PARLEMENT EUROPÉEN 2009 - 2014

Commission des libertés civiles, de la justice et des affaires intérieures

2013/2188(INI)

8.1.2014

PROJET DE RAPPORT

sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures
(2013/2188(INI))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteur: Claude Moraes

PR_INI

SOMMAIRE

Page

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI))

Le Parlement européen,

– vu le traité sur l'Union européenne (traité UE), et notamment ses articles 2, 3, 4, 5, 6, 7, 10, 11 et 21,

– vu le traité sur le fonctionnement de l'Union européenne (traité FUE) et, en particulier, ses articles 15, 16 et 218 et son titre V,

– vu le protocole n° 36 sur les dispositions transitoires, notamment son article 10, ainsi que la déclaration 50 relative à ce protocole,

– vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 et 52,

– vu la convention européenne des droits de l'homme (CEDH), et notamment ses articles 6, 8, 9, 10 et 13, ainsi que ses protocoles annexes,

– vu la Déclaration universelle des droits de l'homme, et notamment ses articles 7, 8, 10, 11, 12 et 14[1],

– vu le Pacte international relatif aux droits civils et politiques, notamment ses articles 14, 17, 18 et 19,

– vu la convention du Conseil de l'Europe pour la protection des données (STE n° 108) et le protocole additionnel du 8 novembre 2001 à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181),

– vu la convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185),

– vu le rapport du rapporteur spécial des Nations unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, soumis le 17 mai 2010[2],

– vu le rapport du rapporteur spécial des Nations unies sur la promotion et la protection de la liberté d'opinion et d'expression, soumis le 17 avril 2013[3],

[1] http://www.un.org/fr/documents/udhr/.
[2] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement.
[3] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

– vu les lignes directrices sur les droits de l'homme et la lutte contre le terrorisme adoptées par le Comité des ministres du Conseil de l'Europe en date du 11 juillet 2002,

– vu la déclaration de Bruxelles du 1er octobre 2010, adoptée lors de la 6e conférence des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne,

– vu la résolution 1954(2013) de l'Assemblée parlementaire du Conseil de l'Europe sur la sécurité nationale et l'accès à l'information,

– vu le rapport sur le contrôle démocratique des services de sécurité adopté par la Commission de Venise le 11 juin 2007[1], dont il attend avec grand intérêt la mise à jour, prévue au printemps 2014,

– vu les témoignages des représentants des commissions de contrôle des services de renseignement de Belgique, des Pays-Bas, du Danemark et de Norvège,

– vu les affaires introduites auprès des tribunaux français[2], polonais et britanniques[3], ainsi qu'auprès de la Cour européenne des droits de l'homme[4], en ce qui concerne les systèmes de surveillance de masse,

– vu la convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, et en particulier son titre III[5],

– vu la décision 520/2000/CE de la Commission, du 26 juillet 2000, relative à la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique,

– vu les rapports d'évaluation de la Commission sur l'application des principes de la "sphère de sécurité" du 13 février 2002 (SEC(2002)196) et du 20 octobre 2004 (SEC(2004)1323),

– vu la communication de la Commission du 27 novembre 2013 (COM(2013)847) sur le fonctionnement de la "sphère de sécurité" du point de vue des citoyens européens et des entreprises établies dans l'Union et la communication de la Commission du 27 novembre 2013 sur le rétablissement de la confiance à l'égard des flux de données entre l'Union européenne et les États-Unis (COM(2013)846),

– vu la résolution du Parlement européen du 5 juillet 2000 sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes

[1] http://www.venice.coe.int/webforms/documents/default.aspx?ref=cdl-ad(2007)016&lang=fr.
[2] La Fédération internationale des ligues des droits de l'homme et la Ligue française pour la défense des droits de l'homme et du citoyen contre X; Tribunal de grande instance de Paris.
[3] Affaires introduites par Privacy International and Liberty auprès de l'Investigatory Powers Tribunal.
[4] Requête conjointe au titre de l'article 34 introduite par Big Brother Watch, Open Rights Group, English Pen, Dr Constanze Kurz (parties demanderesses) contre le Royaume-Uni (partie défenderesse).
[5] JO C 197 du 12.7.2000, p.1.

de la "sphère de sécurité" et les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis, qui a estimé que la pertinence du système ne pouvait être confirmée[1], ainsi que les avis du groupe de travail "Article 29", en particulier l'avis 4/2000 du 16 mai 2000[2],

– vu les accords conclus entre les États-Unis d'Amérique et l'Union européenne en 2004, 2007[3] et 2012[4] sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure,

– vu l'examen conjoint de la mise en œuvre de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert des données des dossiers passagers au ministère américain de la sécurité intérieure[5] accompagnant le rapport de la Commission au Parlement européen et au Conseil sur l'examen conjoint (COM(2013)844),

– vu l'avis de l'avocat général Cruz Villalón concluant que la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications est globalement incompatible avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et que son article 6 est incompatible avec les articles 7 et 52, paragraphe 1, de la charte[6];

– vu la décision 2010/412/UE du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP)[7], ainsi que les déclarations de la Commission et du Conseil qui l'accompagnaient,

– vu l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire[8],

– vu les négociations en cours sur un accord-cadre entre l'Union européenne et les États-Unis d'Amérique relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et judiciaire en matière pénale (l'"l'accord-cadre"),

– vu le règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays

[1] JO C 121 du 24.4.2001, p.152.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32fr.pdf.
[3] JO L 204 du 4.8.2007, p. 18.
[4] JO L 215 du 11.8.2012, p. 5.
[5] SEC(2013)630 du 27.11.2013.
[6] Avis de l'avocat général Cruz Villalón du 12 décembre 2013 dans l'affaire C-293/12.
[7] JO L 195 du 27.7.2010, p. 3.
[8] JO L 181 du 19.7.2003, p. 34.

tiers, ainsi que des actions fondées sur elle ou en découlant[1];

– vu la déclaration de la présidente de la République fédérale du Brésil lors de l'ouverture de la 68e session de l'Assemblée générale des Nations unies le 24 septembre 2013 et les travaux réalisés par la commission parlementaire d'enquête sur l'espionnage créée par le Sénat fédéral du Brésil,

– vu le *Patriot Act* des États-Unis, signé par le président George W. Bush le 26 octobre 2001,

– vu la loi de 1978 sur la surveillance et le renseignement étranger (FISA) et la loi de 2008 portant modification de la FISA,

– vu le décret exécutif n° 12333 adopté par le président américain en 1981 et modifié en 2008,

– vu les propositions législatives en cours d'examen par le Congrès américain, notamment le projet de loi sur la liberté (*US Freedom Act*),

– vu les études réalisées par le Conseil de surveillance de la vie privée et des libertés civiles, le Conseil de sécurité nationale des États-Unis et le groupe d'étude du président sur la révision des renseignements et des technologies, en particulier le rapport publié par ce dernier le 12 décembre 2013 et intitulé "Liberty and Security in a Changing World",

– vu la décision du tribunal de district des États-Unis pour le district de Columbia, Klayman e.a. /Obama e.a., action civile n° 13-0851 du 16 décembre 2013,

– vu le rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail UE-États-Unis sur la protection des données du 27 novembre 2013[2],

– vu ses résolutions du 5 septembre 2001 et du 7 novembre 2002 sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON),

– vu sa résolution du 21 mai 2013 sur la Charte de l'UE: ensemble de normes pour la liberté des médias à travers l'UE[3],

– vu sa résolution 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, dans laquelle il chargeait sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur cette question[4],

– vu sa résolution du 23 octobre 2013 sur la criminalité organisée, la corruption et le

[1] JO L 309 du 29.11.1996, p. 1.
[2] Document du Conseil 16987/13.
[3] Textes adoptés de cette date, P7_TA(2013)0203.
[4] Textes adoptés de cette date, P7_TA(2013)0322.

blanchiment de capitaux: recommandations sur des actions et des initiatives à entreprendre[1],

– vu sa résolution du 23 octobre 2013 sur la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine[2],

– vu sa résolution du 10 décembre 2013 sur l'exploitation du potentiel de l'informatique en nuage[3],

– vu l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement européen et au traitement par celui-ci des informations classifiées détenues par le Conseil concernant des questions autres que celles relevant de la politique étrangère et de sécurité commune[4],

– vu l'annexe VIII de son règlement,

– vu l'article 48 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A70000/2013),

Les incidences de la surveillance de masse

A. considérant que les liens entre l'Europe et les États-Unis d'Amérique sont basés sur l'esprit et les principes de démocratie, de liberté, de justice et de solidarité;

B. considérant que la confiance et la compréhension mutuelles constituent des facteurs clés dans le dialogue transatlantique;

C. considérant qu'en septembre 2001, le monde est entré dans une nouvelle phase qui a eu pour effet de faire figurer la lutte contre le terrorisme parmi les grandes priorités de la plupart des gouvernements; considérant que les révélations basées sur les documents divulgués par Edward Snowden, ancien employé de la NSA, ont contraint des dirigeants démocratiquement élus à traiter les problèmes posés par les capacités croissantes des agences de renseignement dans le cadre de leurs activités de surveillance et leurs conséquences pour l'état de droit dans une société démocratique;

D. considérant que les révélations faites depuis juin 2013 ont suscité de nombreuses inquiétudes au sein de l'Union en ce qui concerne:

- la portée des systèmes de surveillance révélée aux États-Unis et dans les États membres de l'Union;
- le risque élevé de violation des normes juridiques et des droits fondamentaux de l'Union européenne ainsi que des normes européennes en matière de

[1] Textes adoptés de cette date, P7_TA(2013)0444.
[2] Textes adoptés de cette date, P7_TA(2013)0449.
[3] Textes adoptés de cette date, P7_TA(2013)0535.
[4] JO C 353 E du 3.12.2013, pp. 156-167.

protection des données;

- le niveau de confiance entre les partenaires transatlantiques que sont l'Union européenne et les États-Unis;
- le degré de coopération et d'implication de certains États membres de l'Union dans des programmes de surveillance américains ou programmes équivalents au niveau national, comme l'ont révélé les médias;
- le niveau de contrôle et de surveillance effective exercé par les autorités politiques américaines et certains États membres de l'Union européenne sur leurs services de renseignement;
- la possibilité que ces activités de surveillance de masse soient utilisées pour des raisons autres que la sécurité nationale et la lutte contre le terrorisme à proprement parler, par exemple à des fins d'espionnage économique et industriel ou de profilage pour des motifs politiques;
- les rôles et degrés d'implication respectifs des agences de renseignement et des entreprises informatiques et de télécommunications privées;
- les frontières de plus en plus floues entre l'application de la législation et les activités de renseignement, avec pour effet que chaque citoyen est traité comme un suspect;
- les menaces relatives à la vie privée à l'heure du numérique;

E. considérant que l'ampleur sans précédent des activités d'espionnage révélées nécessite une enquête approfondie de la part des autorités américaines, des institutions européennes et des gouvernements et parlements nationaux des États membres;

F. considérant que les autorités américaines ont réfuté certaines des informations divulguées, mais n'ont pas contesté la grande majorité de celles-ci; considérant que le débat public a pris une grande ampleur aux États-Unis ainsi que dans un petit nombre d'États membres de l'Union européenne; considérant que les gouvernements européens restent encore trop souvent silencieux et ne lancent pas d'enquêtes adéquates;

G. considérant qu'il est du devoir des institutions européennes de veiller à ce que le droit de l'Union soit pleinement mis en œuvre dans l'intérêt des citoyens européens et que la force juridique des traités de l'Union ne soit pas compromise par un mépris des effets extraterritoriaux des normes ou actions des pays tiers;

Évolution de la réforme des services de renseignement aux États-Unis

H. considérant que le tribunal de district des États-Unis pour le district de Columbia a jugé, dans sa décision du 16 décembre 2013, que la collecte massive de métadonnées par la NSA contrevenait au quatrième amendement à la constitution des États-Unis[1];

I. considérant qu'une décision du tribunal de district de la région orientale de l'État du

[1] Klayman e.a./Obama e.a.., action civile n° 13-0851, 16 décembre 2013.

Michigan a considéré que le quatrième amendement exigeait l'existence d'un caractère raisonnable pour toutes les recherches effectuées, des mandats préalables pour toutes les recherches raisonnables, des mandats basés sur une cause probable préexistante, ainsi qu'une prise en considération des particularités des personnes, des endroits et des objets et l'interposition d'un magistrat neutre entre les agents répressifs du pouvoir exécutif et les citoyens[1];

J. considérant que dans son rapport du 12 décembre 2013, le groupe d'étude du président sur la révision des renseignements et des technologies propose 45 recommandations au président des États-Unis; considérant que ces recommandations soulignent la nécessité de protéger à la fois la sécurité nationale et la vie privée et les libertés civiles; considérant qu'il invite, à cet égard, le gouvernement américain à mettre fin dans les plus brefs délais à la collecte massive d'enregistrements téléphoniques de citoyens américains au titre de la section 215 du *Patriot Act*, à entreprendre un examen approfondi de la NSA et du cadre juridique américain en matière de renseignement afin de garantir le respect du droit à la vie privée, à cesser les efforts visant à saboter ou rendre vulnérables les logiciels commerciaux (chevaux de Troie et logiciels malveillants), à accroître l'utilisation du cryptage, particulièrement en ce qui concerne les données en transit, et à ne pas saper les efforts visant à créer des normes de cryptage, à nommer un représentant de l'intérêt public chargé de défendre la vie privée et les libertés civiles devant le tribunal de la surveillance du renseignement à l'étranger (*Foreign Intelligence Surveillance Court*), à conférer au Conseil de surveillance de la vie privée et des libertés civiles le pouvoir de superviser les activités des services de renseignement à des fins de renseignement étranger, et pas uniquement à des fins de lutte contre le terrorisme, et de recevoir les plaintes de lanceurs d'alerte, à utiliser les traités en matière d'entraîne judiciaire pour obtenir des communications électroniques et à ne pas utiliser la surveillance pour voler des secrets industriels ou commerciaux;

K. considérant qu'en ce qui concerne les activités de renseignement relatives à des ressortissants non américains au sens de la section 702 de la FISA, les recommandations adressées au président des États-Unis reconnaissent la question fondamentale du respect de la vie privée et de la dignité humaine consacré à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques; considérant que ces recommandations ne préconisent pas d'octroyer aux ressortissants non américains les mêmes droits et protections qu'aux ressortissants américains;

Cadre juridique

Droits fondamentaux

L. considérant que le rapport sur les conclusions des coprésidents de l'Union du groupe de travail ad hoc UE-États-Unis sur la protection des données donne un aperçu de la situation juridique aux États-Unis, mais n'a pas suffisamment contribué à établir les faits relatifs aux programmes de surveillance américains; considérant qu'aucune information n'a été donnée au sujet du groupe de travail dit de "deuxième voie", dans le cadre duquel les États membres discutent bilatéralement avec les autorités

[1] ACLU/NSA n° 06-CV-10204, 17 août 2006.

américaines des questions ayant trait à la sécurité nationale;

M. considérant que les droits fondamentaux, notamment la liberté d'expression, de la presse, de pensée, de conscience, de religion et d'association, le respect de la vie privée, la protection des données, ainsi que le droit à un recours effectif, la présomption d'innocence et le droit à un procès équitable et à la non-discrimination, consacrés dans la Charte des droits fondamentaux de l'Union européenne et la convention européenne des droits de l'homme, constituent des pierres angulaires de la démocratie;

Compétences de l'Union dans le domaine de la sécurité

N. considérant qu'en vertu de l'article 67, paragraphe 3, du traité FUE, l'Union européenne "œuvre pour assurer un niveau élevé de sécurité"; considérant que les dispositions du traité (notamment l'article 4, paragraphe 2, traité UE, ainsi que les articles 72 et 73 du traité FUE) signifient que l'Union européenne dispose de certaines compétences sur les questions ayant trait à la sécurité collective de l'Union; considérant que l'Union exerce sa compétence dans les domaines relatifs à la sécurité intérieure en adoptant un certain nombre d'instruments législatifs et en concluant des accords internationaux (sur les données PNR, le TFTP) visant à lutter contre la grande criminalité et le terrorisme ainsi qu'en élaborant une stratégie pour la sécurité intérieure et des agences travaillant dans ce domaine;

