

Programme de surveillance de la NSA américaine, agences de surveillance dans différents États membres et incidence sur la vie privée des citoyens européens

Résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union (2013/2682(RSP))

Le Parlement européen,

- vu les articles 2, 3, 6 et 7 du traité sur l'Union européenne (traité UE) et l'article 16 du traité sur le fonctionnement de l'Union européenne (traité FUE),
- vu à la charte des droits fondamentaux de l'Union européenne et la convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH),
- vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel du 8 novembre 2001,
- vu la législation de l'Union sur le droit au respect de la vie privée et à la protection des données, notamment la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,
- vu les propositions de la Commission relatives à un règlement et à une directive sur la réforme du régime de protection des données au sein de l'Union,
- vu l'accord entre l'Union européenne et les États-Unis en matière d'entraide judiciaire, qui permet l'échange de données à des fins de prévention des infractions pénales et d'enquêtes en la matière, la convention sur la cybercriminalité (STCE n° 185), l'accord UE - États-Unis sur la sphère de sécurité (2000/520/EC) et la révision en cours des principes de cette sphère de sécurité,
- vu le Patriot Act (loi antiterroriste) et le Foreign Intelligence Surveillance Act (FISA – loi sur les activités de renseignement à l'étranger) adoptés par les États-Unis, y compris la section 702 de la loi de 2008 modifiant le FISA,
- vu les négociations en cours sur un accord-cadre UE - États-Unis sur la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de la coopération policière et judiciaire,

- vu ses résolutions antérieures sur le droit au respect de la vie privée et à la protection des données, notamment celle du 5 septembre 2001 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Échelon)¹,
 - vu les déclarations de Herman van Rompuy, président du Conseil européen, de Martin Schulz, Président du Parlement européen, de Viviane Reding, vice-présidente de la Commission / commissaire chargée de la justice, des droits fondamentaux et de la citoyenneté, et de Catherine Ashton, vice-présidente de la Commission / haute représentante de l'Union pour les affaires étrangères et la politique de sécurité,
 - vu l'article 110, paragraphes 2 et 4, de son règlement,
- A. considérant que le partenariat transatlantique entre l'UE et les États-Unis doit se baser sur la confiance et le respect mutuels, une coopération loyale et mutuelle, le respect des droits fondamentaux et l'état de droit;
 - B. considérant que les États membres sont tenus de respecter les valeurs et les droits fondamentaux consacrés à l'article 2 du traité UE et dans la charte des droits fondamentaux;
 - C. considérant que le respect de ces principes est actuellement remis en question à la suite de la parution, en juin 2013, d'informations dans la presse internationale, qui ont révélé que les autorités américaines avaient la possibilité d'accéder à large échelle, par le biais de programmes tels que Prism, aux données à caractère personnel de citoyens de l'Union lorsqu'ils ont recours à des prestataires américains de services en ligne, et de traiter ces données;
 - D. considérant que cette remise en question concerne non seulement les actions des autorités américaines, mais aussi celles de plusieurs États membres de l'Union européenne, qui, selon la presse internationale, ont coopéré avec Prism et d'autres programmes de même nature ou se sont vu accorder un accès aux bases de données créées;
 - E. considérant, en outre, que plusieurs États membres disposent de programmes de surveillance similaires ou envisagent d'en créer;
 - F. considérant que des questions spécifiques ont été soulevées quant à la compatibilité avec le droit de l'Union de la pratique du GCHQ (agence britannique d'espionnage électronique) consistant à détourner directement les communications électroniques passant par les câbles transatlantiques, dans le cadre d'un programme répondant au nom de code Tempora; considérant que d'autres États membres intercepteraient des communications électroniques transnationales sans mandat formel mais sur décision de juridictions spéciales, qu'ils partageraient leurs données avec d'autres pays (Suède) et qu'ils pourraient élargir leurs capacités de surveillance (Pays-Bas, Allemagne); que des voix se sont élevées, dans d'autres États membres, pour s'inquiéter des pouvoirs d'interception laissés aux services secrets (Pologne);
 - G. considérant que certaines indications donnent à penser que les institutions de l'Union européenne ainsi que les représentations et les ambassades de l'Union et des États membres ont été l'objet d'actions américaines de surveillance et d'espionnage;

¹ JO C 72 E du 21.3.2002, p. 221.

