



Doc. 13748

09 avril 2015

Les opérations de surveillance massive

Avis de commission¹

Commission de la culture, de la science, de l'éducation et des médias

Rapporteur: Sir Roger GALE, Royaume-Uni, Groupe des conservateurs européens

A. Conclusions de la commission

1. La commission de la culture, de la science, de l'éducation et des médias estime que le rapport sur les opérations massives de surveillance de la commission des questions juridiques et des droits de l'homme ([Doc. 13734](#)) arrive à point nommé. A son origine se trouvent les révélations massives par Edward Snowden des données secrètes provenant d'opérations de sécurité nationale des Etats-Unis, du Royaume-Uni, d'Australie et d'autres pays, puis les poursuites engagées contre lui le 14 juin 2013 par un procureur fédéral des Etats-Unis et son départ en Fédération de Russie, où il réside depuis juillet 2013. Toutefois, l'importance politique de l'affaire dépasse à présent largement la personne et les actes d'Edward Snowden.

2. Tout en accueillant favorablement les conclusions générales présentées dans ce rapport sur les opérations de surveillance massive, la commission propose de clarifier encore et de préciser par un certain nombre d'amendements le projet de résolution qu'il contient.

B. Amendements proposés au projet de résolution:

Amendement A (au projet de résolution)

Au paragraphe 2, après les mots «d'autres pays et sur l'absence», insérer le mot «éventuelle».

Amendement B (au projet de résolution)

Supprimer le paragraphe 7.

Amendement C (au projet de résolution)

Dans la version anglaise, au paragraphe 11, première phrase, après le mot «terrorists», remplacer «or» par «and» (sans objet en français).

Amendement D (au projet de résolution)

Au paragraphe 12, deuxième phrase, supprimer le mot «Mais» et après les mots «fondée sur», insérer les mots «des accords internationaux».

1. Renvoi en commission: Renvoi 4003 du 30 septembre 2013. Commission saisie du rapport: Commission des questions juridiques et des droits de l'homme. Voir [Doc. 13734](#). Avis approuvé par la commission le 11 mars 2015.



Amendement E (au projet de résolution)

Au paragraphe 13, deuxième phrase, après le mot «violations», insérer les mots «dans l'intérêt général et sans profit personnel».

Amendement F (au projet de résolution)

Supprimer le paragraphe 14.

Amendement G (au projet de résolution)

Remplacer la deuxième phrase du paragraphe 15 par le texte suivant:

«Rappelant les conclusions présentées dans le rapport sur le contrôle démocratique des forces armées adopté par la Commission européenne pour la démocratie par le droit (Commission de Venise) en 2008, l'Assemblée souligne que les parlements doivent jouer un rôle important dans le suivi, l'examen et le contrôle des services de sécurité nationaux et des forces armées nationales pour garantir le respect des droits de l'homme, de l'Etat de droit et de la responsabilité démocratique, ainsi que du droit international. La sous-traitance d'opérations de sécurité ou de renseignement à des sociétés privées doit être exceptionnelle et ne doit pas entraver le contrôle démocratique de ces opérations.»

Amendement H (au projet de résolution)

Supprimer le paragraphe 16.1.

Amendement I (au projet de résolution)

Après le paragraphe 16, insérer le paragraphe suivant:

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

Amendement J (au projet de résolution)

Dans la version anglaise, au paragraphe 17.1, remplacer les mots «mail secret» par les mots «confidentiality of correspondence» (sans objet en français).

Amendement K (au projet de résolution)

Remplacer le paragraphe 17.3 par le paragraphe suivant:

«accorder une protection crédible et efficace aux donneurs d'alerte qui révèlent les activités de surveillance illégales, conformément à la [Résolution 1729 \(2010\)](#) de l'Assemblée sur la protection des donneurs d'alerte;»

Amendement L (au projet de résolution)

Au paragraphe 17.4, avant-dernière phrase, supprimer les mots «politiques» et «ou diplomatiques».