O. considérant que les notions de "sécurité nationale", de "sécurité intérieure", de "sécurité intérieure de l'Union" et de "sécurité internationale" se recoupent; considérant que la convention de Vienne sur le droit des traités, le principe de coopération loyale entre États membres de l'Union et le principe du droit international humanitaire consistant à interpréter étroitement toute dérogation suggèrent une interprétation restrictive de la notion de "sécurité nationale" et exigent que les États membres s'abstiennent d'empiéter sur les compétences de l'Union;

P. considérant qu'aux termes de la CEDH, les agences des États membres et même les parties privées agissant dans le domaine de la sécurité nationale sont également tenues de respecter les droits consacrés par la CEDH, que ce soient ceux de leurs propres citoyens ou des citoyens des autres États; que cela s'applique également à la coopération avec les autorités des autres États dans le domaine de la sécurité nationale;

Extraterritorialité

Q. considérant que l'application extraterritoriale, par un pays tiers, de ses lois, règlements et autres instruments législatifs ou exécutifs dans des situations relevant de la compétence de l'Union européenne ou de ses États membres peut avoir des répercussions sur l'ordre juridique établi et l'état de droit, voire violer le droit international ou européen, notamment les droits de personnes physiques et morales, en tenant compte de l'étendue et de l'objectif officiel ou officieux d'une telle application; considérant que, dans ces circonstances exceptionnelles, il est nécessaire d'entreprendre une action au niveau de l'Union afin de garantir le respect de l'état de droit et des droits des personnes physiques ou morales dans l'Union, notamment en éliminant, en neutralisant, en bloquant ou en contrecarrant de toute autre manière les

effets de la législation étrangère en cause;

Transferts internationaux de données

R. considérant que le transfert de données à caractère personnel par les institutions, organes, bureaux ou agences de l'Union ou par les États membres vers les États-Unis à des fins répressives en l'absence de garanties et de protections adéquates concernant le respect des droits fondamentaux des citoyens de l'Union, notamment les droits à la vie privée et à la protection des données à caractère personnel, engagerait la responsabilité de l'institution, l'organe, le bureau ou l'agence ou l'État membre en question, au titre de l'article 340 du traité FUE ou de la jurisprudence constante de la CJUE[1] pour violation du droit de l'Union – y compris toute violation des droits fondamentaux consacrés dans la Charte de l'Union européenne;

Transferts vers les États-Unis au titre de la "sphère de sécurité" des États-Unis

S. considérant que le cadre juridique des États-Unis en matière de protection des données ne garantit pas un niveau adéquat de protection pour les citoyens de l'Union européenne;

T. considérant qu'afin de permettre aux responsables de traitements de données de l'Union de transférer des données à caractère personnel vers des entités aux États-Unis, la Commission, dans sa décision 520/2000/CE, a déclaré pertinente la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis, pour les données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis qui se sont engagées à appliquer les principes de la "sphère de sécurité";

U. considérant que dans sa résolution du 5 juillet 2000, le Parlement européen a exprimé des doutes et des craintes en ce qui concerne la pertinence des principes de la "sphère de sécurité" et a appelé la Commission à revoir la décision sans délai, à la lumière des expériences acquises et de l'évolution législative éventuelle;

V. considérant qu'en vertu de la décision 520/2000/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les flux de données vers une organisation adhérant aux principes de la "sphère de sécurité" afin de protéger les individus en ce qui concerne le traitement de leurs données personnelles dans les cas où il est fort probable que les principes sont violés ou lorsque la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves;

W. considérant que la décision 520/2000/CE de la Commission indique également que lorsque les informations recueillies montrent qu'un quelconque organisme chargé de faire respecter les principes ne remplit pas efficacement sa mission, la Commission informe le ministère américain du commerce et, si nécessaire, propose un projet de mesures à prendre en vue d'abroger ou de suspendre ladite décision ou d'en limiter la portée;

[1] Voir notamment les affaires jointes C-6/90 et C-9/90, Francovich e.a./ Italie, arrêt du 28 mai 1991.

X. considérant que dans ses deux premiers rapports sur l'application des principes de la "sphère de sécurité", publiés en 2002 et 2004, la Commission a relevé plusieurs lacunes au niveau de l'application desdits principes et adressé plusieurs recommandations aux autorités américaines en vue de les corriger;

Y. considérant que dans son troisième rapport de mise en œuvre, du 27 novembre 2013, neuf ans après le deuxième rapport et sans qu'aucune des lacunes recensées dans ce rapport ait été rectifiée, la Commission a relevé d'autres lacunes et faiblesses importantes concernant les principes de la "sphère de sécurité" et a conclu que l'application actuelle ne pouvait se poursuivre; considérant que la Commission a souligné que le vaste accès accordé aux agences de renseignement américaines aux données transférées vers les États-Unis par des entités adhérant aux principes de la "sphère de sécurité" pose d'autres questions majeures quant à la continuité de la protection des données de citoyens européens; considérant que la Commission a adressé 13 recommandations aux autorités américaines et s'est engagée à formuler, d'ici à l'été 2014 et en collaboration avec les autorités américaines, des solutions applicables dans les plus brefs délais et qui constitueront la base d'un examen approfondi du fonctionnement des principes de la "sphère de sécurité";

Z. considérant que du 28 au 31 octobre 2013, la délégation de la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE) du Parlement européen à Washington D.C. a rencontré le ministère américain du commerce et la commission fédérale du commerce des États-Unis; considérant que le ministère du commerce a reconnu l'existence d'organisations ayant adhéré aux principes de la "sphère de sécurité", mais dont le statut n'est pas à jour, ce qui signifie qu'elles ne satisfont pas aux exigences de la "sphère de sécurité" alors qu'elles continuent à recevoir des données à caractère personnel provenant de l'Union européenne; considérant que la commission fédérale du commerce a admis la nécessité de réviser les principes de la "sphère de sécurité" afin de les améliorer, surtout en ce qui concerne les mécanismes de plaintes et de résolution alternative des conflits;

AA. considérant que les principes de la "sphère de sécurité" peuvent être limités "dans la mesure du nécessaire pour répondre aux exigences relatives à la sécurité nationale, l'intérêt public ou le respect des lois"; considérant que, en tant que dérogation à un droit fondamental, celle-ci doit toujours être interprétée de manière restrictive et être limitée à ce qui est nécessaire et proportionné dans une société démocratique, et que la législation doit clairement établir les conditions et garanties permettant de rendre cette restriction légitime; considérant qu'une telle dérogation ne doit pas être utilisée d'une manière qui nuirait à la protection apportée par la législation de l'Union européenne sur la protection des données et les principes de la "sphère de sécurité";

AB. considérant que le vaste accès accordé aux agences de renseignement américaines a gravement sapé la confiance transatlantique et a eu des incidences négatives sur la confiance accordée aux organisations américaines actives dans l'Union européenne; considérant que cette situation est encore aggravée par l'absence de moyens de recours judiciaire ou administratif dans le droit américain pour les citoyens de l'Union européenne, en particulier dans des cas d'activités de surveillance menées à des fins de renseignement;

Transferts vers des pays tiers dans le cadre d'une décision relative à la pertinence de la protection

AC. considérant que selon les informations communiquées et les conclusions de l'enquête réalisée par la commission LIBE, les agences nationales de sécurité néozélandaise et canadienne ont été impliquées à un niveau important dans la surveillance de masse des communications électroniques et ont activement coopéré avec les États-Unis dans le cadre du programme dit "Five Eyes" (cinq yeux), et pourraient avoir échangé entre elles des données à caractère personnel de citoyens européens transférées depuis l'Union européenne;

AD. considérant que les décisions 2013/65/UE[1] du 19 décembre 2012 et 2002/2/CE, du 20 décembre 2001[2], de la Commission ont déclaré adéquat le niveau de protection garanti par les lois néozélandaise et canadienne relatives à la protection des informations à caractère personnel et aux documents électroniques; considérant que les révélations susmentionnées nuisent aussi gravement à la confiance vis-à-vis des systèmes juridiques de ces pays en ce qui concerne la continuité de la protection accordée aux citoyens de l'Union européenne; considérant que la Commission ne s'est pas penchée sur cet aspect;

Transferts fondés sur des clauses contractuelles et d'autres instruments

AE. considérant qu'en vertu de la directive 95/46/CE, les transferts internationaux vers des pays tiers peuvent également être réalisés au titre d'un instrument spécifique dans le cadre duquel le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants;

AF. considérant que ces garanties peuvent notamment résulter de clauses contractuelles appropriées;

AG. considérant que la directive 95/46/CE permet à la Commission de décider que des clauses contractuelles types spécifiques apportent les garanties suffisantes requises par la directive et que sur cette base, la Commission a adopté trois modèles de clauses contractuelles types pour les transferts vers des responsables du traitement et des sous-traitants (et sous-traitants ultérieurs) dans des pays tiers;

AH. considérant qu'en vertu des décisions de la Commission établissant les clauses contractuelles types, les autorités compétentes des États membres peuvent exercer leurs compétences pour suspendre le transfert de données lorsqu'il est établi que le droit auquel l'importateur de données est soumis oblige ce dernier à déroger aux règles pertinentes de protection des données au-delà des restrictions nécessaires dans une société démocratique comme le prévoit l'article 13 de la directive 95/46/CE lorsque ces obligations risquent d'altérer considérablement les garanties offertes par la législation applicable en matière de protection des données ou les clauses contractuelles types, ou lorsqu'il est fort probable que les clauses contractuelles types

[1] JO L 28 du 30.1.2013, p. 12.
[2] JO L 2 du 4.1.2002, p. 13.

figurant dans l'annexe ne sont pas ou ne seront pas respectées et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves;

AI. considérant que les autorités nationales de protection des données ont établi des règles d'entreprise contraignantes (REC) en vue de faciliter les transferts internationaux au sein des entreprises multinationales en apportant les garanties adéquates en ce qui concerne la protection de la vie privée et des libertés et droits fondamentaux des personnes ainsi qu'en ce qui concerne l'exercice de ces droits; considérant qu'avant d'être appliquées, les REC doivent être autorisées par les autorités compétentes des États membres, une fois que celles-ci ont évalué leur conformité avec la législation de l'Union sur la protection des données;

Transferts basés sur les accords TFTP et PNR

AJ. considérant que dans sa résolution du 23 octobre 2013, le Parlement européen s'est dit fortement préoccupé par les documents révélés sur les activités de la NSA en ce qui concerne l'accès direct aux données de messagerie financière et aux données connexes, qui constituerait une infraction claire à l'accord, et notamment à son article premier;

AK. considérant que le Parlement européen a demandé à la Commission de suspendre l'accord et a réclamé un accès immédiat à toutes les informations et tous les documents pertinents pour ses délibérations;

AL. considérant qu'à la suite des allégations publiées par les médias, la Commission a décidé d'entamer des consultations avec les États-Unis conformément à l'article 19 de l'accord TFTP; considérant que le 27 novembre 2013, la commissaire Malmström a informé la commission LIBE qu'après avoir rencontré les autorités américaines et compte tenu des réponses apportées par celles-ci dans leurs lettres et pendant leurs réunions, la Commission avait décidé de ne pas poursuivre les consultations au motif qu'aucun élément ne démontrait que le gouvernement américain avait agi contrairement aux dispositions de l'accord et que les États-Unis avaient fourni la garantie écrite qu'ils n'avaient procédé à aucune collecte de données directes qui contreviendrait aux dispositions de l'accord TFTP;

AM. considérant que pendant son séjour à Washington du 28 au 31 octobre 2013, la délégation LIBE a rencontré le département du Trésor des États-Unis; considérant que le Trésor américain a affirmé n'avoir eu, depuis l'entrée en vigueur de l'accord TFTP, aucun accès à des données SWIFT dans l'Union européenne, si ce n'est dans le cadre de l'accord TFTP; considérant que le département du Trésor a refusé de commenter la possibilité que des données SWIFT aient été consultées en dehors de l'accord TFTP par un autre organisme gouvernemental ou ministère américain, ou que l'administration américaine ait eu connaissance des activités de surveillance de masse de la NSA; considérant que le 18 décembre 2013, M. Glenn Greenwald a déclaré lors de l'audition publique consacrée à l'enquête de la commission LIBE que la NSA et le GCHQ avaient ciblé les réseaux SWIFT;

AN. considérant que le 13 novembre 2013, les autorités de protection des données belges et néerlandaises ont décidé d'organiser une enquête conjointe sur la sécurité des réseaux

de paiement de l'organisation SWIFT afin de contrôler si des tiers ont pu accéder de façon non autorisée ou illicite aux données bancaires de citoyens européens[1];

AO. considérant que pendant l'examen conjoint de l'accord UE-États-Unis sur les dossiers des passagers aériens, le ministère américain de la sécurité intérieure a divulgué à 23 reprises des données PNR à la NSA, au cas par cas, dans le cadre d'affaires liées à la lutte contre le terrorisme, dans le respect des conditions spécifiques de l'accord;

AP. considérant que l'examen conjoint ne fait pas mention du fait qu'en cas de traitement de données à caractère personnel à des fins de renseignement, en vertu du droit américain, les ressortissants non américains ne bénéficient d'aucune voie judiciaire ou administrative pour protéger leurs droits et que les protections constitutionnelles ne sont accordées qu'aux ressortissants américains; considérant que cette absence de droits judiciaires ou administratifs annule les protections prévues pour les citoyens de l'Union dans l'accord PNR existant;

Transferts basés sur l'accord entre l'Union européenne et les États-Unis sur l'entraide judiciaire en matière pénale

AQ. considérant que l'accord entre l'Union européenne et les États-Unis sur l'entraide judiciaire en matière pénale du 6 juin 2003[2] est entré en vigueur le 1er février 2010 et a pour but de faciliter la coopération entre l'Union européenne et les États-Unis afin de lutter plus efficacement contre la criminalité, en tenant dûment compte des droits des personnes et de l'état de droit;

Accord-cadre sur la protection des données dans le domaine de la coopération policière et judiciaire (l'"accord-cadre")

AR. considérant que cet accord général a pour finalité d'établir le cadre juridique pour tous les transferts de données à caractère personnel entre l'Union européenne et les États-Unis dans le seul but de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale; considérant que les négociations ont été autorisées par le Conseil le 2 décembre 2010;

AS. considérant que cet accord devrait contenir des principes clairs et précis, juridiquement contraignants, en matière de traitement des données, et devrait notamment reconnaître le droit des citoyens de l'Union d'accéder, de rectifier et d'effacer leurs données à caractère personnel aux États-Unis, ainsi que le droit à des moyens de recours judiciaire ou administratif efficaces pour les citoyens de l'Union et à une surveillance indépendante des activités de traitement de données;

AT. considérant que dans sa communication du 27 novembre 2013, la Commission a indiqué que l'accord-cadre devrait garantir un niveau élevé de protection des citoyens des deux côtés de l'Atlantique et devrait renforcer la confiance des Européens dans les

[1] http://www.privacycommission.be/fr/news/les-instances-europ%C3%A9ennes-charg%C3%A9es-de-contr%C3%B4ler-le-respect-de-la-vie-priv%C3%A9e-examinent-la
[2] JO L 181 du 19.7.2003, p. 25.