- H. considérant que la commissaire Reding a adressé un courrier au ministre de la justice des États-Unis, Eric Holder, pour lui faire part des inquiétudes européennes, lui demander des éclaircissements et des explications sur le programme Prism et les autres programmes de même nature permettant la collecte et la recherche de données et pour s'enquérir de la base juridique autorisant la mise en œuvre de tels programmes; que les autorités américaines restent redevables d'une réponse exhaustive, malgré la réunion qui a eu lieu le 14 juin 2013 à Dublin entre les ministres de la justice de l'Union européenne et des États-Unis;
- I. considérant que l'accord sur la sphère de sécurité charge les États membres et la Commission de garantir la sécurité et l'intégrité des données à caractère personnel; que, selon la presse internationale, les entreprises associées à l'affaire Prism sont toutes parties à l'accord sur la sphère de sécurité; qu'en vertu de l'article 3 dudit accord, la Commission a l'obligation de le dénoncer ou de le suspendre si ses dispositions ne sont pas respectées;
- J. considérant que l'accord entre l'Union européenne et les États-Unis en matière d'entraide judiciaire, ratifié par l'Union et le Congrès des États-Unis, prévoit des modalités de collecte et d'échange d'informations ainsi que de demande et de fourniture d'entraide, afin de recueillir des preuves situées dans un pays en vue de prêter assistance dans le cadre d'enquêtes ou de procédures pénales ouvertes dans un autre;
- K. considérant qu'il serait regrettable que les efforts déployés pour conclure un partenariat transatlantique de commerce et d'investissement, lesquels mettent en lumière la détermination de l'Union européenne et des États-Unis à renforcer encore leur partenariat, soient affectés par les récentes allégations;
- L. considérant que, le 14 juin 2013, la commissaire Malmström a annoncé la création d'un groupe transatlantique d'experts;
- M. considérant que la commissaire Reding a écrit aux autorités britanniques pour exprimer sa préoccupation au sujet des informations parues dans les médias sur le programme Tempora et demander des éclaircissements sur sa portée et son mode opératoire; considérant que les autorités britanniques ont défendu les activités de surveillance du GCHQ et affirmé qu'elles agissaient selon des lignes directrices strictes et légales;
- N. considérant qu'une réforme de la protection des données est en cours au moyen de la révision de la directive 95/46/CE et de son remplacement par la proposition de règlement général sur la protection des données, et par la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données;
- 1. fait part, tout en confirmant son soutien sans faille aux efforts transatlantiques déployés en matière de lutte contre le terrorisme et la criminalité organisée, des graves inquiétudes que lui inspirent tant le programme Prism que les autres programmes similaires, dès lors que, si les informations actuellement disponibles venaient à être confirmées, ces programmes pourraient constituer une grave violation du droit fondamental à la vie privée et à la protection des données dont peuvent se prévaloir les citoyens et les résidents de l'Union, ainsi qu'une violation de la vie privée et familiale, de la confidentialité des communications, de la présomption d'innocence, de la liberté d'expression, de la liberté d'information et de la liberté d'entreprise;

2. condamne vivement l'espionnage des représentations de l'Union européenne qui, si les informations actuellement disponibles venaient à être confirmées, constituerait une grave violation de la convention de Vienne sur les relations diplomatiques et serait de nature à affecter les relations transatlantiques; demande aux autorités des États-Unis de fournir immédiatement des éclaircissements à ce sujet;
3. invite les autorités américaines à fournir à l'Union européenne, dans les meilleurs délais, des informations complètes sur le programme Prism et les autres programmes similaires permettant la collecte de données, notamment en ce qui concerne leur base juridique, leur nécessité et leur proportionnalité, ainsi que les sauvegardes mises en place pour protéger les droits fondamentaux des citoyens de l'Union, telles que la limitation du champ d'application et de la durée de telles procédures, les conditions d'accès et une supervision indépendante, comme le prévoit la convention sur la cybercriminalité et l'a également exigé la commissaire Reding dans sa lettre du 10 juin 2013 adressée au ministre de la justice Eric Holder; invite les autorités américaines à suspendre et à revoir toutes les lois et tous les programmes de surveillance qui violent le droit fondamental des citoyens de l'Union au respect de leur vie privée et à la protection de leurs données, la souveraineté et la juridiction de l'Union et de ses États membres, ainsi que la convention sur la cybercriminalité;
4. invite la Commission, le Conseil et les États membres à user de tous les instruments à leur disposition dans les discussions et les négociations avec les États-Unis, à l'échelon tant politique que technique, dans le but d'atteindre les objectifs susdits, y compris la suspension éventuelle des accords sur les données des dossiers passagers (PNR) ou du programme de surveillance du financement du terrorisme (TFTP);
5. exige que le groupe transatlantique d'experts, dont la création a été annoncée par la commissaire Malmström et auquel le Parlement participera, se voie accorder une habilitation de sécurité de niveau approprié et un accès à tous les documents nécessaires afin de pouvoir mener à bien ses travaux dans un délai convenu; exige également que le Parlement soit correctement représenté dans ce groupe d'experts;
6. invite la Commission et les autorités des États-Unis à reprendre sans délai les négociations sur l'accord-cadre sur la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de la coopération policière et judiciaire; demande à la Commission de veiller, au cours de ces négociations, à ce que l'accord satisfasse au moins aux critères suivants:
 - a) les citoyens de l'Union doivent se voir accorder un droit d'information lorsque leurs données sont traitées aux États-Unis;
 - b) les citoyens de l'Union doivent jouir d'un accès au système judiciaire des États-Unis égal à celui des citoyens américains;
 - c) un droit de recours doit notamment être prévu;
7. invite la Commission à garantir que les normes de l'Union en matière de protection des données et les négociations sur l'actuel paquet relatif à cette même protection des données ne seront pas mises à mal par le partenariat transatlantique de commerce et d'investissement qui sera conclu avec les États-Unis;

