



PARLEMENT EUROPÉEN

2009 - 2014

Document de séance

1.7.2013

B7-0341/2013

PROPOSITION DE RÉSOLUTION

déposée à la suite de déclarations du Conseil et de la Commission

conformément à l'article 110, paragraphe 2, du règlement

sur le programme de surveillance de l'agence nationale de sécurité (NSA) des États-Unis, les organismes et les programmes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union européenne (2013/2682(RSP))

Marie-Christine Vergiat, Cornelia Ernst, Kyriacos Triantaphyllides, Takis Hadjigeorgiou, Mikael Gustafsson, Willy Meyer, Nikolaos Chountis, Patrick Le Hyaric, Alda Sousa, Marisa Matias
au nom du groupe GUE/NGL

RE\942123FR.doc

PE515.885v01-00

FR

Unie dans la diversité

FR

B7-0341/2013

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

Le Parlement européen,

- vu la convention européenne des droits de l'homme, en particulier ses articles 7 et 8, et la Charte des droits fondamentaux de l'Union européenne, en particulier ses articles 48 et 52,
- vu l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire¹,
- vu la convention sur la cybercriminalité (STCE n° 185),
- vu le pacte international relatif aux droits civils et politiques, notamment son article 17 sur les immixtions dans la vie privée, la famille, le domicile ou la correspondance,
- vu la convention de Vienne sur les relations diplomatiques et en particulier ses articles 24 et 27 sur l'inviolabilité des documents et des communications diplomatiques,
- vu l'accord UE–États-Unis sur la sphère de sécurité, notamment son article 3, et la liste des adhérents à l'accord,
- vu sa résolution du 5 septembre 2001 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon)² et le rapport correspondant de sa commission temporaire sur le système d'interception Echelon (A5-0264/2001),
- vu les discussions du 15 février 2012 avec la commissaire Reding sur la législation des pays tiers et la législation de l'Union en matière de protection des données (PV 15/02/2012 – 19),
- vu la directive 2002/58/CE (directive vie privée et communications électroniques),
- vu le paquet sur la protection des données regroupant les propositions COM(2012)0011 et COM(2012)0010,
- vu les négociations en cours sur l'accord UE–États-Unis sur la protection des données à caractère personnel échangées à des fins répressives,
- vu la communication de la Commission intitulée "Exploiter le potentiel de l'informatique en nuage en Europe" (COM(2012)0529),

¹ JO L 181 du 19.7.2003, p. 34.

² JO C 72 E du 21.3.2002, p. 221.

- vu l'accord entre l'Union européenne et les États-Unis concernant le programme de surveillance du financement du terrorisme (TFTP) et l'accord entre l'Union européenne et les États-Unis concernant les données des dossiers passagers (données PNR),
 - vu l'article 110, paragraphe 2, de son règlement,
- A. considérant que, sur la base des informations divulguées par Edward Snowden, ancien agent de renseignements de la NSA qui cherche actuellement à obtenir un asile politique, les journaux du monde entier ont révélé l'existence d'un programme des États-Unis, appelé Prism, qui impliquerait la surveillance à grande échelle des communications de citoyens non américains, et donc également de citoyens européens;
- B. considérant que la commissaire Reding a adressé un courrier au procureur général des États-Unis, Eric Holder, pour lui faire part des inquiétudes européennes, lui demander des clarifications et des explications sur le programme Prism et les autres programmes de même nature permettant la collecte et la recherche de données, et s'enquérir de la base juridique autorisant la mise en œuvre de tels programmes;
- C. considérant que d'après les informations divulguées, certains États membres de l'Union auraient coopéré au programme Prism conduit par les États-Unis ou auraient mis en place des programmes de collecte de renseignements similaires, tels que le projet "Tempora" mené par le GCHQ (agence britannique d'espionnage électronique); considérant que des informations parues dans la presse ont révélé que le GCHQ s'était connecté à des câbles sous-marins à fibres optiques pour avoir accès aux conversations téléphoniques et aux communications sur internet dans le cadre d'un programme portant le nom de code Tempora, en se fondant sur le paragraphe 4 de la section 8 de la loi portant réglementation des pouvoirs d'enquête (RIPA), qui permet au ministre britannique des affaires étrangères de délivrer une autorisation d'interception à large échelle de certaines catégories d'informations liées au terrorisme ou à la criminalité organisée; considérant que des éléments de preuve indiquent que les États-Unis ont été impliqués dans des activités d'espionnage ciblant le personnel diplomatique des représentations permanentes des États membres, ainsi que dans les bureaux des institutions de l'Union européenne; considérant, à cet égard, que le bureau d'un député au Parlement européen a été mis sous écoute par les services de sécurité britanniques;
- D. considérant que la collecte et le stockage massifs de données à caractère personnel sont contraires, en soi, aux principes de proportionnalité et de nécessité consacrés dans la CEDH, en vertu de laquelle toute restriction aux droits fondamentaux doit constituer une mesure proportionnelle et nécessaire dans une société démocratique;
- E. considérant que l'article 48 de la Charte met l'accent sur le principe de présomption d'innocence, et considérant qu'en l'absence d'accusation ou de poursuites formelles, les activités de surveillance et les actions policières préventives comportent un risque élevé de violation du principe de présomption d'innocence dès lors qu'elles sont menées à grande échelle sans qu'aucune infraction pénale n'ait été détectée au préalable;
- F. considérant que l'article 52 de la Charte dispose: "Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité,

des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui";

