Richard J. Leon a estimé que les opérations massives de collecte de métadonnées et de millions de conversations téléphoniques semblaient porter atteinte au respect de la vie privée des citoyens américains, garanti par le quatrième amendement, et a invité les autorités à faire part de leurs observations sur la question. Cette affaire finira sans doute par être examinée par la Cour suprême des États-Unis. Mais, quelle qu'en soit l'issue, les conclusions préliminaires du juge Leon sont une bénédiction pour M. Snowden ; ce dernier soutient en effet qu'il a révélé les activités de la NSA parce qu'il les jugeait inconstitutionnelles. Il sera difficile de considérer que sa conviction était déraisonnable dès lors qu'un juge fédéral américain la partage. Il se peut également que cette affaire ait une influence sur l'éventuelle amnistie sous condition de M. Snowden, dont le processus a été enclenché sous la forme d'une proposition faite en ce sens par un haut responsable de la NSA, que la Maison-Blanche s'est empressée de rejeter ; voir DIE WELT du 17 décembre 2013, « US-Bundesrichter setzt das Weisse Haus unter Druck » ; lien vers le jugement : https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48 ; lien vers la déclaration de M. Snowden publiée par le New York Times : http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html).

3.2. Le Protocole additionnel à la Convention européenne des droits de l'homme sur la protection des donneurs d'alerte (améliorer la protection des donneurs d'alerte)

57. Pour ce deuxième sujet, je commencerai, une fois encore, par proposer une modification de l'intitulé du rapport, en abandonnant la mention d'un « protocole additionnel à la Convention européenne des droits de l'homme ». Il ne s'agit que de l'une des solutions possibles (qui n'est probablement pas la plus réaliste) pour améliorer la protection des donneurs d'alerte. Comme je l'ai déclaré lors de la réunion de la commission du 6 novembre 2013, j'aimerais également examiner les autres options disponibles.

58. S'agissant du sujet qui nous occupe, nous pourrons prolonger et amplifier le rapport de l'Assemblée de 2010[60] sur la protection des donneurs d'alerte. En préparant ce rapport, j'ai eu la chance de collaborer avec un groupe d'acteurs de la société civile réunis par Transparency International, qui a rédigé une série de principes directeurs applicables à la protection des donneurs d'alerte. J'ai également obtenu, par l'intermédiaire du réseau CERDP (Centre européen de recherche et de documentation parlementaires), des informations sur la législation en vigueur applicable aux donneurs d'alerte des États membres, qui est assez limitée. Ironie de l'histoire, le cadre juridique le plus efficace semble être celui des États-Unis d'Amérique. Dans sa Résolution 1729 (2010), l'Assemblée a largement souscrit aux principes directeurs susmentionnés et a encouragé le Comité des Ministres à engager le dialogue avec la société civile, afin de réfléchir aux voies et aux moyens qui permettront de protéger plus efficacement les donneurs d'alerte.

59. Je pourrai également tirer parti des travaux de notre collègue Arcadio Diaz Tejera sur « La sécurité nationale et l'accès à l'information »[61]. Les « principes de Tshwane », relatifs à l'accès à l'information et à la sécurité nationale, qui ont été avalisés par l'Assemblée dans sa Résolution 1954 (2013), énoncent une série de principes applicables à la protection des donneurs d'alerte dans le cadre de la sécurité nationale, qui s'avèrent extrêmement pertinents pour le cas de M. Snowden. La Commission interaméricaine des droits de l'homme y a largement souscrit à l'occasion de son audition thématique consacrée à « la liberté d'expression et la surveillance des communications par les États-Unis », qui a eu lieu fin octobre 2013[62].

60. Le Comité des Ministres a réagi favorablement aux recommandations de l'Assemblée[63] et a notamment convenu de la nécessité d'élaborer des lignes directrices supplémentaires sur cette question, en vue d'établir un ensemble commun de principes auxquels tous les États membres devraient adhérer. En juin 2012, le Comité européen de coopération juridique (CDCJ) a chargé son Bureau et ses membres de France, d'Irlande et du Royaume-Uni d'établir un avant-projet d'instrument juridique. En mai 2013, une conférence des parties prenantes a eu lieu à Strasbourg, au cours de laquelle j'ai eu l'honneur de représenter l'Assemblée parlementaire. Le CDCJ a approuvé un projet de recommandation du Comité des Ministres sur la protection des donneurs d'alerte et a adopté une note explicative[64] lors de sa réunion du 16 décembre 2013, ouvrant ainsi la voie à son adoption par le Comité des Ministres courant 2014.

