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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Résolution 2045 (2015)[1]

Les opérations de surveillance massive

Assemblée parlementaire

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

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

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

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

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

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

---

1. *Discussion par l'Assemblée* le 21 avril 2015 (12e séance) (voir Doc. 13734, rapport de la commission des questions juridiques et des droits de l'homme, rapporteur: M. Pieter Omtzigt; et Doc. 13748, avis de commission de la culture, de la science, de l'éducation et des médias, rapporteur: Sir Roger Gale). *Texte adopté par l'Assemblée* le 21 avril 2015 (12e séance).
Voir également la Recommandation 2067 (2015).

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

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

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

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

11. L'Assemblée reconnaît la nécessité d'une surveillance ciblée et efficace des personnes soupçonnées de mener des activités terroristes et d'autres groupes de criminels organisés. Cette surveillance ciblée peut être un outil efficace pour faire respecter la loi et prévenir la criminalité. Parallèlement, elle observe que, d'après des études indépendantes réalisées aux Etats-Unis, les opérations de surveillance massive ne semblent pas avoir contribué à prévenir les attentats terroristes, contrairement à ce qu'affirmaient autrefois les hauts responsables des services de renseignement. Au contraire, des ressources qui pourraient servir à prévenir des attaques sont redirigées vers la surveillance massive, laissant des personnes potentiellement dangereuses libres d'agir.

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

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

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

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

16. Rappelant les conclusions présentées dans le rapport sur le contrôle démocratique des services de sécurité, adopté par la Commission européenne pour la démocratie par le droit (Commission de Venise) en 2015, l'Assemblée souligne que les parlements doivent jouer un rôle important dans le suivi, l'examen et le contrôle des services de sécurité nationaux et des forces armées nationales pour garantir le respect des

droits de l'homme, de l'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.

17. L'Assemblée se félicite de l'enquête approfondie menée par le Parlement européen, qui a conduit à l'adoption, le 12 mars 2014, d'une résolution très complète sur l'affaire de la NSA et ses répercussions sur les relations transatlantiques. L'Assemblée souscrit pleinement, en particulier:

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

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

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

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

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

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

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

19.4. à convenir d'un «code du renseignement» multilatéral, destiné à leurs services de renseignement, qui définisse les principes régissant la coopération aux fins de lutte contre le terrorisme et la criminalité organisée. Ce code devrait prévoir un engagement mutuel à appliquer à la surveillance des ressortissants et résidents des pays partenaires les mêmes dispositions qui s'appliquent à leurs propres ressortissants et résidents, ainsi qu'à échanger les données obtenues par des mesures de surveillance légales uniquement dans le but pour lequel elles ont été collectées. Le recours aux mesures de surveillance à des fins politiques, économiques ou diplomatiques dans les Etats participants devrait être interdit. L'adhésion à ce code devrait être ouverte à tous les Etats qui mettent en œuvre à l'échelon national un cadre juridique correspondant aux dispositions énoncées aux paragraphes 19.1 à 19.3;

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

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

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