C. Exposé des motifs, par Sir Roger Gale, rapporteur pour avis

1. Introduction

1. Le 30 septembre 2013, suite au débat d'actualité du 27 juin 2013 sur l'ingérence de l'Etat dans la vie privée sur internet, la commission a tenu un échange de vues avec Lawrence Early, juriste auprès de la Cour européenne des droits de l'homme, Dorothee Belz, vice-présidente et responsable des affaires juridiques et internes de Microsoft Corporation Europe, et Duncan Campbell, journaliste, Brighton, Royaume-Uni². Après avoir entendu encore Duncan Campbell à Paris, le 11 mars 2014, dans le cadre de la préparation

du rapport d'Axel Fischer (Allemagne, PPE/DC) sur l'amélioration de la protection et de la sécurité des utilisateurs dans le cyberspace, la commission a décidé de demander au Bureau de l'Assemblée d'être saisie pour avis sur le rapport relatif aux opérations de surveillance massive.

2. Surveillance massive

2. La surveillance massive n'est pas un phénomène nouveau. La dictature nazi en Allemagne s'y livrait déjà par une surveillance directe de la population par le canal d'un grand nombre des agents d'îlot (*Blockwart*); le progrès technique a ensuite permis aux régimes communistes de mettre en place un dispositif de surveillance massive, qui a débouché sur les écoutes téléphoniques à grande échelle et le stockage d'abord conventionnel, puis électronique, des données par le célèbre KGB, en particulier dans les «pays frères» ou pays satellites contrôlés par l'Union soviétique. Cette pratique a engendré une profonde défiance de la population à l'égard des autorités publiques, espionnes de leur propre peuple, comme le décrit George Orwell dans son roman *1984*. C'est ce thème que l'on retrouve dans le mot d'Alexandre Soljenitsyne («Notre liberté repose sur ce que les autres ignorent de notre existence») décrivant la situation en URSS et placé en exergue du rapport sur les opérations de surveillance massive.

3. Si les Etats non démocratiques ont utilisé la surveillance massive pour contrôler et museler l'opposition politique, les technologies de surveillance ont aussi été employées par des Etats démocratiques contre la criminalité à grande échelle et le terrorisme. Au lendemain des attentats commis par la «Fraction Armée rouge» en Allemagne de l'Ouest dans les années 1970, la Cour européenne des droits de l'homme avait estimé en l'affaire *Klass et autres c. Allemagne* (Requête n° 5029/71) 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. (...) 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.» «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.³»

4. L'essor de la téléphonie portable, depuis la fin du XX^e siècle, a permis aux services secrets d'intercepter largement les communications de ce type. Cette pratique des Etats-Unis d'Amérique et de leurs alliés a fait l'objet du rapport du Parlement européen du 11 juillet 2001 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)⁴. Par ailleurs, la Cour européenne des droits de l'homme a encore étoffé sa jurisprudence en la matière: «Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer: la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements⁵.»

5. Le rapide développement des communications par internet et la simplicité technique de leur interception et de leur écoute ont pour effet que la surveillance atteint aujourd'hui un niveau inédit. Même si la façon dont les révélations d'Edward Snowden ont été publiées par un quotidien national britannique est extrêmement contestable, mettant ainsi en danger la vie de personnes participant à la lutte contre le terrorisme, elles ont cependant fait la lumière sur les pratiques des services nationaux de sécurité des Etats-Unis et de pays coopérant avec eux. On peut toutefois avancer l'hypothèse que d'autres pays possèdent aussi le matériel et les compétences leur permettant de procéder à la surveillance massive de leurs ressortissants et de ressortissants étrangers à l'extérieur de leurs frontières utilisant internet et des appareils

2. <https://pace.coe.int/documents/19871/25990/CoECultureCommittee1Oct2013REV.pdf/ee1f16ef-1faf-49a9-8b41-f2767e300b3c>.

3. <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-62068>.

4. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//FR&language=FR.

5. *Liberty et autres c. Royaume-Uni* (Requête n° 58243/00), citant sa décision en l'affaire *Weber et Saravia c. Allemagne* (Requête n° 54934/00), <http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-87208>.

portables pour leurs communications. De plus, des sociétés commerciales multinationales utilisent la surveillance de masse et le profilage des utilisateurs d'internet pour cibler leur publicité. Ce phénomène a d'ailleurs été abordé par le Comité des Ministres dans sa Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, ainsi que dans sa Recommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche.