61. Depuis l'adoption du dernier rapport de l'Assemblée en 2010, la Cour européenne des droits de l'homme a rendu deux arrêts importants sur la question des donneurs d'alerte : *Heinisch c. Allemagne* (2011)[65] et *Sosinowska c. Pologne* (2011)[66]. En outre, Transparency International[67] et d'autres réseaux internationaux spécialisés ont œuvré pour parfaire leurs principes directeurs et leurs ensembles de bonnes pratiques, qui pourraient alimenter le nouveau rapport.

---

[60] Voir le doc. 12006, adopté le 29 avril 2010.
[61] Voir la Résolution 1954 (2013), adoptée sur la base du rapport établi par M. Diaz Tejera (Espagne/SOC), doc. 13293 du 3 septembre 2013.
[62] Voir notamment le témoignage d'Emi MacLean de l'Open Society Justice Initiative, qui a également pris part à la formulation des « principes de Tshwane » (texte disponible auprès du Secrétariat).
[63] Doc. 12479 du 24 janvier 2011.
[64] Établi par Mme Anna Myers, coordinatrice du groupe d'experts**,** Whistleblowing International Network (WIN), Londres.
[65] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105777#{%22languageisocode%22:[%22FRA%22],%22appno%22:[%2228274/08%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-105778%22]}.
[66] http://echr.ketse.com/doc/10247.09-en-20111018/view/.
[67] Voir International Principles for whistleblower legislation : les meilleures pratiques en matière de législation pour la protection des donneurs d'alerte et le soutien dispensé à leur action dans l'intérêt général, Transparency International 2013.

62. Dans le cadre de ce mandat de rapporteur, j'ai l'intention de faire tout d'abord le bilan des suites données aux recommandations pertinentes de l'Assemblée, à la fois par le Comité des Ministres et par les États membres et observateurs du Conseil de l'Europe.

63. J'aimerais également réexaminer les recommandations et les principes directeurs susmentionnés, y compris les « principes de Tshwane » pertinents, à la lumière de l'affaire de la NSA. J'aimerais soumettre les principes généralement admis à un « cas pratique », en les appliquant à des affaires récentes qui ont eu un fort retentissement, comme celles de M. Edward Snowden et de M. Bradley et Mme Chelsea Manning[68]. Outre les aspects purement juridiques de la question, il serait également utile d'examiner le rôle et le développement des nouveaux réseaux et plates-formes internationaux, qui constituent autant de mécanismes supplémentaires de protection des donneurs d'alerte.

64. J'ai également l'intention de me pencher sur une proposition intéressante, qui figure dans un rapport récemment remis au Parlement européen[69] et préconise de prendre des mesures de protection des donneurs d'alerte à l'échelon européen, y compris sous la forme d'un droit d'asile accordé aux donneurs d'alerte persécutés dans leur pays d'origine en raison des révélations qu'ils ont faites dans l'intérêt général.

65. Compte tenu de ces propositions et suggestions, et de celles qui seront formulées lors de la future audition de la commission, je prévois de présenter, dans la version définitive du rapport, des propositions concrètes visant à améliorer la protection des donneurs d'alerte. L'Assemblée pourrait les transmettre à l'ensemble des États membres du Conseil de l'Europe et au Comité des Ministres, afin qu'il les prenne en compte dans ses travaux actuels sur la question.

4. Propositions d'investigation

66. Afin d'accomplir la mission qui m'a été confiée dans le cadre de mes deux mandats de rapporteur, je souhaiterais organiser deux auditions distinctes devant la commission : l'une portera sur les opérations massives de surveillance et l'autre sera consacrée à la protection des donneurs d'alerte. Ces deux auditions pourraient avoir lieu à l'occasion d'une réunion de la commission organisée pendant la partie de session de l'Assemblée d'avril 2014. Idéalement, ces auditions pourraient se dérouler le même jour, l'une le matin et l'autre l'après-midi, et être publiques. Cela permettrait à la commission d'apprécier en temps réel les implications des interventions faites à propos d'un sujet sur le second sujet et aux experts de participer à l'examen de ces questions en se rendant une seule fois à Strasbourg. Pour ce qui est de l'ordre du jour des deux auditions, je propose de débuter par les opérations massives de surveillance, qui illustrent parfaitement à la fois les possibilités et les risques inhérents à l'action des donneurs d'alerte et pourront ainsi tenir lieu d'excellent aperçu de la question pour la deuxième audition.

67. Les experts invités aux auditions sont d'ordinaire simplement choisis par le rapporteur. Mais à la lumière des échanges occasionnés par la réunion de la commission du 12 novembre 2013, je préfère soumettre à la commission, pour approbation, un certain nombre de propositions précises.

68. J'aimerais inviter à ces deux auditions des experts qui ne partagent pas le même point de vue, afin que nous puissions profiter d'un débat animé et que nous parvenions à des conclusions parfaitement objectives.

69. L'idéal serait de pouvoir entendre un représentant des autorités américaines compétentes et M. Snowden au cours des deux auditions.