8. invite la Commission à mener une révision approfondie de l'accord sur la sphère de sécurité à la lumière des révélations récentes, conformément à l'article 3 dudit accord;
9. fait part des graves préoccupations que lui inspirent les révélations concernant les programmes de surveillance supposés de certains États membres, qu'ils soient mis en œuvre unilatéralement ou avec le soutien de l'agence nationale de sécurité américaine; invite tous les États membres à examiner la compatibilité de tels programmes avec le droit primaire et dérivé de l'Union, notamment avec l'article 16 du traité FUE sur la protection des données, et avec les obligations de l'Union relatives aux droits fondamentaux qui découlent de la CEDH et des traditions constitutionnelles communes des États membres;
10. souligne que toutes les entreprises fournissant des services dans l'Union doivent, sans exception, se conformer au droit de l'Union et qu'elles sont responsables de tout manquement;
11. souligne que les entreprises relevant de la juridiction d'un pays tiers devraient alerter de manière claire et visible les utilisateurs situés dans l'Union quant à l'éventualité que leurs données soient traitées par des agences répressives et de renseignement à la suite de décisions ou d'ordonnances édictés secrètement;
12. regrette que la Commission ait retiré l'ex-article 42 de la version du règlement sur la protection des données qui avait filtré; invite la Commission à expliquer cette décision; demande au Conseil d'adopter l'approche du Parlement et de rétablir une disposition analogue;
13. souligne que, dans les États démocratiques et ouverts, fondés sur l'état de droit, les citoyens ont le droit d'avoir connaissance des atteintes graves à leurs droits fondamentaux et de les dénoncer, y compris lorsqu'elles impliquent leur propre gouvernement; souligne qu'il est impératif de se doter de procédures permettant aux lanceurs d'alertes de dénoncer les violations graves des droits fondamentaux et d'offrir à ces personnes la protection dont elles ont besoin, y compris au niveau international; exprime son soutien durable au journalisme d'enquête et à la liberté des médias;
14. invite le Conseil à accélérer d'urgence ses travaux sur l'ensemble du paquet sur la protection des données et, plus précisément, sur la proposition de directive relative à la protection des données,
15. souligne la nécessité de créer un équivalent européen des commissions d'enquête et de contrôle parlementaires-judiciaires mixtes sur les services de renseignement qui existent déjà dans certains États membres;
16. charge sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur la question en collaboration avec les parlements nationaux et le groupe d'experts UE – États-Unis créé par la Commission et d'établir un rapport d'ici à la fin de l'année:
 - a) en collectant toutes les informations et les preuves pertinentes provenant de sources tant américaines qu'européennes (mission d'information);
 - b) en enquêtant sur les soupçons relatifs à des activités de surveillance qui seraient menées par les autorités des États-Unis ainsi qu'à toute activité similaire à l'initiative de certains

États membres (inventaire des responsabilités);

- c) en évaluant l'impact des programmes de surveillance en ce qui concerne: les droits fondamentaux des citoyens de l'Union (notamment le droit au respect de la vie privée et à la protection des communications, la liberté d'expression, la présomption d'innocence et le droit à un recours effectif); la protection effective des données tant au sein de l'Union que pour les citoyens de l'Union en dehors du territoire de cette dernière, en se concentrant notamment sur l'efficacité du droit de l'Union en ce qui concerne les mécanismes fondés sur l'extraterritorialité; la sécurité de l'Union à l'ère de l'informatique en nuage; la valeur ajoutée et la proportionnalité de tels programmes en ce qui concerne la lutte contre le terrorisme; la dimension extérieure de l'espace de liberté, de sécurité et de justice (en évaluant la validité des décisions en matière d'adéquation relatives aux transferts vers les pays tiers, tels que ceux mis en œuvre en vertu de l'accord sur la sphère de sécurité, des accords internationaux et d'autres instruments juridiques prévoyant une assistance et une coopération juridiques) (analyse des dommages et des risques);
 - d) en examinant les mécanismes de recours les plus appropriés en cas de violations avérées (recours administratifs et juridictionnels et régimes d'indemnisation);
 - e) en formulant des recommandations visant à prévenir de nouvelles violations et à garantir un niveau élevé et crédible de protection des données à caractère personnel des citoyens de l'Union par des moyens adéquats, notamment l'adoption d'un paquet relatif à la protection des données digne de ce nom (recommandations politiques et législation);
 - f) en formulant des recommandations visant à renforcer la sécurité informatique des institutions, organes et organismes de l'Union au moyen de règles internes de sécurité adéquates applicables aux systèmes de communication, afin de prévenir tout accès non autorisé, la divulgation ou la perte d'informations et de données à caractère personnel, et d'y remédier (réponse aux violations de la sécurité);
17. charge son Président de transmettre la présente résolution à la Commission, au Conseil, au Conseil de l'Europe, aux parlements des États membres, au président des États-Unis, au Sénat et à la Chambre des représentants des États-Unis, ainsi qu'aux ministres de la sécurité intérieure et de la justice des États-Unis.