échanges de données entre l'Union européenne et les États-Unis, en fournissant ainsi une base permettant de développer la coopération et le partenariat entre l'Union et les États-Unis en matière de sécurité;

AU. considérant que les négociations sur l'accord n'ont pas progressé en raison de la persistance du gouvernement américain à refuser de reconnaître aux citoyens de l'Union le droit effectif à des moyens de recours administratif et judiciaire et de l'intention d'inclure de vastes dérogations aux principes de protection des données qui figureront dans l'accord, tels que la limitation des finalités, la conservation des données ou les transferts ultérieurs, nationaux ou à l'étranger;

Réforme dans le domaine de la protection des données

AV. considérant que le cadre juridique de l'Union européenne en matière de protection des données fait actuellement l'objet d'un réexamen en vue de mettre en place un système complet, cohérent, moderne et solide pour l'ensemble des activités de traitement de données dans l'Union; considérant que la Commission a présenté en janvier 2012 un ensemble de propositions législatives: un règlement général sur la protection des données[1], qui remplacera la directive 95/46/CE et établira une législation uniforme dans toute l'Union, et une directive[2] qui établira un cadre harmonisé pour l'ensemble des activités de traitement de données réalisées par les autorités répressives à des fins répressives et réduira les divergences actuelles entre les législations nationales;

AW. considérant que le 21 octobre 2013, la commission LIBE a adopté ses rapports législatifs sur les deux propositions ainsi qu'une décision concernant l'ouverture de négociations avec le Conseil en vue de faire adopter les instruments juridiques avant la fin de la présente législature;

AX. considérant que bien que le Conseil européen des 24 et 25 octobre 2013 ait réclamé l'adoption en temps voulu d'un cadre général rigoureux de l'Union sur la protection des données en vue de renforcer la confiance des citoyens et des entreprises à l'égard de l'économie numérique, il n'est pas parvenu à définir une approche globale concernant le règlement général sur la protection des données et la directive[3];

Sécurité informatique et informatique en nuage

AY. considérant que la résolution du 10 décembre[4] souligne le potentiel économique offert par l'informatique en nuage pour la croissance et l'emploi;

AZ. considérant que le niveau de protection des données dans un environnement d'informatique en nuage ne doit pas être moins élevé à celui exigé dans un autre cadre de traitement de données; considérant que le droit de l'Union en matière de protection des données, neutre sur le plan technologique, s'applique déjà pleinement aux services

[1] COM(2012) 11 du 25.1.2012.
[2] COM(2012) 10 du 25.1.2012.
[3] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/ec/139210.pdf

[4] AT-0353/2013 PE506.114V2.00.

d'informatique en nuage actifs dans l'Union européenne;

BA. considérant que les activités de surveillance de masse donnent aux agences de renseignement l'accès aux données à caractère personnel stockées par les particuliers de l'Union européenne dans le cadre d'accords de services en nuage avec les grands fournisseurs d'informatique en nuage américains; considérant que les services de renseignement américains ont accédé à des données à caractère personnel stockées dans des serveurs localisés sur le sol européen en exploitant les réseaux internes de Yahoo et Google[1]; considérant que ces activités constituent une violation des obligations internationales; considérant qu'il n'est pas impossible que les services de renseignement aient également accédé à des informations stockées dans des services en nuage par les autorités ou entreprises publiques et les institutions des États membres;

Contrôle démocratique des services de renseignement

BB. considérant que les services de renseignement jouent un rôle important dans la protection de la société démocratique contre les menaces intérieures et extérieures; considérant qu'ils jouissent à cet effet de capacités et de pouvoirs spéciaux; considérant que ces pouvoirs doivent être utilisés dans le respect de l'état de droit, sans quoi ils risquent de perdre leur légitimité et de saper la nature démocratique de la société;

BC. considérant que le degré élevé de confidentialité qu'imposent les activités mêmes des services de renseignements pour éviter la mise en péril des opérations en cours, la divulgation des modus operandi ou la mise en danger des agents ne permet pas la transparence absolue ni l'exercice du contrôle démocratique et judiciaire ordinaire;

BD. considérant que les développements technologiques ont conduit les services de renseignements à coopérer sans cesse davantage à l'échelle internationale, notamment par l'échange de données à caractère personnel, ce qui crée souvent une confusion des genres entre renseignement et répression;

BE. considérant que la plupart des mécanismes et organes de contrôle nationaux existants ont été créés ou réorganisés dans les années 1990 et n'ont pas nécessairement été adaptés aux progrès technologiques rapides de la décennie écoulée;

BF. considérant que le contrôle démocratique des services de renseignement est toujours effectué au niveau national, malgré l'accroissement des échanges d'informations entre les États membres de l'Union ainsi qu'entre les États membres et les pays tiers; considérant qu'il existe un écart grandissant entre, d'une part, le niveau de coopération internationale et, d'autre part, les capacités de contrôle limitées au niveau national, ce qui engendre un contrôle démocratique insuffisant et inefficace;

Conclusions principales

[1] *The Washington Post* du 31 octobre 2013.

1. considère que les récentes révélations faites dans la presse par des lanceurs d'alerte et des journalistes, associées aux témoignages d'experts recueillis pendant cette enquête, ont permis d'obtenir des preuves irréfutables de l'existence de systèmes vastes, complexes et technologiquement très avancés conçus par les services de renseignement des États-Unis et de certains États membres dans le but de collecter, de stocker et d'analyser les données et métadonnées de communication et de localisation des citoyens du monde entier, à une échelle sans précédent, sans aucun discernement et sans se baser sur des soupçons;

2. vise expressément les programmes de renseignement de la NSA, qui permettent la surveillance de masse des citoyens de l'Union européenne grâce à un accès direct aux serveurs centraux des grandes entreprises américaines du secteur de l'internet (programme PRISM), à l'analyse de contenus et de métadonnées (programme Xkeyscore), au contournement du cryptage en ligne (BULLRUN), à l'accès aux réseaux informatiques et téléphoniques et aux données de localisation, ainsi que les systèmes de l'agence de renseignement britannique GCHQ, notamment son activité de surveillance en amont (programme Tempora) et son programme de décryptage (Edgehill); estime possible qu'il existe des programmes d'une nature similaire, bien qu'à une échelle plus réduite, dans d'autres pays de l'Union européenne comme la France (DGSE), l'Allemagne (BND) et la Suède (FRA);

3. prend note des allégations de piratage ou d'exploitation des systèmes de Belgacom par l'agence de renseignement britannique GCHQ; rappelle que Belgacom a indiqué ne pas être en mesure de confirmer que les institutions de l'Union européenne étaient ciblées ou touchées, et a déclaré que les logiciels malveillants utilisés étaient des logiciels extrêmement complexes dont le développement et l'utilisation nécessitaient d'importantes ressources financières et humaines dont n'auraient pas pu disposer des entités privées ou des pirates;

4. déclare que la confiance a été profondément mise à mal, à savoir la confiance entre les deux partenaires transatlantiques, la confiance entre les États membres de l'Union, la confiance entre les citoyens et leur gouvernement, la confiance à l'égard du respect de l'état de droit et la confiance vis-à-vis de la sécurité des services informatiques; pense que pour restaurer la confiance à tous ces égards, il est urgent d'adopter un plan global;

5. note que plusieurs gouvernements affirment que ces programmes de surveillance de masse sont nécessaires à la lutte contre le terrorisme; soutient pleinement la lutte contre le terrorisme, mais est convaincu que celle-ci ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, confidentiels, voire parfois illégaux; exprime dès lors des craintes en ce qui concerne la légalité, la nécessité et la proportionnalité de ces programmes;

6. considère douteux qu'une collecte de données de cette ampleur soit uniquement motivée par la lutte contre le terrorisme, étant donné qu'elle suppose la collecte de toutes les données possibles de l'ensemble des citoyens; souligne par conséquent l'existence possible d'autres intentions de pouvoir, comme par exemple l'espionnage politique et économique;

7. s'interroge sur la compatibilité des activités d'espionnage économique de masse de

certains États membres avec le droit du marché intérieur et de la concurrence de l'Union européenne consacré aux titres I et VII du traité FUE; réaffirme le principe de coopération loyale établi à l'article 4, paragraphe 3, du traité UE et le principe selon lequel que les États membres "s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union";

8. note que les traités internationaux et la législation de l'Union européenne et des États-Unis, ainsi que les mécanismes de contrôle nationaux, n'ont prévu ni les systèmes de contre-pouvoir, ni le contrôle démocratique nécessaires;

9. condamne avec véhémence le recueil à grande échelle, systémique et aveugle des données à caractère personnel de personnes innocentes, qui comprennent souvent des informations personnelles intimes; souligne que l'utilisation de systèmes de surveillance de masse aveugle par les services de renseignement constitue une grave entrave aux droits fondamentaux des citoyens; souligne que le respect de la vie privée n'est pas un droit de luxe, mais constitue la pierre angulaire d'une société libre et démocratique; souligne par ailleurs que la surveillance de masse a des répercussions potentiellement graves sur la liberté de la presse, la liberté de pensée et la liberté d'expression, et qu'elle entraîne un risque élevé d'utilisation abusive des informations collectées à l'encontre d'adversaires politiques; insiste sur le fait que ces activités de surveillance de masse semblent également donner lieu à des actions illégales de la part des services de renseignement et qu'elles soulèvent des questions au sujet de l'extraterritorialité des législations nationales;

10. estime que les programmes de surveillance constituent une nouvelle étape vers la mise en place d'un État de la prévention à part entière, modifiant le paradigme établi du droit pénal dans les sociétés démocratiques et encourageant en revanche une combinaison d'activités de répression et de renseignement avec des garanties juridiques floues, satisfaisant rarement au contrôle démocratique et non respectueux des droits fondamentaux, en particulier de la présomption d'innocence; rappelle à cet égard la décision de la Cour constitutionnelle fédérale allemande[1] sur l'interdiction du recours au profilage préventif (*präventive Rasterfahndung*) en l'absence d'éléments démontrant la mise en péril d'autres droits importants et juridiquement protégés, selon laquelle une menace générale ou des tensions internationales ne suffisent pas à justifier de telles mesures;

11. insiste sur le fait que les législations, traités et tribunaux secrets constituent une violation de l'état de droit; signale qu'il se peut que les arrêts des cours ou tribunaux et les décisions d'autorités administratives d'un pays tiers autorisant, directement ou indirectement, les activités de contrôle telles que celles examinées par l'enquête dont il est ici question ne soient pas reconnus ou appliqués automatiquement, mais qu'ils doivent être soumis au cas par cas aux procédures nationales appropriées en matière de reconnaissance mutuelle et d'entraide judiciaire, notamment aux règles imposées par les accords bilatéraux;

12. souligne que les préoccupations susmentionnées sont exacerbées par les développements rapides sur le plan technologique et sociétal; estime qu'étant donné

[1] N° 1 BvR 518/02 du 4 avril 2006.

que les appareils internet et mobiles sont omniprésents dans la vie quotidienne moderne ("informatique ubiquitaire") et que le modèle commercial de la plupart des entreprises du secteur de l'internet est basé sur le traitement de données à caractère personnel de toutes sortes mettant en péril l'intégrité de la personne, l'ampleur de ce problème est sans précédent;

13. considère qu'il est évident, comme l'ont souligné les experts en technologie qui ont témoigné dans le cadre de l'enquête, qu'au stade de développement technologique actuel, il n'existe aucune garantie, que ce soit pour les institutions publiques européennes ou pour les citoyens, que leur sécurité informatique ou leur vie privée puisse être protégée des intrusions par des agences de renseignement bien équipées de pays de l'Union ou de pays tiers ("pas de sécurité informatique à 100 %"); note que le seul moyen de remédier à cette situation alarmante est que les Européens acceptent de consacrer suffisamment de moyens, humains et financiers, à la préservation de l'indépendance et de l'autosuffisance de l'Europe;

14. rejette vivement l'idée selon laquelle ces questions relèveraient strictement de la sécurité nationale et, dès lors, de l'unique compétence des États membres; rappelle une récente décision de la Cour de justice selon laquelle "bien qu'il appartienne aux États membres d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une décision concerne la sûreté de l'État ne saurait entraîner l'inapplicabilité du droit de l'Union"[1]; rappelle par ailleurs que la protection de la vie privée de tous les citoyens de l'Union européenne est en jeu, de même que la sécurité et la fiabilité de tous les réseaux de communication de l'Union; pense par conséquent qu'une discussion et une action au niveau européen ne sont pas seulement légitimes, mais nécessaires pour l'autonomie et la souveraineté de l'Union;

15. se félicite des discussions, enquêtes et réexamens qui ont été menés dans plusieurs régions du monde sur le sujet abordé par l'enquête; attire l'attention sur l'initiative "Global Government Surveillance Reform", signée par les grandes entreprises technologiques du monde et réclamant des modifications en profondeur des législations nationales en matière de surveillance, notamment une interdiction mondiale de la collecte massive de données afin de contribuer à préserver la confiance du public à l'égard de l'internet; prend note avec grand intérêt des recommandations récemment publiées par le groupe d'étude du président américain sur la révision des renseignements et des technologies; prie instamment les gouvernements de tenir pleinement compte de ces demandes et recommandations et de procéder à une refonte de leurs cadres nationaux régissant les services de renseignement afin de mettre en œuvre les garanties et les mécanismes de contrôle appropriés;

16. félicite les institutions et les experts ayant contribué à cette enquête; déplore le fait que les autorités de plusieurs États membres aient refusé de coopérer dans l'enquête réalisée par le Parlement européen au nom de ses citoyens; salue l'ouverture dont ont fait preuve plusieurs membres du Congrès et des parlements nationaux;

17. est conscient que dans des délais aussi serrés, seule une enquête préliminaire sur toutes les questions soulevées depuis juillet 2013 a pu être réalisée; reconnaît à la fois

[1] N° 1 BvR 518/02 du 4 avril 2006.

l'ampleur des révélations dont il est question et leur caractère permanent; adopte par conséquent une approche à long terme consistant en une série de propositions spécifiques ainsi qu'en un mécanisme prévoyant un suivi au cours de la prochaine législature, afin de faire en sorte que les conclusions formulées continuent demeurent des priorités politiques majeures de l'Union;

18. entend demander à la Commission européenne de prendre des engagements politiques forts après les élections de mai 2014 en vue de mettre en œuvre les propositions et recommandations de l'enquête; attend des candidats qui participeront aux prochaines auditions du Parlement pour les nouveaux commissaires qu'ils fassent preuve d'un engagement adéquat;

Recommandations

19. demande aux autorités américaines et aux États membres de l'Union européenne d'interdire les activités de surveillance de masse aveugle et le traitement massif de données à caractère personnel;

20. exhorte certains États membres de l'Union, y compris le Royaume-Uni, l'Allemagne, la France, la Suède et les Pays-Bas, à réviser, le cas échéant, leur législation nationale et leurs pratiques régissant les activités des services de renseignement de manière à s'assurer de leur conformité avec les normes de la convention européenne des droits de l'homme et à respecter leurs obligations relatives aux droits fondamentaux que sont la protection des données, le droit à la vie privée et la présomption d'innocence; souhaite en particulier souligner, compte tenu des nombreuses informations fournies par les médias faisant état d'une surveillance de masse au Royaume-Uni, que le cadre juridique actuel consistant en une "interaction complexe" entre trois actes législatifs distincts – la loi de 1998 sur les droits de l'homme, la loi de 1994 sur les services de renseignement et la loi de 2000 sur la règlementation des pouvoirs d'enquête – devrait être révisé;

21. invite les États membres à s'abstenir d'accepter des données provenant de pays tiers et ayant été collectées illégalement, ainsi que d'accepter que des gouvernements ou agences de pays tiers effectuent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens, notamment la protection des droits de l'homme au titre du traité UE, de la CEDH et de la Charte des droits fondamentaux de l'Union européenne;

22. exhorte les États membres à satisfaire immédiatement à l'obligation positive, qui leur incombe au titre de la convention européenne des droits de l'homme, de protéger leurs citoyens des activités de surveillance contraires aux dispositions de la convention, y compris lorsque ces activités visent à garantir la sécurité nationale, réalisées par des pays tiers et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers;