- G. considérant que la Cour européenne des droits de l'homme a, à juste titre, prévenu qu'un système de surveillance secrète destiné à protéger la sécurité nationale "crée un risque de saper, voire de détruire, la démocratie au motif de la défendre" et que "la législation elle-même créée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance [...]";
- H. 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; considérant que la Commission est tenue, au titre de l'article 3, de dénoncer ou de suspendre l'accord si ses dispositions ne sont pas respectées;
- I. considérant que le paquet relatif à la protection des données est actuellement débattu par les deux colégislateurs;
- J. considérant qu'il existe de sérieux doutes quant à la volonté de certains États membres, et en particulier du Royaume-Uni, d'adopter une attitude constructive concernant la mise en œuvre de la directive relative à la protection des données dans le secteur répressif afin d'améliorer les normes en matière de protection des données dans le domaine de la coopération judiciaire et policière;
- K. considérant que la commissaire Viviane Reding a adressé en novembre 2011 à ses collègues un projet de règlement en matière de protection des données qui contenait une disposition conditionnant la communication des données des utilisateurs aux autorités de pays tiers à l'existence d'une base juridique telle qu'un accord d'entraide judiciaire et à l'autorisation de l'autorité compétente chargée de la protection des données;
- L. considérant que les pressions très fortes exercées par les États-Unis pourraient être à l'origine de la suppression de ces dispositions de la proposition définitive de la Commission;
- M. considérant que les États membres de l'Union européenne sont tenus de respecter les valeurs fondamentales consacrées à l'article 2 du traité sur l'Union européenne, de même que les droits à la vie privée et à la protection des données, tels qu'inscrits dans la Charte des droits fondamentaux;
- N. considérant que le Parlement européen a rejeté la proposition de la Commission de mettre en place un système PNR à l'échelle européenne, compte tenu de l'existence de sérieux doutes quant à la légalité, à la nécessité et à la proportionnalité d'un tel système;
- O. considérant que la directive sur la conservation des données a été contestée devant plusieurs cours constitutionnelles et a été portée devant la Cour de justice européenne en vue d'obtenir une décision préjudicielle, ce pour des motifs liés aux principes de proportionnalité et de nécessité;
- P. considérant que le nouveau règlement Europol fait actuellement l'objet de discussions au

sein du Parlement européen;

1. se déclare profondément choqué par les révélations concernant l'existence du programme Prism qui, si les informations disponibles à ce jour devaient être confirmées, impliquerait une violation des droits fondamentaux à la vie privée et à la protection des données des citoyens de l'Union, ainsi que le non-respect des principes fondamentaux de nécessité et de proportionnalité;
2. estime qu'il y a raisonnablement lieu de croire que les communications du Parlement européen, des députés et du personnel ont été interceptées par le programme Tempora, et ce en violation des obligations qui s'imposent au Royaume-Uni en matière de droits de l'homme; enjoint en conséquence à son service juridique d'examiner les possibilités juridiques d'intenter une action contre le gouvernement britannique, notamment auprès de la Cour européenne des droits de l'homme;
3. demande une suspension immédiate des négociations avec les États-Unis concernant l'accord relatif à un partenariat transatlantique sur le commerce et les investissements; prie la Commission de suspendre toutes nouvelles négociations concernant l'accord de libre échange (ALE) ou sa mise en œuvre avec les États-Unis jusqu'à ce que le Parlement ait été pleinement informé sur ce sujet, que l'accord UE-États-Unis relatif à la protection des données ait été conclu de manière satisfaisante et que de réelles garanties aient été fournies concernant l'interruption effective de toute activité de surveillance illégale des entreprises, des citoyens et des institutions et représentations diplomatiques de l'Union européenne;
4. rappelle le principe de présomption d'innocence, qui est un pilier essentiel de l'état de droit dans les sociétés démocratiques; se déclare vivement opposé à la multiplication des activités dites de "prévention policière", qui renversent le principe de présomption d'innocence et placent tout le monde dans une position de criminel potentiel;
5. est profondément préoccupé par les politiques de l'Union européenne et des États membres de plus en plus axées sur la sécurité et qui portent gravement atteinte aux droits fondamentaux et aux libertés des citoyens et des résidents de l'Union européenne; est strictement opposé à l'approche fondée sur la peur qui semble guidée par l'idée selon laquelle une sécurité de plus en plus poussée permettra automatiquement de créer une zone de liberté et de justice;
6. invite les autorités américaines à fournir à leurs partenaires européens, à l'échelon tant de l'Union que des États membres, des informations sur la portée du programme Prism, sur l'existence d'autres programmes similaires et sur le niveau d'implication des États membres de l'Union; invite aussi les États membres à dévoiler l'existence de tout programme de cette nature, qu'il soit déjà en fonctionnement ou en phase d'élaboration;
7. rappelle les limites fixées par la jurisprudence de la Cour européenne des droits de l'homme en ce qui concerne les activités de surveillance des personnes par l'État, à savoir que toute atteinte au droit fondamental à la vie privée des citoyens doit être proportionnée et nécessaire dans une société démocratique, qu'elle ne peut être autorisée que dans les limites de la loi et qu'elle doit faire l'objet d'un contrôle démocratique et judiciaire adéquat;