70. Lors de l'audition consacrée aux opérations massives de surveillance, M. Snowden pourrait faire la synthèse de ses révélations à ce jour, et éventuellement nous communiquer de nouvelles informations, et un représentant américain (peut-être un haut responsable compétent du gouvernement) pourrait prendre position, en nous expliquant à la fois si les éléments donnés par M Snowden sont exacts et, si tel est le cas, ce qui justifie une telle activité de surveillance de la part de la NSA.

---

[68] Voir http://assembly.coe.int/nw/xml/News/News-View-EN.asp?newsid=4553&lang=2&cat=5.

[69] *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, étude de la Direction générale des politiques internes de l'Union du Parlement européen (Direction C, Direction des droits des citoyens et des affaires constitutionnelles), 2013 ; auteurs : Didier Bigo, Sergio Carrera, Nicholas Hernanz, Joanna Parkin, Francesco Ragazzi et Amandine Scherrer ; voir notamment la recommandation 8 p. 46.

71. À l'occasion de l'audition consacrée à la protection des donneurs d'alerte, le représentant américain pourrait être invité à nous faire part des raisons qui motivent le fait de traiter M. Snowden comme un criminel et M. Snowden pourrait nous expliquer pourquoi il a fait le choix de donner l'alerte sur les activités de son ancien employeur.

72. Nous devrions également, pour chacune des auditions, inviter un ou deux experts supplémentaires, qui pourraient nous présenter les faits sous un angle complémentaire et définir les grandes lignes des solutions susceptibles d'être apportées à cette situation.

73. Je propose d'inviter à l'audition sur les opérations massives de surveillance, outre le représentant américain et M. Snowden :

(1) Ben Scott, conseiller principal de l'Open Technology Institute à la New America Foundation et directeur du programme de stratégie numérique pour l'Europe à la Stiftung Neue Verantwortung de Berlin. Il a également exercé les fonctions de conseiller pour les questions technologiques au Département d'État américain, et

(2) Hansjörg Geiger, ancien directeur du Bundesnachrichtendienst (BND) allemand, auteur d'une proposition de « code du renseignement », qui sera adopté par tous les pays membres de l'OTAN en vue de rétablir la confiance entre les pays qui partagent le même point de vue.

74. Pour ce qui est de la protection des donneurs d'alerte, je propose d'inviter les experts supplémentaires suivants :

(1) Anna Myers, responsable du réseau de donneurs d'alerte établi au Royaume-Uni et conseillère auprès du Conseil de l'Europe pour le projet de recommandation du Comité des Ministres sur la protection des donneurs d'alerte, et

(2) Brendan Howlin, ministre irlandais de la Dépense publique et de la Réforme, qui a mis en place une législation visant à promouvoir la protection des donneurs d'alerte en Irlande.

75. J'ai conscience du caractère controversé que revêt la proposition d'inviter M. Snowden. Mais je suis convaincu que ses interventions sur ces deux sujets seront dignes d'intérêt. Le fait de l'inviter renforcera inévitablement la visibilité médiatique de M. Snowden, mais, disons-le franchement, cette visibilité ne lui fait pas défaut et ne sera pas moindre si nous ne l'invitons pas. Comme je l'ai expliqué en novembre dernier, le fait d'entendre ce qu'il a à dire ne signifie pas adopter son point de vue ni avaliser son action. Les déclarations de M. Snowden seront contrebalancées par les exposés du représentant américain et des autres experts, dont l'un au moins possède une solide expérience dans le domaine du renseignement. La possibilité de procéder à un échange de vues avec un interlocuteur controversé, sans entraîner de tension dans les relations bilatérales de l'un ou l'autre pays, représente l'un des avantages propres à une assemblée internationale comme la nôtre, et il importe que nous en tirions parti.

76. Je suis également conscient que M. Snowden ne sera peut-être pas en mesure de se rendre à Strasbourg. Il est recherché aux États-Unis et ces derniers pourraient demander son extradition à la France, l'État-siège du Conseil de l'Europe, lequel pourrait être lié par un certain nombre d'obligations en tant que tel. Il appartiendra en définitive à M. Snowden, en accord avec ses hôtes russes, de décider s'il se sent suffisamment en confiance pour accepter cette invitation. En guise de solution de repli, nous pourrions inviter M. Snowden à participer à cette audition par voie de téléconférence ou la commission pourrait m'autoriser à lui rendre visite en Russie et à lui rendre compte de cet entretien.

77. Outre ces deux auditions, j'aimerais également demander à la commission l'autorisation de rencontrer un expert en technologies de l'information spécialisé dans les questions de la sécurité sur internet et un expert juridique, afin qu'ils me conseillent sur la viabilité technique et juridique des propositions que j'ai l'intention de formuler dans la version définitive de mon rapport sur les opérations massives de surveillance.