23. invite le secrétaire général du Conseil de l'Europe à lancer la procédure au titre de l'article 52 selon laquelle "[t]oute Haute Partie contractante fournira sur demande du Secrétaire Général du Conseil de l'Europe les explications requises sur la manière dont

son droit interne assure l'application effective de toutes les dispositions de cette Convention";

24. invite les États membres à prendre immédiatement les mesures nécessaires, y compris en matière judiciaire, contre les violations de leur souveraineté, et, par là-même, contre les violations du droit public international général commises par l'intermédiaire des programmes de surveillance de masse; exhorte également les États membres de l'Union à faire usage de toutes les mesures internationales à leur disposition pour défendre les droits fondamentaux des citoyens européens, notamment en déclenchant la procédure de plainte interétatique prévue par l'article 41 du Pacte international relatif aux droits civils et politiques (PIDCP);

25. invite les États-Unis à réviser sans tarder leur législation afin de la rendre conforme au droit international, à reconnaître le droit à la vie privée et les autres droits des citoyens de l'Union européenne, à prévoir des moyens de recours judiciaire pour les citoyens de l'Union et à signer le protocole additionnel permettant aux particuliers de soumettre des plaintes au titre du PIDCP;

26. est fermement opposé à la conclusion d'un protocole additionnel ou à la formulation d'une orientation pour la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest) concernant l'accès transfrontalier à des données informatiques stockées susceptible de légitimer l'accès des services de renseignement à des données stockées dans une autre juridiction sans l'autorisation de celle-ci et sans le recours aux instruments d'entraide judiciaire existants, étant donné que cela pourrait donner aux autorités répressives la possibilité d'accéder librement à distance aux serveurs et aux systèmes informatiques situés dans d'autres juridictions et que cela serait contraire à la convention n° 108 du Conseil de l'Europe;

27. invite la Commission à réaliser, avant juillet 2014, une évaluation de l'applicabilité du règlement (CE) n° 2271/96 aux cas de conflits de législations lors de transferts de données à caractère personnel;

Transferts internationaux de données

Le cadre juridique américain en matière de protection des données et la "sphère de sécurité" des États-Unis

28. observe que les entreprises qui ont été identifiées dans les révélations faites aux médias comme étant impliquées dans la surveillance de masse à grande échelle des personnes concernées dans l'Union effectuée par la NSA, sont des entreprises qui ont adhéré aux principes de la "sphère de sécurité" et que cette sphère est l'instrument juridique utilisé pour le transfert des données européennes à caractère personnel vers les États-Unis (Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); est préoccupé par le fait que ces entreprises ont reconnu qu'elles ne cryptaient pas les flux d'informations et de communications entre leurs centres de données, ce qui permet aux services de renseignement d'intercepter les informations[1];

[1] *The Washington Post* du 31 octobre 2013.

29. considère que l'accès à grande échelle par les agences de renseignement américaines aux données européennes à caractère personnel traitées par la "sphère de sécurité" ne répond pas en soi aux critères de dérogation visés au point "sûreté de l'État";

30. estime qu'étant donné que, dans les circonstances actuelles, les principes de la "sphère de sécurité" ne permettent pas d'assurer une protection suffisante pour les citoyens de l'Union, ces transferts doivent être réalisés dans le cadre d'autres instruments, comme des clauses contractuelles ou des règles d'entreprise contraignantes établissant des garanties et des protections spécifiques;

31. invite la Commission à présenter des mesures prévoyant la suspension immédiate de la décision 2000/520/CE, qui déclare la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes publiées par le ministère du commerce des États-Unis d'Amérique;

32. invite les autorités compétentes des États membres, à savoir les autorités chargées de la protection des données, à faire usage de leurs compétences existantes pour suspendre sans attendre les flux de données à destination de toute organisation ayant adhéré aux principes de la "sphère de sécurité" américaine et à exiger que ces flux de données ne soient réalisés que dans le cadre d'autres instruments, pour autant qu'ils contiennent les garanties et les protections nécessaires en ce qui concerne la protection de la vie privée et les droits et libertés fondamentaux des individus;

33. invite la Commission à présenter d'ici juin 2014 une évaluation complète du cadre américain en matière de respect de la vie privée, portant sur les activités commerciales, policières et de renseignement, face à l'écart grandissant entre les systèmes juridiques européen et américain de protection des données à caractère personnel;

Transferts vers d'autres pays tiers dans le cadre de la décision relative à la pertinence de la protection

34. rappelle que la directive 95/46/CE dispoe que les transferts vers un pays tiers de données à caractère personnel ne peuvent avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la directive, le pays tiers en question assure un niveau de protection adéquat, l'objet de cette disposition étant d'assurer la continuité de la protection offerte par la législation européenne en matière de protection des données lorsque des données à caractère personnel sont transférées hors de l'Union européenne;

35. rappelle que la directive 95/46/CE précise que le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; dans le même ordre d'idées, rappelle que ladite directive confère également à la Commission des compétences d'exécution pour déclarer qu'un pays tiers assure un niveau de protection adéquat au regard des critères établis par la directive 95/46/CE; souligne que la directive 95/46/CE permet aussi à la Commission de déclarer qu'un pays tiers n'assure pas le niveau de protection adéquat;

36. rappelle que dans ce dernier cas, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause, et que la Commission engage des négociations en vue de remédier à la situation;

37. invite la Commission et les États membres à déterminer sans tarder si le niveau de protection adéquat assuré par la Nouvelle-Zélande et par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, tel que déclaré par les décisions 2013/65/UE[1] du 19 décembre 2012 et 2002/2/CE de la Commission du 20 décembre 2001, a été affecté par la participation de leurs agences nationales de renseignement à la surveillance de masse des citoyens de l'Union européenne et, le cas échéant, à prendre les mesures appropriées pour suspendre ou annuler les décisions relatives à la pertinence de la protection; attend de la Commission qu'elle rende compte au Parlement européen de ses observations sur les pays mentionnés plus haut avant décembre 2014;

Transferts fondés sur des clauses contractuelles et d'autres instruments

38. rappelle que les autorités nationales chargées de la protection des données ont indiqué que ni les clauses contractuelles types, ni les règles d'entreprise contraignantes n'étaient rédigées en prenant en considération les situations d'accès aux données à caractère personnel à des fins de surveillance de masse, et que cet accès ne serait pas conforme aux clauses dérogatoires des clauses contractuelles ou des règles d'entreprise contraignantes qui concernent des dérogations exceptionnelles répondant à un intérêt légitime dans une société démocratique, lorsqu'elles sont nécessaires et proportionnées;

39. invite les États membres à interdire ou à suspendre les flux de données vers des pays tiers sur la base des clauses contractuelles types, des clauses contractuelles ou des règles d'entreprise contraignantes autorisées par les autorités nationales compétentes lorsqu'il est établi que la loi à laquelle l'importateur de données est soumis lui impose des obligations qui vont au-delà des restrictions nécessaires dans une société démocratique et qui risquent d'avoir un effet contraire important sur les garanties fournies par la législation applicable en matière de protection des données et les clauses contractuelles types, ou parce que la poursuite du transfert entraînerait un risque imminent de dommages graves pour les personnes dont les données sont traitées;

40. invite le groupe de travail "Article 29" à publier des lignes directrices et des recommandations sur les garanties et les protections que doivent contenir les instruments contractuels en ce qui concerne les transferts internationaux de données européennes à caractère personnel en vue d'assurer la protection de la vie privée, ainsi que des droits et libertés fondamentaux des individus, en tenant notamment compte de la législation des pays tiers en matière de renseignement et de sécurité nationale et de la participation des entreprises qui reçoivent les données dans un pays tiers à des activités de surveillance de masse par les agences de renseignement d'un pays tiers;

41. invite la Commission à examiner les clauses contractuelles types qu'elle a établies en

[1] JO L 28 du 30.1.2013, p. 12.

vue de déterminer si elles assurent la protection nécessaire en ce qui concerne l'accès aux données à caractère personnel transférées en vertu des clauses à des fins de renseignement et, le cas échéant, à les revoir;

Transferts fondés sur l'accord en matière d'entraide judiciaire

42. invite la Commission à effectuer avant fin 2014 une évaluation approfondie de l'accord en matière d'entraide judiciaire existant, conformément à l'article 17 dudit accord, afin de contrôler sa mise en œuvre concrète et, plus particulièrement, de vérifier si les États-Unis l'ont bien utilisé pour obtenir des informations ou des données dans l'Union européenne et si l'accord a été contourné pour obtenir des informations directement dans l'Union européenne, ainsi que d'évaluer les incidences sur les droits fondamentaux des personnes; signale que cette évaluation doit non seulement porter sur les déclarations officielles des États-Unis pour constituer une base d'analyse suffisante, mais qu'elle doit aussi s'appuyer sur des évaluations spécifiques dans l'Union européenne; souligne que ce réexamen approfondi doit également porter sur les conséquences de l'application de l'architecture constitutionnelle de l'Union à cet instrument afin de l'adapter à la législation de l'Union, en tenant compte, notamment, du protocole 36 et de l'article 10 de ladite législation et de la déclaration 50 concernant ce protocole;

Entraide judiciaire européenne en matière pénale

43. invite le Conseil et la Commission à informer le Parlement au sujet de l'utilisation effective par les États membres de la convention relative à l'entraide judiciaire en matière pénale entre les États membres, et notamment du titre III relatif à l'interception des télécommunications; invite la Commission à présenter une proposition, conformément à la déclaration 50, concernant le protocole 36, comme demandé, avant fin 2014 en vue de l'adapter au cadre du traité de Lisbonne;

Transferts basés sur les accords TFTP et PNR

44. estime que les informations fournies par la Commission européenne et le département du Trésor des États-Unis ne précisent pas si les agences de renseignement américaines ont accès aux messages financiers SWIFT dans l'Union européenne en interceptant les réseaux SWIFT ou les systèmes d'exploitation ou les réseaux de communication des banques, seules ou en coopération avec des agences de renseignement nationales européennes et sans avoir recours aux canaux bilatéraux existants en matière d'entraide judiciaire et de coopération judiciaire;

45. réaffirme sa résolution du 23 octobre 2013 et invite la Commission à suspendre l'accord TFTP;

46. invite la Commission européenne à réagir au fait que trois des principaux systèmes informatisés de réservation utilisés par les compagnies aériennes partout dans le monde sont basés aux États-Unis et que les données PNR sont sauvegardées dans des systèmes en nuage opérant sur le sol américain et régis par le droit américain, ce qui n'est pas conforme aux dispositions en matière de pertinence de la protection des données;

Accord-cadre pour la protection des données dans le domaine de la coopération policière et judiciaire ("l'accord-cadre")

47. considère qu'une solution satisfaisante au titre de l'accord-cadre en question est une condition préalable nécessaire à la pleine restauration de la confiance entre les partenaires transatlantiques;

48. demande une reprise immédiate des négociations avec les États-Unis sur l'accord-cadre, en vue de prévoir des droits bien définis pour les citoyens de l'Union européenne et des recours administratifs et judiciaires efficaces et exécutoires aux États-Unis sans aucune discrimination;

49. invite la Commission et le Conseil à ne se lancer dans aucun autre accord ou mesure sectoriels en matière de transfert de données à caractère personnel à des fins policières tant que l'accord-cadre ne sera pas entré en vigueur;

50. exhorte la Commission à rendre compte de façon détaillée des différents points du mandat de négociation et de la situation en avril 2014 au plus tard;

Réforme dans le domaine de la protection des données

51. invite la présidence du Conseil et la majorité d'États membres qui sont favorables à un niveau élevé de protection des données à faire preuve d'initiative politique et de responsabilité et à accélérer leurs travaux sur l'ensemble du paquet relatif à la protection des données en vue de permettre son adoption en 2014, afin que les citoyens de l'Union puissent bénéficier d'une meilleure protection dans un avenir très proche;

52. souligne que le règlement relatif à la protection des données et la directive relative à la protection des données sont tous deux nécessaires pour protéger les droits fondamentaux des individus et doivent dès lors être traités comme un tout à adopter simultanément afin de s'assurer que l'ensemble des activités de traitement de données dans l'Union prévoient un niveau élevé de protection en toutes circonstances;

Informatique en nuage

53. observe que les pratiques mentionnées plus haut ont eu une influence négative sur la confiance dans l'informatique en nuage et dans les fournisseurs de services d'informatique en nuage américains; souligne dès lors que le développement des services en nuage européens est un élément essentiel pour assurer la croissance et l'emploi, ainsi que la confiance dans les services et les fournisseurs de services d'informatique en nuage et pour assurer un niveau élevé de protection des données personnelles;

54. réaffirme ses graves préoccupations quant à la divulgation directe obligatoire de données et d'informations à caractère personnel de citoyens de l'Union, traitées dans le cadre d'accords de services d'informatique en nuage, à des pays tiers par des fournisseurs de services d'informatique en nuage soumis au droit de pays tiers ou utilisant des serveurs de stockage situés dans des pays tiers, et quant à l'accès direct à

distance aux données et aux informations à caractère personnel traitées par des forces de l'ordre et des services de renseignements de pays tiers;

55. déplore le fait qu'un tel accès soit habituellement obtenu par l'application directe de leurs propres dispositions juridiques par les autorités de pays tiers, sans recourir aux instruments internationaux mis en place pour la coopération juridique, tels que les accords d'entraide judiciaire ou d'autres formes de coopération judiciaire;

56. demande à la Commission et aux États membres d'accélérer les travaux relatifs au partenariat européen de l'informatique en nuage;

57. rappelle 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;

Partenariat transatlantique de commerce et d'investissement (TTIP)

58. reconnaît que l'Union européenne et les États-Unis poursuivent les négociations relatives à un partenariat transatlantique de commerce et d'investissement, qui revêt une importance stratégique majeure pour le renforcement de la croissance économique et pour la capacité de l'Union et des États-Unis à définir les normes réglementaires mondiales futures;

59. souligne avec force, compte tenu de l'importance de l'économie numérique dans la relation et dans la cause du rétablissement de la confiance entre l'Union européenne et les États-Unis, que le Parlement européen n'approuvera le TTIP final qu'à condition que l'accord respecte pleinement les droits fondamentaux reconnus par la charte de l'Union européenne, et que la protection de la vie privée des individus en ce qui concerne le traitement et la diffusion des données à caractère personnel doit continuer à être régie par l'article XIV de l'AGCS;

Contrôle démocratique des services de renseignement

60. souligne que, malgré le fait que le contrôle des activités des services de renseignement doit s'appuyer à la fois sur la légitimité démocratique (cadre juridique solide, autorisation ex ante et vérification ex post), et sur une capacité et une expertise techniques suffisantes, ces deux aspects, et en particulier les capacités techniques, font cruellement défaut dans la majorité des organes de contrôle européens et américains actuels;

61. invite, comme il l'a fait dans le cas d'*ECHELON*, l'ensemble des parlements nationaux qui ne l'ont pas encore fait à mettre en place une surveillance appropriée des activités de renseignement assurée par les parlementaires ou des organes spécialisés juridiquement habilités à enquêter; invite les parlements nationaux à s'assurer que ces comités/organes de surveillance disposent des ressources, de l'expertise technique et des moyens juridiques nécessaires pour pouvoir contrôler efficacement les services de renseignement;

62. recommande la mise en place d'un groupe de haut niveau afin de renforcer la

coopération dans le domaine du renseignement au niveau de l'Union, conjugué à un mécanisme de contrôle approprié en vue d'assurer à la fois la légitimité démocratique et une capacité technique appropriée; souligne que le groupe de haut niveau doit travailler en étroite collaboration avec les parlements nationaux afin de proposer les nouvelles mesures à prendre pour renforcer la collaboration dans l'Union en matière de contrôle;

63. invite ce groupe de haut niveau à définir des normes ou des règles minimales contraignantes à l'échelle de l'Europe sur le contrôle (ex ante et ex post) des services de renseignement, fondées sur les bonnes pratiques existantes et sur les recommandations d'organisations internationales (les Nations unies, le Conseil de l'Europe, etc.);