8. rappelle le principe de proportionnalité, consacré dans la Convention sur la cybercriminalité, qui a été signée par les États-Unis et qui prévoit, à son article 15, l'obligation de respecter le principe de proportionnalité lors de la mise en œuvre de mesures visant à assurer la cybersécurité;
9. réaffirme le droit des citoyens de connaître l'existence d'actes législatifs ou de politiques susceptibles d'entraîner une limitation de leurs droits et libertés fondamentaux, ainsi que de demander des comptes à ceux qui les ont mis en œuvre;
10. demande au Conseil d'accélérer ses travaux sur la directive relative à la protection des données, s'agissant d'un instrument absolument indispensable pour garantir l'état de droit et protéger les droits des citoyens dans le domaine répressif;
11. invite les colégislateurs de l'Union à adopter une approche horizontale à l'égard des propositions législatives relatives à des politiques de répression qui impliquent la collecte et le stockage de données à caractère personnel, en particulier les propositions de l'Union concernant les données PNR et les propositions d'Europol, au lieu d'opter pour une approche fragmentaire susceptible de créer un enchevêtrement inexploitable de normes et de principes incohérents;
12. demande que le Parlement prenne officiellement position contre l'adoption de toutes nouvelles mesures répressives impliquant la collecte et le stockage de données avant l'adoption de la directive relative à la protection des données;
13. souligne, à cet égard, que selon les rapports d'évaluation de l'Autorité de contrôle commune d'Europol, l'accord UE–États-Unis sur le programme de surveillance du financement du terrorisme (TFTP) permet le transfert en masse de données à caractère personnel et risque donc d'être condamné par des cours constitutionnelles au motif qu'il ne respecte pas le principe de proportionnalité consacré dans la CEDH;
14. souligne que les entreprises qui offrent des services aux citoyens de l'Union sont tenues de se conformer au droit de l'Union, en particulier à la législation relative à la protection des données, et est hostile au concept d'autorégulation par les entreprises dès lors qu'il s'agit des droits fondamentaux;
15. 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;
16. souligne que les entreprises offrant des services aux citoyens et aux résidents de l'Union qui relèvent d'une juridiction d'un pays tiers devraient alerter de manière claire et visible les utilisateurs concernés quant à la possibilité que leurs données soient traitées par des agences répressives et de renseignement à la suite d'ordres ou d'injonctions dictés secrètement;
17. prend acte des initiatives prises par certaines entreprises en ligne qui participent activement à dévoiler l'identité des autorités publiques qui ont demandé et obtenu l'accès à des données d'utilisateurs; invite instamment les autres entreprises de ce type à suivre leur

exemple sans attendre;

18. met en exergue la nécessité de procédures permettant aux lanceurs d'alerte de dévoiler l'existence de systèmes de surveillance secrets sans craindre de conséquences juridiques; invite les États membres, en coordination avec le SEAE, à offrir l'asile politique à Edward Snowden, qui a eu le courage de dévoiler une telle situation de violation systématique et à grande échelle des droits fondamentaux, ainsi qu'à traiter sa demande rapidement;
19. demande aux représentants de l'Union de débattre avec leurs homologues américains de la question des règles applicables en matière de protection des données dans le cadre de leurs relations bilatérales et, dans ce contexte, de veiller à ce que les droits fondamentaux et le droit à la vie privée et à la protection des données soient respectés par les deux parties; invite la Commission à recourir à tous les outils de négociation dont elle dispose pour garantir la réalisation de cet objectif;
20. déplore l'utilisation abusive systématique du concept de "sécurité nationale" qui sert à couvrir des intérêts économiques nationaux ou les intérêts politiques des personnes qui sont au pouvoir; condamne l'utilisation de cette notion vague pour justifier l'espionnage de citoyens et de diplomates de l'Union;
21. souligne la nécessité de créer un équivalent européen des commissions d'enquête et de contrôle parlementaires-judiciaires mixtes sur les services de renseignements qui existent déjà dans certains États membres;
22. charge sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur ce sujet et d'en rendre compte à la plénière d'ici la fin de l'année, en évaluant notamment la possibilité de créer une commission d'enquête et de contrôle au niveau de l'Union qui serait chargée d'examiner la coopération entre les services de renseignement des États membres et l'utilisation qui est faite des données à caractère personnel des citoyens de l'Union;
23. charge son Président de transmettre la présente résolution au Conseil, à la Commission, 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, au Secrétaire d'État des États-Unis à la sécurité intérieure, ainsi qu'au procureur général des États-Unis.