6. L'examen des opérations de surveillance massive doit dûment tenir compte de leur objectif. Si la surveillance massive à caractère privé ou commercial ne relève en général pas des exceptions au droit à la protection de la vie privée garanti à l'article 8 de la Convention européenne des droits de l'homme (STE n° 5), la surveillance massive pratiquée par les services de police doit respecter les garde-fous mis en place par la Cour européenne des droits de l'homme⁶. La sécurité nationale est mentionnée expressément à l'article 8 de la Convention et justifie clairement des restrictions du droit au respect de la vie privée, mais elle doit impérativement être définie avec précision dans le droit national et le gouvernement ne doit pas utiliser les mesures prises à ce titre pour persécuter une opposition politique démocratique⁷. En ce qui concerne une définition étroite de la notion de sécurité nationale, il est possible d'évoquer les Principes de Johannesburg de 1995 sur la sécurité nationale, la liberté d'expression et l'accès à l'information⁸.

7. A la suite des attentats de Paris, les ministres de l'Intérieur de plusieurs pays d'Europe, du Canada et des Etats-Unis ont publié le 11 janvier 2015 à Paris une déclaration appelant au renforcement de la coopération internationale, en particulier transatlantique, dans la lutte contre le terrorisme international. Cet appel a été repris à la réunion informelle de Riga des ministres de la Justice et de l'Intérieur des Etats membres de l'Union européenne (29 et 30 janvier 2015)⁹. Une coopération de ce type avait permis en 2007 l'arrestation en Allemagne de terroristes islamistes du groupe informellement appelé «cellule du Sauerland», grâce à l'interception de communications téléphoniques et de courriers électroniques entre l'Allemagne et le Pakistan par l'Agence de sécurité nationale des Etats-Unis, qui en a informé les autorités allemandes. Les services de sécurité russes avaient intercepté des appels téléphoniques de Tamerlan Tsarnaev et de sa mère et en avaient informé les services secrets des Etats-Unis, mais les frères Tsarnaev ont tout de même pu réaliser leurs attentats à la bombe lors du marathon de Boston en 2013, révélant les effets parfois désastreux et mortels d'une coopération inefficace¹⁰.

8. En 2013, le Parlement européen s'est opposé à l'échange proposé de données sur les passagers voyageant entre l'Union européenne et les Etats-Unis. Après les attentats contre *Charlie Hebdo* du 7 janvier 2015, le Président du Conseil de l'Union européenne a appelé le Parlement européen à accélérer ses travaux sur le système européen de dossiers passagers (PNR). Le 11 février 2015, le Parlement européen a finalement accepté de boucler les travaux sur le PNR pour la fin de l'année 2015¹¹. Ces travaux devraient être liés à la mise au point du Règlement général sur la protection des données de l'Union européenne et à l'adhésion de cette dernière à 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).

9. Edward Snowden, qui travaillait pour un sous-traitant privé de l'Agence nationale de sécurité (NSA) des Etats-Unis, a déclaré au quotidien *The Guardian* que le gouvernement s'était arrogé des pouvoirs dont il n'était pas investi, en dehors de tout contrôle public, ce qui voulait dire que les personnes comme lui avaient toute latitude pour outrepasser les autorisations¹². Cette autocritique montre bien le problème qu'engendre le fait que la responsabilité juridique des sociétés privées de sécurité ne va pas au-delà des clauses d'un contrat et de la législation nationale générale, alors que le contrôle démocratique parlementaire ne s'applique qu'aux autorités publiques et aux services de sécurité publics. Il conviendrait d'une manière générale d'éviter ce genre de sous-traitance pour prévenir le contournement du contrôle parlementaire, comme le recommande la Commission européenne pour la démocratie par le droit (Commission de Venise) dans son rapport de 2008 sur le contrôle démocratique des forces armées¹³.

6. Voir, par exemple, *Weber et Saravia c. Allemagne* (Requête n° 54934/00), *op. cit.*

7. Voir l'analyse de la jurisprudence de la Cour européenne des droits de l'homme de 2013, publiée par le greffe de la Cour (en anglais):

[www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20\(final\).pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20(final).pdf).