64. invite le groupe de haut niveau à limiter strictement dans le temps la durée de la surveillance ordonnée, à moins que sa poursuite ne soit dûment justifiée par l'autorité compétente/de contrôle;

65. invite le groupe de haut niveau à définir des critères de transparence renforcée, fondés sur le principe général d'accès à l'information et sur les principes dits "de Tshwane"[1];

66. entend organiser une conférence avec les organes de contrôle nationaux, qu'ils soient parlementaires ou indépendants, avant la fin 2014;

67. invite les États membres à s'appuyer sur les bonnes pratiques en vue de permettre à leurs organes de contrôle d'accéder plus facilement aux informations sur les activités de renseignement (informations classées secrètes et informations d'autres services comprises) et de leur conférer le pouvoir d'effectuer des visites sur place, de les doter d'un ensemble solide de compétences en matière d'interrogation, de même que de l'expertise technique suffisante et des ressources nécessaires, de bénéficier d'une stricte indépendance vis-à-vis du pouvoir exécutif et de les obliger à rendre compte de la situation auprès de leurs parlements respectifs;

68. invite les États membres à développer la coopération entre les organes de contrôle, notamment au sein du réseau européen des organes nationaux de contrôle des services de renseignement (ENNIR);

69. exhorte la Commission à présenter, avant septembre 2014, une proposition de base juridique pour les activités du centre d'analyse du renseignement de l'Union (IntCen), ainsi qu'un mécanisme de contrôle approprié adapté à ses activités, comprenant la présentation de rapports réguliers au Parlement européen;

70. invite la Commission à présenter, avant septembre 2014, une proposition concernant une procédure européenne d'habilitation de sécurité pour l'ensemble des titulaires européens d'une charge publique, étant donné que le système actuel, qui s'appuie sur l'habilitation de sécurité réalisée par l'État membre dont la personne est ressortissante, prévoit des conditions différentes et des procédures d'une durée variable selon les systèmes nationaux, ce qui se traduit par un traitement différent des députés et de leur

[1] "The Global Principles on National Security and the Right to Information", juin 2013.

personnel en fonction de leur nationalité;

71. rappelle les dispositions de l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement européen et au traitement par celui-ci des informations classées secrètes détenues par le Conseil concernant des questions autres que celles relevant de la politique étrangère et de sécurité commune qui doivent servir à améliorer le contrôle au niveau de l'Union;

Agences de l'Union européenne

72. invite l'autorité de contrôle commune d'Europol, de même que les autorités nationales responsables de la protection des données, à réaliser une inspection conjointe avant la fin 2014 en vue de vérifier si les informations et les données à caractère personnel communiquées à Europol ont été obtenues légalement par les autorités nationales, et notamment si les informations ou les données ont d'abord été obtenues par des services de renseignement dans l'Union ou dans un pays tiers, et si des mesures appropriées sont en place pour prévenir l'utilisation et la diffusion ultérieure de ces informations ou de ces données;

73. invite Europol à demander aux autorités compétentes des États membres, conformément à ses compétences, d'ouvrir des enquêtes sur la cybercriminalité et les attaques informatiques éventuelles commises par des gouvernements ou des acteurs privés dans le cadre des activités examinées;

Liberté d'expression

74. se déclare profondément préoccupé par les atteintes de plus en plus nombreuses à la liberté de la presse et par l'effet paralysant qu'ont sur les journalistes les intimidations des autorités nationales, notamment en ce qui concerne la protection de la confidentialité des sources journalistiques; réitère l'appel lancé dans sa résolution du 21 mai 2013 sur "la Charte de l'UE: ensemble de normes pour la liberté des médias à travers l'UE";

75. estime que la détention de M. Miranda et la saisie du matériel en sa possession en vertu de l'annexe 7 à la loi sur le terrorisme de 2000 (*Terrorism Act*) (ainsi que la demande adressée au journal *The Guardian de détruire ou de remettre le matériel) constituent une atteinte au droit à la liberté d'expression tel que reconnu par l'article* 10 de la CEDH et l'article 11 de la Charte de l'Union;

76. invite la Commission à présenter une proposition en vue d'un cadre exhaustif pour la protection des lanceurs d'alerte dans l'Union européenne qui s'intéresse plus particulièrement aux particularités de la dénonciation en matière de renseignement, un domaine pour lequel les dispositions relatives à la dénonciation en matière financière peuvent s'avérer insuffisantes, et prévoyant de solides garanties d'immunité;

Sécurité informatique dans l'Union européenne

77. indique que les incidents récents font clairement ressortir l'extrême vulnérabilité de l'Union européenne, et plus particulièrement des institutions de l'Union, des

gouvernements et des parlements nationaux, des grandes entreprises européennes et des infrastructures et des réseaux informatiques européens, aux attaques sophistiquées réalisées au moyen de logiciels complexes; observe que ces attaques exigent de tels moyens financiers et humains qu'elles émanent probablement d'entités étatiques agissant pour le compte de gouvernements étrangers ou même de certains gouvernements nationaux européens qui les soutiennent; dans ce contexte, considère l'affaire du piratage ou de l'espionnage de la société de télécommunications Belgacom comme un exemple inquiétant d'attaque contre la capacité informatique de l'Union;

78. estime que les révélations en matière de surveillance de masse qui ont provoqué cette crise peuvent être l'occasion pour l'Europe de prendre l'initiative pour mettre en place, à moyen terme, une capacité de ressources informatiques clés; invite la Commission et les États membres à profiter des marchés publics pour promouvoir cette capacité dans l'Union en faisant des normes de sécurité et de respect de la vie privée dans l'Union une condition essentielle dans les marchés publics de produits et de services informatiques;

79. est fortement préoccupé par les signes qui indiquent que des services de renseignement étrangers cherchent à assouplir les normes de sécurité informatique et à installer des "portes dérobées" ("backdoors") dans toute une série de systèmes informatiques;

80. invite l'ensemble des États membres, la Commission, le Conseil et le Conseil européen à faire face au danger que représente le manque d'autonomie de l'Union en matière d'outils, de sociétés et de fournisseurs dans le secteur de l'informatique (matériel, logiciels, services et réseau) et de capacités de cryptage et cryptographiques;

81. invite la Commission, les organes de standardisation et l'ENISA à définir, avant septembre 2014, des normes et des règles minimales de sécurité et sur la vie privée pour les systèmes, les réseaux et les services informatiques, y compris les services d'informatique en nuage, afin de mieux protéger les données à caractère personnel des citoyens de l'Union; estime que ces normes doivent être définies dans le cadre d'un processus ouvert et démocratique, qui ne soit pas dirigé par un pays, une entité ou une société multinationale uniques; est d'avis que, bien que des questions légitimes de maintien de l'ordre et de renseignement doivent être prises en considération afin de faciliter la lutte contre le terrorisme, ces préoccupations ne doivent pas déboucher sur un affaiblissement généralisé de la fiabilité de l'ensemble des systèmes informatiques;

82. indique que tant les sociétés de télécommunications que les régulateurs des télécommunications européens et nationaux ont clairement négligé la sécurité informatique de leurs utilisateurs et de leurs clients; invite la Commission à utiliser pleinement les compétences qui lui sont conférées en vertu de la directive-cadre sur la vie privée et les communications électroniques pour renforcer la protection de la confidentialité des communications en adoptant des mesures visant à s'assurer que l'équipement terminal est compatible avec le droit des utilisateurs de contrôler et de protéger leurs données à caractère personnel, et pour assurer un niveau de sécurité élevé des réseaux et services de télécommunication, notamment en imposant un cryptage de pointe des communications;

83. est favorable à la stratégie de cybersécurité de l'Union, mais considère qu'elle n'aborde pas toutes les menaces possibles et qu'elle devrait être étendue aux comportements malveillants des États;

84. invite la Commission à présenter, en janvier 2015 au plus tard, un plan d'action en vue de renforcer l'indépendance de l'Union européenne dans le secteur informatique, prévoyant une approche plus cohérente afin de renforcer les capacités technologiques informatiques européennes (systèmes, équipement, services informatiques, informatique en nuage, cryptage et anonymisation) et de protéger l'infrastructure informatique critique (y compris en termes de propriété et de vulnérabilité);

85. invite la Commission à déterminer, dans le cadre du prochain programme de travail du programme Horizon 2020, si des moyens supplémentaires doivent être consacrés à la promotion de la recherche, du développement, de l'innovation et de la formation européens dans le domaine des technologies informatiques, et notamment des technologies et des infrastructures visant à renforcer la protection de la vie privée, de la cryptologie, de l'informatique sécurisée, des solutions de sécurité ouvertes ("open source") et de la société de l'information;

86. invite la Commission à établir les responsabilités actuelles et à examiner, avant juin 2014, la nécessité d'un mandat élargi, d'une meilleure coordination et de ressources et de capacités techniques supplémentaires pour le centre de lutte contre la cybercriminalité d'Europol, l'ENISA, la CERT-EU et le CEPD afin de leur permettre d'enquêter plus efficacement sur les atteintes informatiques majeures dans l'Union et de réaliser (ou d'aider les États membres et les organes de l'Union à réaliser) plus efficacement les enquêtes techniques sur place liées à des atteintes informatiques majeures;

87. estime qu'il est nécessaire que l'Union européenne s'appuie sur une académie informatique européenne, qui rassemble les meilleurs experts européens dans tous les domaines connexes, qui serait chargée d'offrir à l'ensemble des institutions et des organes pertinents de l'Union des conseils scientifiques sur les technologies informatiques, y compris les stratégies liées à la sécurité; invite, pour commencer, la Commission à constituer un groupe d'experts scientifiques indépendant;

88. invite le secrétariat du Parlement européen à effectuer, avant septembre 2014, un examen et une évaluation complets de la fiabilité du Parlement européen sur le plan de la sécurité informatique, en s'intéressant plus particulièrement aux moyens budgétaires, aux ressources en personnel, aux capacités techniques, à l'organisation interne et à l'ensemble des éléments pertinents, en vue d'améliorer la sécurité des systèmes informatiques du PE; considère que cette évaluation doit au moins produire des informations, des analyses et des recommandations sur:

- la nécessité de réaliser des audits réguliers, rigoureux et indépendants sur la sécurité et des essais de pénétration, en sélectionnant des experts en sécurité externes qui assurent la transparence et garantissent des références vis-à-vis de pays tiers ou tout type de groupe d'intérêts;

- l'inclusion dans les procédures d'appels d'offres relatives aux nouveaux

systèmes informatiques de conditions spécifiques en matière de sécurité informatique et de respect de la vie privée, y compris la possibilité d'une condition relative à des logiciels ouverts ("open source") en tant que condition d'achat;

- la liste des sociétés américaines sous contrat avec le Parlement européen dans les domaines de l'informatique et des télécommunications, en prenant en considération les révélations à propos des contrats conclus par la NSA avec des entreprises telles que RSA, dont les produits sont utilisés par le Parlement européen en vue de protéger l'accès à distance à ses données par ses députés et son personnel;

- la fiabilité et la résilience des logiciels tiers commerciaux utilisés par les institutions européennes dans leurs systèmes informatiques en ce qui concerne les pénétrations et les intrusions par les autorités policières et de renseignement européennes et non européennes;

- le recours accru aux systèmes ouverts et la réduction du nombre de systèmes commerciaux prêts à l'emploi utilisés;

- les incidences du recours accru aux outils mobiles (*smartphones*, tablettes, qu'ils soient professionnels ou personnels) et ses conséquences sur la sécurité informatique du système;

- la sécurité des communications entre différents lieux de travail du Parlement européen et des systèmes informatiques utilisés au Parlement européen;

- l'utilisation et l'emplacement des serveurs et des centres informatiques pour les systèmes informatiques du Parlement européen et les conséquences pour la sécurité et l'intégrité des systèmes;

- la mise en œuvre concrète de la réglementation existante sur les atteintes à la sécurité et la notification rapide des autorités compétentes par les fournisseurs de réseaux de télécommunication accessibles au public;

- l'utilisation du stockage en nuage par le Parlement européen, y compris le type de données stockées en nuage, la façon dont le contenu et l'accès à celui-ci sont protégés et le lieu où le nuage est situé, en précisant le régime juridique applicable en matière de protection des données;

- un plan permettant l'utilisation de technologies cryptographiques supplémentaires, notamment le cryptage authentifié de bout en bout pour l'ensemble des services informatique et de communication, comme l'informatique en nuage, la messagerie électronique, la messagerie instantanée et la téléphonie;

- l'utilisation des signatures électroniques dans les courriers électroniques;

- une analyse des avantages de l'utilisation de GNU Privacy Guard en tant que

norme de cryptage par défaut pour les courriers électroniques, qui permettrait en même temps d'utiliser les signatures numériques;

- la possibilité de mettre en place un service de messagerie instantanée sécurisé au sein du Parlement européen, permettant une communication sécurisée, où le serveur ne verrait que du contenu crypté;

89. invite les institutions et les agences de l'Union européenne à réaliser une démarche similaire, avant décembre 2014, notamment le Conseil européen, le Conseil, le Service européen pour l'action extérieure (SEAE) (y compris les délégations de l'Union), la Commission, la Cour de justice de l'Union européenne et la Banque centrale européenne; invite les États membres à effectuer des évaluations similaires;

90. souligne qu'en ce qui concerne l'action extérieure de l'Union européenne, des évaluations des besoins budgétaires connexes s'imposent et des mesures initiales doivent être prises au plus vite dans le cas du Service européen pour l'action extérieure et que des moyens suffisants doivent être réservés dans le projet de budget 2015;

91. est d'avis que les systèmes informatiques à grande échelle utilisés dans le domaine de la liberté, de la sécurité et de la justice, comme le système d'information Schengen II, le système d'information sur les visas, Eurodac et les éventuels systèmes futurs, doivent être développés et exploités de sorte à éviter que les données ne soient compromises à la suite des demandes émises par les États-Unis en vertu de la loi américaine *Patriot Act*; invite l'eu-LISA à rendre compte au Parlement de la fiabilité des systèmes en place avant fin 2014;

92. invite la Commission et le SEAE à prendre des mesures au niveau international, avec les Nations unies notamment, et en collaboration avec les partenaires intéressés (comme le Brésil) et à mettre en œuvre une stratégie européenne en faveur de la gouvernance démocratique de l'internet en vue de prévenir l'influence injustifiée de toute entité individuelle, de toute entreprise ou de tout pays sur les activités de l'ICANN et de l'IANA en assurant une représentation appropriée de l'ensemble des parties concernées au sein de ces organes;

93. demande que soit reconsidérée l'architecture globale de l'internet en termes de flux de données et de stockage des données, en privilégiant le renforcement de la minimisation des données et de la transparence et la réduction du stockage de masse centralisé de données brutes, ainsi qu'en évitant l'acheminement inutile du trafic par le territoire de pays qui ne répondent pas aux normes de base en matière de droits fondamentaux, de protection des données et de respect de la vie privée;

94. invite les États membres, en collaboration avec l'ENISA, le Centre de lutte contre la cybercriminalité d'Europol, les CERT et les autorités nationales de protection des données de même que les unités nationales de lutte contre la cybercriminalité, à lancer une campagne d'information et de sensibilisation en vue de permettre aux citoyens de faire des choix mieux informés en ce qui concerne les données à caractère personnel à mettre en ligne et le meilleur moyen de les protéger, notamment grâce à des mesures "d'hygiène numérique", au cryptage et à l'informatique en nuage sécurisée, en utilisant pleinement la plate-forme d'information sur le secteur public prévue dans la directive

"Service universel";

95. invite la Commission à évaluer, avant septembre 2014, les possibilités d'encourager les fabricants de logiciels et de matériel à renforcer la sécurité et la vie privée au moyen de fonctions par défaut dans leurs produits, y compris la possibilité d'introduire une responsabilité légale pour les fabricants pour les vulnérabilités connues non corrigées ou l'installation de portes dérobées secrètes et de décourager la collecte excessive et disproportionnée de données à caractère personnel en masse et, le cas échéant, à présenter des propositions législatives;

Rétablissement de la confiance

96. estime que l'enquête a fait ressortir la nécessité pour les États-Unis de rétablir la confiance avec leurs partenaires, étant donné qu'il y va essentiellement des activités des agences de renseignement américaines;

97. indique que la crise de confiance qui a éclaté s'étend:

– à l'esprit de coopération au sein de l'Union européenne, certaines activités de renseignement nationales risquant de compromettre la réalisation des objectifs de l'Union;

– aux citoyens, qui se rendent compte qu'ils peuvent être espionnés non seulement par des pays tiers ou des sociétés multinationales, mais aussi par leur propre gouvernement;

– au respect de l'état de droit et à la crédibilité des garanties démocratiques dans une société numérique;

Entre l'Union européenne et les États-Unis

98. rappelle l'important partenariat historique et stratégique entre les États membres de l'Union et les États-Unis, fondé sur une croyance commune dans la démocratie, l'état de droit et les droits fondamentaux;

99. estime que les activités de surveillance de masse des citoyens et d'espionnage des dirigeants politiques des États-Unis ont gravement nui aux relations entre l'Union européenne et les États-Unis et eu des conséquences négatives sur la confiance dans les organisations américaines agissant dans l'Union européenne; signale que ce phénomène est encore exacerbé par l'absence de moyens de recours judiciaire ou administratif dans le cadre du droit américain pour les citoyens de l'Union, notamment dans les cas liés à des activités de surveillance à des fins de renseignement;

100. reconnaît, à la lumière des défis mondiaux auxquels sont confrontés l'Union européenne et les États-Unis, que le partenariat transatlantique doit être renforcé et qu'il est essentiel que la coopération transatlantique se poursuive dans la lutte contre le terrorisme; affirme, cependant, que des mesures claires doivent être prises par les États-Unis pour rétablir la confiance et souligner à nouveau les valeurs fondamentales communes sur lesquelles s'appuie le partenariat;

101. est disposé à se lancer activement dans un dialogue avec ses homologues américains afin que, dans le débat public et au Congrès en cours aux États-Unis sur la réforme de la surveillance et le réexamen de la surveillance du renseignement, les droits des citoyens de l'Union soient pris en considération sur le plan du respect de la vie privée, que les droits à l'information et au respect de la vie privée soient garantis dans les tribunaux américains et qu'il soit mis fin à la discrimination actuelle;

102. demande instamment que les réformes nécessaires soient réalisées et que des garanties efficaces soient accordées aux Européens afin de veiller à ce que le recours à la surveillance et au traitement des données à des fins de renseignement étranger soit limité à des situations bien définies et lié à des soupçons raisonnables ou à une cause probable d'activité terroriste ou criminelle; souligne que ces activités doivent, dans ce cas, faire l'objet d'un contrôle judiciaire transparent;

103. estime que des signaux politiques clairs s'imposent de la part de nos partenaires américains afin de démontrer que les États-Unis font la distinction entre leurs alliés et leurs adversaires;

104. exhorte la Commission européenne et le gouvernement américain à aborder, dans le cadre des négociations en cours sur l'accord-cadre entre l'Union et les États-Unis relatif au transfert de données à des fins policières, les droits à l'information et au recours judiciaire des citoyens de l'Union et à conclure ces négociations, avant l'été 2014, conformément aux engagements pris à l'occasion de la réunion ministérielle UE-États-Unis sur la justice et les affaires intérieures du 18 novembre 2013;

105. encourage les États-Unis à adhérer à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention n° 108) du Conseil de l'Europe, comme ils ont adhéré à la convention de 2001 sur la cybercriminalité, renforçant ainsi le fondement juridique commun entre les alliés transatlantiques;

106. invite les institutions de l'Union à étudier les possibilités de mettre en place avec les États-Unis un code de conduite qui garantirait qu'aucune activité d'espionnage n'est réalisée à l'encontre d'institutions et d'installations européennes;

Au sein de l'Union européenne

107. estime également que la participation et les activités des États membres de l'Union européenne ont produit une perte de confiance; est d'avis que seule une clarté totale sur les fins et les moyens de la surveillance, un débat public et, au final, une révision de la législation, comprenant un renforcement du système de contrôle judiciaire et parlementaire, pourront rétablir la confiance perdue;

108. est conscient que certains États membres de l'Union s'efforcent d'assurer une communication bilatérale avec les autorités américaines à propos des allégations d'espionnage et que certains d'entre eux ont conclu (Royaume-Uni) ou envisagent de conclure (Allemagne, France) des accords dits "de lutte contre l'espionnage"; souligne que ces États membres sont tenus de respecter pleinement les intérêts de l'Union européenne dans son ensemble;

109. estime que ces accords ne doivent pas violer les traités européens, en particulier le principe de la coopération loyale (visé à l'article 4, paragraphe 3, du traité UE) ou saper les politiques de l'Union en général et, plus précisément, le marché intérieur, la concurrence loyale et le développement économique, industriel et social; se réserve le droit de faire jouer les procédures du traité dans l'hypothèse où ces accords devraient s'avérer contradictoires avec les principes de cohésion ou fondamentaux de l'Union sur lesquels elle s'appuie;

Sur le plan international

110. invite la Commission à présenter, avant janvier 2015, une stratégie européenne en faveur de la gouvernance démocratique de l'internet;

111. invite les États membres à donner suite à l'appel lancé lors de la 35e conférence internationale des commissaires à la protection des données et de la vie privée afin de "promouvoir l'adoption d'un protocole additionnel à l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP). Ce protocole devrait être fondé sur les normes élaborées et avalisées par la Conférence internationale ainsi que sur les précisions formulées dans l'observation générale n° 16 relative au Pacte afin de favoriser l'établissement de normes mondiales concernant la protection des données à caractère personnel et la protection de la vie privée conformément à la primauté du droit"; demande à la haute représentante/vice-présidente de la Commission et au Service européen pour l'action extérieure d'adopter des mesures proactives;

112. invite les États membres à développer une stratégie cohérente et solide au sein des Nations unies, en appuyant notamment la résolution sur "le droit à la vie privée à l'ère numérique", proposée par le Brésil et l'Allemagne, telle qu'adoptée par la troisième commission de l'Assemblée générale des Nations unies (commission des droits de l'homme), le 27 novembre 2013;

Plan prioritaire: un habeas corpus numérique européen

113. décide de soumettre aux citoyens, aux institutions et aux États membres de l'Union européenne les recommandations mentionnées plus haut en guise de plan prioritaire pour la prochaine législature;

114. décide de lancer un *habeas corpus* numérique européen pour la protection de la vie privée fondé sur les sept actions suivantes, sous la surveillance du Parlement européen:

action 1: adopter le paquet relatif à la protection des données en 2014;

action 2: conclure l'accord-cadre entre l'Union européenne et les États-Unis assurant des mécanismes de recours adéquats aux citoyens européens en cas de transfert de données de l'Union européenne vers les États-Unis à des fins répressives;

action 3: suspendre la "sphère de sécurité" jusqu'à ce qu'une analyse complète de celle-ci soit effectuée et que ses lacunes soient corrigées en veillant à ce que le

transfert de données à caractère personnel à des fins commerciales à partir de l'Union européenne vers les États-Unis ne puisse se faire qu'en respectant les normes européennes les plus strictes;

action 4: suspendre l'accord TFTP en attendant i) la conclusion des négociations concernant l'accord-cadre; ii) la réalisation d'une enquête approfondie sur la base d'une analyse européenne et la prise en compte de l'ensemble des préoccupations soulevées par le Parlement dans sa résolution du 23 octobre;

action 5: protéger l'état de droit et les droits fondamentaux des citoyens de l'Union, en s'intéressant plus particulièrement aux menaces qui pèsent sur la liberté de la presse et la confidentialité professionnelle (y compris dans les relations entre l'avocat et son client), ainsi qu'au renforcement de la protection des lanceurs d'alerte;

action 6: élaborer une stratégie européenne en faveur de l'indépendance des technologies de l'information (aux niveaux national et européen);

action 7: faire de l'Union européenne un exemple en matière de gouvernance démocratique et neutre de l'internet;

115. invite les institutions et les États membres de l'Union européenne à appuyer et promouvoir l'*habeas corpus* numérique européen; s'engage à surveiller le respect des droits des citoyens de l'Union, en s'appuyant sur le calendrier ci-après pour suivre la mise en œuvre:

- avril-juillet 2014: un groupe de contrôle basé sur la commission d'enquête LIBE responsable de la surveillance de nouvelles révélations éventuelles dans les médias concernant les mandats d'enquête et du suivi de la mise en œuvre de la présente résolution;

- à partir de juillet 2014: un mécanisme de surveillance permanent des transferts de données et des recours judiciaires au sein de la commission compétente;

- printemps 2014: une invitation formelle du Conseil européen à intégrer l'*habeas corpus* numérique européen dans les lignes directrices à adopter au titre de l'article 68 du traité FUE;

- automne 2014: un engagement selon lequel l'*habeas corpus* numérique européen et les recommandations connexes serviront de critères déterminants pour l'approbation de la prochaine Commission;

- 2014-2015: un groupe axé sur la confiance/les données/les droits des citoyens, formé par le Parlement européen et le Congrès américain, ainsi que les parlements d'autres pays tiers engagés dans le processus, comme le Brésil, et qui se réunira régulièrement;

- 2014-2015: une conférence avec les organes de surveillance des services de renseignement des parlements nationaux européens;

- 2015: une conférence rassemblant des experts européens de haut niveau dans différents domaines relatifs à la sécurité des technologies de l'information (y compris les mathématiques, la cryptographie, les technologies de renforcement de la protection de la vie privée, etc.) afin d'encourager la définition d'une stratégie européenne concernant les technologies de l'information pour la législature à venir;

116. charge son président de transmettre la présente résolution au Conseil européen, au Conseil, à la Commission, aux parlements et aux gouvernements des États membres, aux autorités nationales chargées de la protection des données, au CEPD, à l'eu-LISA, à l'ENISA, à l'Agence des droits fondamentaux, au groupe de travail "Article 29", au Conseil de l'Europe, au Congrès des États-Unis d'Amérique, au gouvernement américain, au président, au gouvernement et au Parlement de la République fédérative du Brésil et au Secrétaire-général des Nations unies.

EXPOSÉ DES MOTIFS

"La fonction du souverain, qu'il soit un monarque ou une assemblée, consiste dans la fin pour laquelle le pouvoir souverain lui a été confié, à savoir procurer au peuple la sécurité"
Hobbes, Leviathan (chapitre XXX)

"Nous ne pouvons faire l'éloge de notre société auprès des autres en nous écartant des valeurs fondamentales qui la rendent admirable"
Lord Bingham of Cornhill,
Ancien Lord Chief Justice d'Angleterre et du pays de Galles

Méthodologie

En juillet 2013, la commission d'enquête LIBE a été chargée de la tâche extrêmement difficile d'assurer le mandat[1] de la plénière consistant à enquêter à propos de la surveillance électronique de masse des citoyens de l'Union européenne dans un délai très court de moins de six mois.

Au cours de cette période, elle a organisé 15 auditions couvrant tous les groupes de questions imposés dans la résolution du 4 juillet, en s'appuyant sur les travaux d'experts européens et américains aux connaissances et parcours très variés: institutions européennes, parlements nationaux, Congrès américain, universitaires, journalistes, société civile, spécialistes dans le domaine de la sécurité et de la technologie et entreprises privées. De plus, une délégation de la commission LIBE s'est rendue à Washington du 28 au 30 octobre 2013 pour rencontrer des représentants des pouvoirs exécutif et législatif (universitaires, avocats, experts en sécurité, représentants des entreprises)[2]. Une délégation de la commission des affaires étrangères (AFET) était également dans la ville pendant cette période. Elles se sont rencontrées à quelques reprises.

Le rapporteur, les rapporteurs fictifs[3] des différents groupes politiques et trois membres de la commission AFET[4] ont rédigé ensemble une série de documents de travail[5] permettant de présenter les principaux résultats de l'enquête. Le rapporteur souhaiterait remercier tous les rapporteurs fictifs et les membres de la commission AFET pour leur étroite coopération et leur profond engagement tout au long de ce processus exigeant.

---

[1] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_fr.pdf.
[2] Voir le rapport de la délégation de Washington.
[3] Liste des rapporteurs fictifs: Axel Voss (PPE), Sophia in't Veld (ALDE), Jan Philipp Albrecht (Verts/ALE), Timothy Kirkhope (EFD), Cornelia Ernst (GUE).
[4] Liste des membres de la commission AFET: José Ignacio Salafranca Sánchez-Neyra (PPE), Ana Gomes (S&D), Annemie Neyts-Uyttebroeck (ALDE).
[5] Voir annexe I.

Ampleur du problème

Un intérêt croissant pour la sécurité et les avancées technologiques ont permis aux États d'en savoir plus au sujet de leur citoyens que jamais auparavant. En étant capables de collecter des données sur le contenu des communications, ainsi que des métadonnées, et en suivant les activités électroniques des citoyens, notamment l'utilisation qu'ils font de leurs *smartphones* et de leurs tablettes, les services de renseignement sont de fait capables de savoir la quasi-totalité des informations portant sur une personne. **Cette évolution a contribué à un changement radical dans les travaux et la pratique des agences de renseignement, qui se sont éloignées du concept traditionnel de surveillance ciblée en tant que moyen nécessaire et proportionnel pour combattre le terrorisme, en recourant à des systèmes de surveillance de masse**.

Aucun débat public ni aucun processus décisionnel démocratique n'a précédé ce recours croissant à la surveillance de masse. Il faut parler de l'objectif et du niveau de la surveillance, mais aussi de sa place dans une société démocratique. La situation créée par les révélations d'Edward Snowden est-elle le signe d'un changement général au sein de la société qui accepterait de troquer le respect de la vie privée contre sa sécurité? Sommes-nous face à une telle violation de la vie privée et de l'intimité que non seulement les criminels peuvent connaître chaque détail de la vie des citoyens, mais également les sociétés des technologies de l'information et les agences de renseignement? Est-ce un fait qu'il faut accepter sans discuter? Ou bien est-ce la responsabilité du législateur d'adapter les instruments politiques et juridiques existant pour limiter les risques et éviter toute dérive si des forces moins démocratiques devaient arriver au pouvoir?

Réactions face à la surveillance de masse et débat public

La teneur du débat sur la surveillance de masse n'est pas la même au sein des différents pays de l'Union européenne. En fait, dans de nombreux États membres, elle ne fait l'objet d'aucun débat public et l'intérêt des médias pour la question varie. L'Allemagne semble être le pays où les réactions face aux révélations ont été les plus virulentes et de nombreux débats publics ont abordé leurs conséquences. Au Royaume-Uni et en France, malgré les enquêtes des quotidiens *The Guardian* et *Le Monde*, les révélations semblent avoir suscité peu de réactions, en raison, entre autres, de la participation supposée de leurs services de renseignement aux activités de la NSA. La commission d'enquête LIBE a pu entendre les précieuses contributions des organes de contrôle parlementaire belges, néerlandais, danois et norvégiens. Les parlements britannique et français n'ont cependant pas souhaité participer aux travaux de la commission. Ces différences illustrent une nouvelle fois le fait que le contrôle démocratique sur ces questions n'est pas le même au sein des différents pays de l'Union européenne et que les organes de contrôle parlementaires doivent coopérer davantage.

À la suite des révélations d'Edward Snowden dans les médias, le débat public s'est focalisé sur deux principaux types de réactions. D'une part se trouvent ceux qui contestent la légitimité des informations publiées, car, selon eux, la plupart des informations diffusées dans les médias reposent sur une mauvaise interprétation des faits; par ailleurs, de nombreuses personnes remettent en question la validité des révélations, sans les contester pour autant, en raison des risques présumés que celles-ci pourraient présenter pour la sécurité nationale et la lutte contre le terrorisme.