8. www.article19.org/data/files/medialibrary/1803/Johannesburg-Principles.Fra.pdf.

9. https://eu2015.lv/images/Kalendars/leM/2015_01_29_jointstatement_JHA.pdf.

10. www.bbc.com/news/world-us-canada-26975845.

11. <http://ecrgroup.eu/news/european-parliament-agrees-to-reach-passenger-name-records-agreement-this-year/>.

12. *The Guardian*, 11 juin 2013, www.theguardian.com/world/2013/jun/10/obama-pressured-explain-nsa-surveillance.

13. [www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2008\)004-f](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2008)004-f).

10. En sa qualité de rapporteur de la commission des questions juridiques et des droits de l'homme, Pieter Omtzigt (Pays-Bas, PPE/DC) prépare également un rapport sur l'amélioration de la protection des donneurs d'alerte¹⁴, en parallèle au présent rapport sur les opérations de surveillance massive. Ces deux rapports procèdent à une ample analyse juridique des actes d'Edward Snowden. Outre l'énorme quantité de renseignements copiés qu'Edward Snowden avait emportés avec lui en quittant les Etats-Unis pour la Chine, puis la Russie fin juin 2013, il possède lui-même manifestement une valeur stratégique considérable pour les services de sécurité russes en raison de l'expérience et des connaissances qu'il a accumulées dans ses importantes fonctions auprès des services secrets américains. Ce savoir a probablement déjà été utilisé pour percer des structures internationales de renseignement et améliorer les activités de renseignement de la Russie dans le cyberspace. Eu égard au déficit considérable de transparence et d'accès à l'information au sein des autorités russes, il est peu probable que l'asile, un permis de séjour, un logement et un travail rémunéré aient été offerts par la Russie à Edward Snowden par pur altruisme et solidarité avec les donneurs d'alerte en général.

11. En conclusion, il vaut la peine de rappeler dans ce contexte un autre extrait d'un arrêt de la Cour européenne des droits de l'homme en l'affaire *Klass et autres c. Allemagne* (Requête n° 5029/71): «En évaluant l'étendue de la sauvegarde offerte par l'article 8 [de la Convention européenne des droits de l'homme] 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 l'Etat doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire.» Cette constatation est d'une actualité plus brûlante que jamais.

3. Justification des amendements proposés

(A) Le projet de résolution évoque au paragraphe 2 «l'absence de dispositions légales et de protections techniques adéquates aux échelons national et international», mais rien dans le rapport ne vient étayer une affirmation aussi radicale et catégorique. De fait, le Conseil de l'Europe a produit des traités internationaux qui garantissent une protection juridique, comme la Convention européenne des droits de l'homme et la Convention sur la cybercriminalité (STE n° 185).

(B) Le paragraphe 7 avance une série d'allégations qu'il ne justifie pas. Il convient de les étayer, ou bien de supprimer ce paragraphe.

(C) Dans la version anglaise, le paragraphe 11 parle de «effective, targeted surveillance of suspected terrorists or other organised criminal groups» [surveillance ciblée et efficace des personnes soupçonnées de mener des activités terroristes ou d'autres groupes de criminels organisés]. Il est important de conserver la possibilité d'une surveillance ciblée des personnes soupçonnées de terrorisme ET des personnes soupçonnées d'appartenir à des organisations criminelles.

(D) La confiance n'est possible entre les partenaires transatlantiques que moyennant la mise en place de cadres juridiques appropriés. Le Conseil de l'Europe propose en la matière un certain nombre de traités juridiques ouverts à la signature d'Etats non membres, en particulier la Convention européenne sur l'entraide judiciaire en matière pénale (STE n° 30), la Convention européenne pour la répression du terrorisme (STE n° 90), la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STE n° 141), la Convention sur la cybercriminalité et la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Il est donc nécessaire de fonder la coopération future sur des accords plutôt que sur la simple confiance.

(E) Il est impossible de protéger sans réserve le «droit de donner l'alerte», car cela pourrait déboucher sur la vente d'informations confidentielles et sensibles dans des buts intéressés. Cet amendement s'inspire de la [Résolution 1729 \(2010\)](#) de l'Assemblée sur la protection des donneurs d'alerte.