D'autre part se trouvent ceux qui estiment que les informations révélées doivent faire l'objet d'un débat public éclairé en raison de l'ampleur des problèmes qu'elles suscitent sur le plan des aspects essentiels d'une démocratie: l'état de droit, les droits fondamentaux, le respect de la vie privée des citoyens, la responsabilité publique des services de répression et de renseignement, etc. C'est certainement le cas des journalistes et rédacteurs des principaux organes de presse dans le monde au courant des révélations, comme *The Guardian*, *Le Monde*, *Der Spiegel*, *The Washington Post* et Glenn Greenwald.

Les deux types de réactions présentés ci-dessus reposent sur une série de raisons qui, si elles étaient prises en compte, pourraient conduire à des réactions relativement opposées quant à la nécessité que l'Union européenne intervienne.

Cinq raisons de ne pas intervenir

– *L'argument selon lequel les services de renseignement et la sécurité nationale ne relèvent pas des domaines d'activité de l'Union européenne.*

Les révélations d'Edward Snowden concernent les activités des services de renseignement des États-Unis et de certains États membres, mais la sécurité nationale est une compétence nationale, et non européenne (sauf en matière de sécurité intérieure de l'Union européenne). Dès lors, aucune action n'est envisageable à l'échelle européenne.

– *L'argument du terrorisme et des risques pour les lanceurs d'alerte*

Tout suivi de ces révélations, ou le simple fait de les prendre en considération, affaiblit davantage la sécurité des États-Unis et de l'Union européenne, car il ne condamne pas la publication de documents dont le contenu, même s'il était expurgé de toute information compromettante comme l'avancent les médias concernés, pourrait donner des informations précieuses aux groupes terroristes.

– *L'argument de la "trahison" selon lequel le lanceur d'alerte n'a aucune légitimité*

Comme l'avancent surtout certaines personnes aux États-Unis et au Royaume-Uni, toute discussion lancée ou toute action envisagée à la suite des révélations de M. E. Snowden est intrinsèquement partiale et non pertinente, car elle reposerait sur un acte de trahison.

– *L'argument du réalisme et des intérêts stratégiques généraux*

Même si certaines fautes et activités illégales doivent encore être confirmées, il convient de les mettre en balance avec la nécessité de préserver la relation particulière entre les États-Unis et l'Europe pour préserver leurs intérêts économiques, commerciaux et étrangers communs.

– *L'argument de la bonne gouvernance selon lequel il faut avoir confiance dans son gouvernement*

Les gouvernements américain et européens sont élus démocratiquement. En matière de sécurité, et même lorsque leurs activités de renseignement visent à combattre le

terrorisme, ils respectent en principe les normes démocratiques. Cette présomption de "bonne gouvernance légitime" repose non seulement sur la bonne volonté des détenteurs du pouvoir exécutif dans ces États, mais également sur les mécanismes de contrôle démocratique garantis dans leur Constitution.

On peut constater que les raisons de ne pas intervenir sont nombreuses et convaincantes. Elles pourraient expliquer pourquoi, après quelques réactions virulentes initiales, la plupart des gouvernements européens ont préféré ne pas intervenir. L'action principale du Conseil des ministres a été de mettre sur pied un "groupe transatlantique d'experts en protection des données", qui s'est réuni trois fois avant de publier un rapport final. Un deuxième groupe est censé s'être rencontré pour discuter de questions relatives aux services de renseignement des autorités américaines et des États membres, mais aucune information n'est disponible à ce sujet. Le Conseil européen a abordé le problème de la surveillance dans une simple déclaration des chefs d'État et de gouvernement[1]. Jusqu'à présent, seuls quelques parlements nationaux ont ouvert une enquête à ce sujet.

Cinq raisons d'intervenir

– *L'argument de la surveillance de masse: dans quelle société voulons-nous vivre?*

Dès les premières révélations de juin 2013, le roman de George Orwell intitulé "1984" a souvent été évoqué. Depuis les attentats du 11 septembre, l'accent mis sur la sécurité et l'évolution vers une surveillance ciblée et spécifique ont sérieusement ébranlé le concept de vie privée. L'histoire de l'Europe et des États-Unis nous montrent le danger d'une surveillance de masse et d'une évolution progressive vers des sociétés où le respect de la vie privée n'existe pas.

– *L'argument des droits fondamentaux*

La surveillance de masse et indiscriminée menace les droits fondamentaux des citoyens, y compris le droit au respect de la vie privée, le droit à la protection des données, le droit à la liberté de la presse et le droit à un procès équitable que garantissent les traités européens, la Charte des droits fondamentaux et la CEDH. Ces droits ne peuvent être ni contournés ni négociés dans le but d'obtenir un quelconque avantage, à moins que des instruments juridiques ne le prévoient en bonne et due forme et en respectant pleinement les traités.

– L'argument de la sécurité intérieure de l'Union européenne:

La compétence nationale en matière de renseignement et de sécurité nationale n'exclut pas la possibilité d'une compétence européenne parallèle. L'Union européenne a exercé les compétences que lui confèrent les traités européens en matière de sécurité intérieure en adoptant une série d'instruments législatifs et d'accords internationaux destinés à lutter

[1] Conclusions du Conseil européen des 24 et 25 octobre 2013, notamment: "Les chefs d'État ou de gouvernement ont pris note de l'intention exprimée par la France et l'Allemagne de mener des négociations bilatérales avec les États-Unis en vue de parvenir avant la fin de l'année à un accord sur les relations mutuelles dans ce domaine. Ils ont noté qu'il est loisible à d'autres pays de l'UE de participer à cette initiative. Ils ont également attiré l'attention sur le groupe qui a été mis en place entre l'UE et les États-Unis sur la question connexe de la protection des données et ont demandé que des progrès rapides et constructifs soient réalisés en la matière."

contre la grande criminalité et le terrorisme et en définissant une stratégie de sécurité intérieure avec des agences spécialisées dans ce domaine. Par ailleurs, d'autres services témoignant de la nécessité d'une plus grande coopération à l'échelle européenne en matière de renseignement ont été développés: l'INTCEN (au sein du SEAE) et le coordinateur de la lutte contre le terrorisme (au sein du secrétariat général du Conseil), aucun des deux ne disposant d'une base juridique.

– *L'argument de la surveillance insuffisante*

Si les services de renseignement assurent une fonction indispensable en protégeant la société des menaces intérieures et extérieures, ils doivent respecter l'état de droit. Ils doivent donc être soumis à un mécanisme de contrôle rigoureux et minutieux. La surveillance des activités de renseignement est assurée à l'échelle nationale, mais compte tenu du caractère international des menaces envers la sécurité, à présent, de nombreuses informations sont échangées entre les États membres et des pays tiers comme les États-Unis; il faut améliorer les mécanismes de surveillance à l'échelle nationale et européenne afin d'éviter que les mécanismes de surveillance traditionnels ne deviennent inefficaces et obsolètes.

– *L'effet paralysant sur les médias et la protection des lanceurs d'alerte*

Les révélations d'Edward Snowden et les articles et reportages parus ensuite dans les médias ont souligné le rôle essentiel que les médias assurent dans une démocratie afin de garantir la responsabilité des gouvernements. Lorsque les mécanismes de surveillance ne parviennent pas à empêcher la surveillance de masse, ou à intervenir le cas échéant, le rôle des médias et des lanceurs d'alerte dans la révélation d'éventuels irrégularités ou abus de pouvoir est extrêmement important. La réaction des autorités américaines et britanniques a montré la vulnérabilité de la presse et des dénonciateurs et la nécessité impérieuse de mieux les protéger.

L'Union européenne est invitée à choisir entre un maintien du statu quo (suffisamment de raisons de ne pas intervenir, attendre et voir comment évolue la situation) et une politique réaliste (la surveillance n'est pas un phénomène nouveau, mais il existe suffisamment de preuves d'une ampleur inégalée de son champ d'action et des capacités de agences de renseignement qui font que l'Union européenne doit intervenir).

L'*habeas corpus* dans une société de la surveillance

En 1679, le parlement britannique a adopté l'*Habeas Corpus Act*, qui a marqué une étape importante en garantissant le droit à disposer d'un juge dans les cas de juridictions concurrentes et de conflits de droit. Aujourd'hui, nos démocraties garantissent des droits aux personnes condamnées ou détenues faisant physiquement l'objet d'une procédure pénale ou renvoyées devant un tribunal. Mais leurs données, lorsqu'elles sont envoyées, traitées, enregistrées et suivies sur les réseaux numériques, forment un "corps de données à caractère personnel", une sorte de corps numérique propre à chaque individu permettant de révéler de nombreux éléments de son identité, de ses habitudes et de ses préférences en tout genre.

L'*habeas corpus* est reconnu comme étant un instrument juridique fondamental pour protéger la liberté d'un individu contre l'action arbitraire de l'État. Ce qu'il faut aujourd'hui, c'est

étendre l'*habeas corpus* au domaine numérique. Il en va du droit au respect de la vie privée et du respect de l'intégrité et de la dignité des personnes. La collecte massive de données sans tenir compte des dispositions européennes en matière de protection de données et les violations spécifiques du principe de proportionnalité dans la gestion des données vont à l'encontre des traditions constitutionnelles des États membres et des principes fondamentaux de l'ordre constitutionnel européen.

Aujourd'hui, la principale nouveauté est que ces risques ne proviennent pas seulement d'activités criminelles (contre lesquelles le législateur européen a adopté une série d'instruments) ou d'éventuelles cyberattaques de la part du gouvernement des pays moins démocratiques. Ces risques peuvent également provenir des services de répression et de renseignement de pays démocratiques, qui placent les citoyens européens et les entreprises au cœur de conflits de droit entraînant une insécurité juridique, avec d'éventuelles violations de leurs droits, sans possibilité de faire appel à des mécanismes de recours adéquats.

La gouvernance des réseaux est nécessaire pour assurer la sécurité des données à caractère personnel. Avant le développement des États modernes, la sécurité des citoyens sur la route et dans les rues ne pouvait être garantie et leur intégrité physique était menacée. Aujourd'hui, même si elles dominent notre quotidien, les autoroutes de l'information ne sont pas sûres. L'intégrité des données numériques doit être protégée, contre les criminels bien évidemment, mais également contre un éventuel abus de pouvoir des autorités publiques ou des contractants et sociétés privées opérant dans le cadre de mandats judiciaires secrets.

Recommandations de la commission d'enquête LIBE

Nombre des problèmes soulevés aujourd'hui sont extrêmement similaires à ceux révélés par l'enquête du Parlement européen sur le programme ECHELON de 2001. L'impossibilité pour la législature précédente d'assurer le suivi des conclusions et des recommandations de l'enquête ECHELON devrait également servir de leçon importante pour la présente enquête. C'est pour cette raison que la présente résolution, qui reconnait l'ampleur des révélations en jeu et leur nature continue, est prospective et veille à avancer des propositions spécifiques afin de permettre leur suivi au cours du prochain mandat parlementaire, garantissant ainsi que ses conclusions restent en tête des priorités de l'agenda politique européen.

Cela étant, le rapporteur aimerait soumettre au vote du Parlement les mesures suivantes:

Un *habeas corpus* numérique européen pour protéger la vie privée sur la base de sept actions:

action 1: adopter le paquet relatif à la protection des données en 2014;

action 2: conclure l'accord-cadre entre l'Union européenne et les États-Unis assurant des mécanismes de recours adéquats aux citoyens européens en cas de transfert de données de l'Union européenne vers les États-Unis à des fins répressives;

action 3: suspendre la "sphère de sécurité" jusqu'à ce qu'une analyse complète de celle-ci soit effectuée et que ses lacunes soient corrigées en veillant à ce que le transfert de données à caractère personnel à des fins commerciales à partir de

l'Union européenne vers les États-Unis ne puisse se faire qu'en respectant les normes européennes les plus strictes;

action 4: suspendre l'accord TFTP en attendant i) la conclusion des négociations concernant l'accord-cadre; ii) la réalisation d'une enquête approfondie sur la base d'une analyse européenne et la prise en compte de l'ensemble des préoccupations soulevées par le Parlement dans sa résolution du 23 octobre.

action 5: protéger l'état de droit et les droits fondamentaux des citoyens de l'Union, en s'intéressant plus particulièrement aux menaces qui pèsent sur la liberté de la presse et la confidentialité professionnelle (y compris dans les relations entre l'avocat et son client), ainsi qu'au renforcement de la protection des lanceurs d'alerte;

action 6: élaborer une stratégie européenne en faveur de l'indépendance des technologies de l'information (aux niveaux national et européen);

action 7: faire de l'Union européenne un exemple en matière de gouvernance démocratique et neutre de l'internet;

Après la conclusion de l'enquête, le Parlement européen devrait continuer à agir en tant que défenseur des droits des citoyens européens en respectant le calendrier suivant pour contrôler la mise en œuvre des actions:

- avril-juillet 2014: un groupe de contrôle basé sur la commission d'enquête LIBE responsable de la surveillance de nouvelles révélations éventuelles dans les médias concernant les mandats d'enquête et du suivi de la mise en œuvre de la présente résolution;

- à partir de juillet 2014: un mécanisme de surveillance permanent des transferts de données et des recours judiciaires au sein de la commission compétente;

- printemps 2014: une invitation formelle du Conseil européen à intégrer l'*habeas corpus* numérique européen dans les lignes directrices à adopter au titre de l'article 68 du traité FUE;

- automne 2014: un engagement selon lequel l'*habeas corpus* numérique européen et les recommandations connexes serviront de critères déterminants pour l'approbation de la prochaine Commission;

- 2014-2015: un groupe axé sur la confiance/les données/les droits des citoyens, formé par le Parlement européen et le Congrès américain, ainsi que les parlements d'autres pays tiers engagés dans le processus, comme le Brésil, et qui se réunira régulièrement;

- 2014-2015: une conférence avec les organes de surveillance des services de renseignement des parlements nationaux européens;

- 2015: une conférence rassemblant des experts européens de haut niveau dans

différents domaines relatifs à la sécurité des technologies de l'information (y compris les mathématiques, la cryptographie, les technologies de renforcement de la protection de la vie privée, etc.) afin d'encourager la définition d'une stratégie européenne concernant les technologies de l'information pour la législature à venir.

ANNEXE I: LISTE DES DOCUMENTS DE TRAVAIL

Commission d'enquête LIBE

Rapporteur et rapporteurs fictifs: co-auteurs	Questions	Résolution du PE du 4 juillet 2013 (voir paragraphes 15 et 16)
M. Moraes (S&D)	Programmes de surveillance des États-Unis et de l'UE et leurs incidences sur les droits fondamentaux des citoyens de l'Union	16 a), b), c) et d)
M. Voss (PPE)	**Activités de surveillance des États-Unis à l'égard des données de l'Union et de leurs conséquences juridiques éventuelles sur les accords et la coopération transatlantiques**	16 a), b) et c)
M^{me} In't Veld (ALDE) et M^{me} Ernst (GUE)	Contrôle démocratique des services de renseignement des États membres et des organes de renseignement de l'Union européenne	15, 16 a), c) et e)
M. Albrecht (Verts/ALE)	Relation entre les pratiques de surveillance dans l'Union et les dispositions de l'Union européenne et des États-Unis en matière de protection des données	16 c), e) et f)
M. Kirkhope (ECR)	Portée de la sécurité internationale, européenne et nationale dans la perspective européenne	16 a) et b)
Trois membres de la commission AFET	Aspects relatifs à la politique étrangère de l'enquête sur la surveillance électronique de masse des citoyens européens	16 a), b) et f)

ANNEXE II: LISTE DES AUDITIONS ET DES EXPERTS

COMMISSION D'ENQUÊTE LIBE
SUR LE PROGRAMME DE SURVEILLANCE DE L'AGENCE NATIONALE DE SECURITÉ AMÉRICAINE (NSA),
LES ORGANISMES DE SURVEILLANCE DE PLUSIEURS ÉTATS MEMBRES
ET LEUR IMPACT SUR LA VIE PRIVÉE DES CITOYENS DE L'UNION ET SUR LA COOPÉRATION TRANSATLANTIQUE EN MATIÈRE DE JUSTICE ET D'AFFAIRES INTÉRIEURES

À la suite de la résolution du Parlement européen du 4 juillet 2013 (paragraphe 16), la commission LIBE a organisé une série d'auditions afin de réunir des informations relatives aux différents aspects en jeu, d'évaluer les conséquences des activités de surveillance couvertes, notamment sur les droits fondamentaux et les dispositions relatives à la protection des données, d'envisager des mécanismes de recours et de formuler des recommandations destinées à protéger les droits des citoyens européens, ainsi que de renforcer la sécurité des technologies de l'information des institutions européennes.