(F) A la suite des révélations d'Edward Snowden, le Président des Etats-Unis a annoncé au mois de janvier 2014 un changement de pratiques de la NSA et des procédures de la cour des Etats-Unis concernant la surveillance par le renseignement à l'étranger (*Foreign Intelligence Surveillance Court*). Le Congrès des Etats-Unis a ouvert une enquête, de même que les gouvernements de la France, de l'Allemagne, de

14. Voir la proposition de recommandation correspondante d'Andrej Hunko (Allemagne, GUE) et plusieurs de ses collègues, [Doc. 13278](#).

l'Espagne et d'autres pays. De plus, il n'y a pas de signes qu'Edward Snowden ait été traité «sans ménagement». Comme il est en Russie depuis la fin juin 2013, un tel traitement ne peut de fait lui avoir été infligé hors de la Russie, et le rapport ne dit rien de la façon dont il est traité en Russie.

(G) L'Assemblée n'a aucune raison de penser que la commission d'enquête du Parlement allemand ne serait pas en mesure d'assumer son rôle parlementaire; il conviendrait plutôt d'évoquer la nécessité du contrôle démocratique parlementaire des services de sécurité et des forces armées des Etats membres. Cela faisait l'objet d'une analyse approfondie et d'une recommandation dans le rapport sur le contrôle démocratique des forces armées adopté par la Commission européenne pour la démocratie par le droit (Commission de Venise) en 2008. Par ailleurs, il importe de rappeler aux gouvernements le risque que représente la sous-traitance d'activités de renseignement à des sociétés privées non soumises à ce contrôle démocratique.

(H) Dans sa résolution du 12 mars 2014, le Parlement européen invitait le Secrétaire Général du Conseil de l'Europe à ouvrir une enquête contre des Etats Parties en vertu de l'article 52 de la Convention européenne des droits de l'homme. Il y a sans doute de bonnes raisons pour que cette enquête n'ait pas été ouverte, plusieurs parlements et gouvernements d'Etats Parties ayant depuis lors débattu de leur coopération avec l'Agence de sécurité nationale des Etats-Unis et d'autres services de renseignements étrangers. Dans ce domaine, beaucoup de choses dépendront aussi des progrès de la coordination des politiques et législations de l'Union européenne. Nous ne devrions donc pas insister sur cette demande au Secrétaire Général.

(I) En 2013, le Parlement européen s'est opposé à la proposition d'échange de dossiers des passagers voyageant entre l'Union européenne et les Etats-Unis. Au lendemain des attentats contre *Charlie Hebdo* du 7 janvier 2015, le Président du Conseil de l'Union européenne a appelé le Parlement européen à accélérer ses travaux sur le système européen de dossiers passagers (PNR). Cet appel aux institutions de l'Union européenne a été repris par les ministres de l'Intérieur réunis à Paris le 11 janvier 2015. Ces travaux doivent être liés à la mise au point du règlement général de l'Union européenne sur la protection des données et à l'adhésion de l'Union européenne à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

(J) L'article 8 de la Convention européenne des droits de l'homme couvre bien le droit à la protection de la confidentialité de la correspondance, mais la notion de secret du courrier («mail secret» dans la version anglaise) n'existe pas et son sens très étroit pourrait prêter à confusion.

(K) Dans sa [Résolution 1729 \(2010\)](#) sur la protection des donneurs d'alerte, l'Assemblée examine soigneusement cette question à la lumière des normes du Conseil de l'Europe. Il est donc nécessaire que l'Assemblée rappelle ici cette résolution. L'asile a été refusé à Edward Snowden par plusieurs pays pour des raisons d'ordre juridique. Même la Russie a converti son statut de demandeur d'asile en celui de résident. Enfin, la plupart des pays du monde n'accordent pas l'asile à une personne faisant valoir qu'elle pourrait faire l'objet de poursuites injustes, surtout lorsqu'il existe des accords d'entraide judiciaire, comme c'est le cas entre les Etats-Unis et de nombreux pays d'Europe.

(L) La surveillance peut parfois se justifier pour des raisons d'ordre politique ou diplomatique, mais en aucun cas pour de l'espionnage industriel.