Date	Objet	Experts
5 septembre 2013, de 15 heures à 18 h 30 (BXL)	- Échange de vues avec les journalistes qui ont révélé l'affaire et publié les faits	• Jacques FOLLOROU, *Le Monde* • Jacob APPELBAUM, journaliste d'investigation, concepteur de logiciel et chercheur dans le domaine de la sécurité informatique dans le cadre du projet Tor • Alan RUSBRIDGER, rédacteur en chef de *The Guardian News and Media* (par vidéoconférence)
	- Suivi de la commission temporaire sur le système d'interception ECHELON	• Carlos COELHO (député européen), ancien président de la commission temporaire sur le système d'interception ECHELON • Gerhard SCHMID (ancien député européen et rapporteur du rapport ECHELON de 2001) • Duncan CAMPBELL,

		journaliste d'investigation et auteur du rapport STOA intitulé "Interception Capabilities 2000"
12 septembre 2013, de 10 heures à midi (STR)	- Compte rendu de la réunion du groupe transatlantique (UE – États-Unis) d'experts en protection des données des 19 et 20 septembre 2013 – méthode de travail et coopération avec la commission d'enquête LIBE (à huis clos) - Échange de vues avec le groupe de travail "Article 29" sur la protection des données	• Darius ŽILYS, présidence du Conseil, directeur du département "Droit international", ministre lituanien de la justice (co-président du groupe de travail ad hoc sur la protection des données) • Paul NEMITZ, directeur de la DG JUST, Commission européenne (co-président du groupe de travail ad hoc sur la protection des données) • Paul NEMITZ, directeur de la DG HOME, Commission européenne (co-président du groupe de travail ad hoc sur la protection des données) • Jacob KOHNSTAMM, président
24 septembre 2013, de 9 heures à 11 h 30 et de 15 heures à 18 h 30 (BXL) **Avec la commission AFET**	- Allégations selon lesquelles la NSA intercepterait les données SWIFT utilisées dans le cadre du programme TFTP - Compte rendu de la réunion du groupe transatlantique (UE – États-Unis) d'experts en protection des données des 19 et 20 septembre 2013	• Cecilia MALMSTRÖM, commissaire européenne • Rob WAINWRIGHT, directeur d'Europol • Blanche PETRE, avocate principale de SWIFT • Darius ŽILYS, présidence du Conseil, directeur du département "Droit international", ministre lituanien de la justice (co-président du groupe de travail ad hoc sur la protection des données) • Paul NEMITZ, directeur de la DG JUST, Commission européenne (co-président du groupe de travail ad hoc sur la protection des données) • Paul NEMITZ, directeur de la

	- Échange de vues avec la société civile américaine (partie I) - Efficacité de la surveillance dans la lutte contre la criminalité et le terrorisme en Europe - Présentation de l'étude sur les programmes de surveillance américains et leurs conséquences sur le respect de la vie privée des citoyens européens	DG HOME, Commission européenne (co-président du groupe de travail ad hoc sur la protection des données) • Jens-Henrik JEPPESEN, directeur, affaires européennes, Center for Democracy & Technology (CDT) • Greg NOJEIM, avocat principal et directeur du projet "Freedom, Security & Technology", Center for Democracy & Technology (CDT) (par vidéoconférence) • Reinhard KREISSL, coordinateur, Increasing Resilience in Surveillance Societies (IRISS) (par vidéoconférence) • Caspar BOWDEN, chercheur indépendant, ancien conseiller principal en matière de respect de la vie privée chez Microsoft, auteur de la note d'information commandée par la commission LIBE sur les programmes de surveillance américains et leurs conséquences sur le respect de la vie privée des Européens
30 septembre 2013, de 15 heures à 18 h 30 (BXL) **Avec la commission AFET**	- Échange de vues avec la société civile américaine (partie II) - Activités des lanceurs d'alerte en matière de surveillance et leur protection juridique	• Marc ROTENBERG, Electronic Privacy Information Centre (EPIC) • Catherine CRUMP, American Civil Liberties Union (ACLU) Interventions de lanceurs d'alerte: • Thomas DRAKE, ancien cadre supérieur de la NSA • J. Kirk WIEBE, ancien analyste principal de la NSA • Annie MACHON, ancien agent de renseignement pour le MI5 Interventions d'ONG au sujet de la protection juridique des lanceurs

		d'alerte: • Jesselyn RADACK, avocate et représentante de six lanceurs d'alerte, Government Accountability Project • John DEVITT, Transparency International Ireland
3 octobre 2013 De 16 heures à 18 h 30 (BXL)	- Allégations de piratage/écoute des systèmes de télécommunication par les services de renseignement (UK GCHQ)	• Geert STANDAERT, vice-président Service Delivery Engine, BELGACOM S.A. • Dirk LYBAERT, secrétaire général, BELGACOM S.A. • Frank ROBBEN, Commission de la protection de la vie privée Belgique, corapporteur "dossier Belgacom"
7 octobre 2013, de 19 heures à 21 h 30 (STR)	- Conséquences des programmes de surveillance américains sur la sphère sécurisée américaine - Conséquences des programmes de surveillance américains sur les autres instruments de transfert internationaux (clauses contractuelles, règles d'entreprise contraignantes)	• Imke SOMMER, Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (ALLEMAGNE) • Christopher CONNOLLY – Galexia • Peter HUSTINX, contrôleur européen de la protection des données (CEPD) • **Isabelle FALQUE-PIERROTIN, p**résidente de la CNIL (FRANCE)
14 octobre 2013, de 15 heures à 18 h 30 (BXL)	- Surveillance électronique de masse des citoyens européens à l'échelle internationale, Conseil de l'Europe et	• Martin SCHEININ, ancien rapporteur spécial des Nations unies pour la promotion et la protection des droits de l'homme dans la lutte antiterroriste, professeur au European University Institute et responsable du projet "SURVEILLE" du 7e PC • Judge Bostjan ZUPANČIČ, juge à la CEDH (par

		vidéoconférence)
	législation de l'UE - Jurisprudence en matière de programmes de surveillance	• Douwe KORFF, professeur de droit, London Metropolitan University • Dominique GUIBERT, vice-président de la Ligue des droits de l'homme (LDH) • Nick PICKLES, directeur de Big Brother Watch • Constanze KURZ, informaticienne, chef de projet au Forschungszentrum für Kultur und Informatik
7 novembre 2013, de 9 heures à 11 h 30 et de 15 heures à 18 h 30 (BXL)	- Le rôle du centre d'analyse du renseignement européen IntCen dans les activités de l'UE dans le domaine du renseignement (à huis clos) - Programmes nationaux de surveillance de masse des données personnelles dans les États membres et leur compatibilité avec le droit européen - Le rôle du contrôle parlementaire des services de renseignement à l'échelle nationale à l'ère de la surveillance de masse (partie I) Commission de Venise (Royaume-Uni) - Groupe transatlantique d'experts	• Ilkka SALMI, directeur du centre d'analyse du renseignement européen (IntCen) • Sergio CARRERA, chercheur principal et directeur de la section JAI, Centre pour les études politiques européennes, Bruxelles • Francesco Ragazzi, professeur assistant en relations internationales, université de Leiden • Iain CAMERON, membre de la commission européenne pour la démocratie par le droit – "commission de Venise" • Ian LEIGH, professeur de droit, université de Durham • David BICKFORD, ancien directeur juridique des agences de sécurité et de renseignement MI5 et MI6 • Gus HOSEIN, directeur général, Privacy International • Paul NEMITZ, directeur, "Droits fondamentaux et citoyenneté", DG JUST, Commission européenne • Reinhard PRIEBE, directeur,

	(UE-États-unis)	"Gestion des crises et sécurité intérieure", DG HOME, Commission européenne
11 novembre 2013, de 15 heures à 18 h 30 (BXL)	- Programmes de surveillance américains et leurs conséquences sur le respect de la vie privée des citoyens européens (intervention de M. Jim SENSENBRENNER, membre du Congrès américain)	• Jim SENSENBRENNER, Chambre des représentants américaine (membre de la commission sur le pouvoir judiciaire et président de la sous-commission sur la criminalité, le terrorisme, la sécurité intérieure et les enquêtes)
	- Le rôle du contrôle parlementaire des services de renseignement à l'échelle nationale à l'ère de la surveillance de masse (NL, SW) (partie II)	• Peter ERIKSSON, président de la commission sur la Constitution, Parlement suédois (Riksdag) • A.H. VAN DELDEN, président du comité d'évaluation indépendant néerlandais des services de renseignements et de sécurité (CTIVD)
	- Programmes américains de la NSA pour la surveillance électronique de masse et le rôle des sociétés des technologies de l'information (Microsoft, Google, Facebook)	• Dorothee BELZ, vice-présidente, affaires juridiques et "corporate" Microsoft EMEA (Europe, Moyen-Orient et Afrique) • Nicklas LUNDBLAD, directeur, politiques publiques et relations gouvernementales, Google • Richard ALLAN, directeur de la politique publique pour les pays EMEA, Facebook
14 novembre 2013, de 15 heures à 18 h 30 (BXL) **Avec la commission AFET**	- Sécurité des technologies de l'information des institutions européennes (partie I) (PE, COM (CERT-UE), (EU-LISA)	• Giancarlo VILELLA, directeur général, DG ITEC, Parlement européen • Ronald PRINS, directeur et co-fondateur de Fox-IT • Freddy DEZEURE, chef de la force de travail CERT-UE, DG DIGIT, Commission européenne • Luca ZAMPAGLIONE, agent de sécurité, EU-LISA
	- Le rôle du contrôle parlementaire des services de renseignement à	• Armand DE DECKER, vice-président du Sénat belge, membre du comité de

	l'échelle nationale à l'ère de la surveillance de masse (partie III) (BE, DA)	surveillance des services de renseignement • Guy RAPAILLE, président du comité de surveillance des services de renseignement (Comité R) • Karsten LAURITZEN, membre de la commission des affaires juridiques, porte-parole pour les affaires juridiques, Parlement danois
18 novembre 2013, de 19 heures à 21 h 30 (STR)	- Jurisprudence et autres plaintes concernant les programmes de surveillance nationaux (partie II) (ONG polonaise)	• Adam Bodnar, vice-président, Helsinki Foundation for Human Rights, Pologne
2 décembre 2013, de 15 heures à 18 h 30 (BXL)	- Le rôle du contrôle parlementaire des services de renseignement à l'échelle nationale à l'ère de la surveillance de masse (partie IV) (Norvège)	• Michael TETZSCHNER, membre de la commission permanente sur le droit de regard et les affaires constitutionnelles, Norvège (Stortinget)
5 décembre 2013, de 15 heures à 18 h 30 (BXL)	- Sécurité des technologies de l'information des institutions européennes (partie II) - Les conséquences de la surveillance de masse sur la confidentialité dans le cadre des relations entre les avocats et leurs clients	• Olivier BURGERSDIJK, responsable stratégique, Centre européen de lutte contre la cybercriminalité, EUROPOL • Udo HELMBRECHT, directeur général de l'ENISA • Florian WALTHER, consultant indépendant spécialisé dans la sécurité des technologies de l'information • Jonathan GOLDSMITH, secrétaire général, Conseil consultatif des barreaux européens (CCBE)
9 décembre 2013 (STR)	- Rétablir la confiance dans les flux d'échange de données entre l'Union européenne et les États-Unis - Résolution du Conseil de l'Europe 1954 (2013) "Sécurité nationale et accès à l'information"	• Viviane REDING, vice-présidente de la Commission européenne • Arcadio DÍAZ TEJERA, membre du sénat espagnol, membre de l'assemblée parlementaire du Conseil de l'Europe et rapporteur pour la résolution 1954 (2013) "Sécurité nationale et accès à l'information"
17 et	Commission d'enquête	• Vanessa GRAZZIOTIN,

18 décembre (BXL)	parlementaire sur l'espionnage du sénat brésilien (vidéoconférence) Instruments issus des technologies de l'information permettant de protéger le respect de la vie privée Échange de vues avec le journaliste à l'origine de la publication des faits (partie II) vidéoconférence)	présidente de la commission d'enquête parlementaire sur l'espionnage • Ricardo DE REZENDE FERRAÇO, rapporteur de la commission d'enquête parlementaire sur l'espionnage • Bart PRENEEL, professeur de sécurité informatique et de cryptographie industrielle à l'université KU Leuven, Belgique • Stephan LECHNER, directeur, Institut pour la protection et la sécurité des citoyens (IPSC), - Centre commun de recherche (JRC), Commission européenne • Christopher SOGHOIAN, technologue en chef, porte-parole, projet Privacy & Technology, American Civil Liberties Union • Christian HORCHERT, consultant en sécurité des technologies de l'information, Allemagne • Glenn GREENWALD, auteur et chroniqueur spécialisé dans les questions de sécurité nationale et les libertés civiles, précédemment pour le quotidien *The Guardian*

ANNEXE III: LISTE DES EXPERTS QUI ONT REFUSÉ DE PARTICIPER AUX AUDITIONS PUBLIQUES DE LA COMMISSION D'ENQUÊTE LIBE

1. Experts qui ont décliné l'invitation du président de la commission LIBE

États-Unis

- M. Keith Alexander, général de l'armée américaine, directeur de la NSA[1]
- M. Robert S. Litt, conseil général, Bureau du directeur des services nationaux de renseignement[2]
- M. Robert A. Wood, chargé d'affaires, représentant des États-Unis auprès de l'Union européenne

Royaume-Uni

- Sir Iain Lobban, directeur du quartier général des communications du Royaume-Uni (GCHQ)

France

- M. Bajolet, directeur général de la sécurité extérieure, France
- M. Calvar, directeur central de la sécurité intérieure, France

Pays-Bas

- M. Ronald Plasterk, ministre de l'intérieur et des relations du royaume des Pays-Bas
- M. Ivo Opstelten, ministre de la sécurité et de la justice des Pays-Bas

Pologne

- M. Dariusz Łuczak, directeur de l'agence pour la sécurité intérieure de Pologne
- M. Maciej Hunia, directeur de l'agence polonaise des renseignements extérieurs

Sociétés privées des technologies de l'information

- Tekedra N. Mawakana, directeur global de la politique publique et conseiller général adjoint, Yahoo
- D[r] Saskia Horsch, cadre supérieur, politiques publiques, Amazon

[1] Le rapporteur a rencontré M. Alexander, le président Brok et le sénateur Feinstein le 29 octobre 2013 à Washington.
[2] La délégation LIBE a rencontré M. Litt le 29 octobre 2013 à Washignton.

Sociétés européennes de télécommunication

- M[me] Doutriaux, Orange
- M. Larry Stone, président du groupe affaires publiques et gouvernementales, British Telecom, Royaume-Uni
- Telekom, Allemagne
- Vodafone

2. Experts qui n'ont pas répondu à l'invitation du président de la commission LIBE

Allemagne

- M. Gerhard Schindler, Präsident des Bundesnachrichtendienstes

Pays-Bas

- M[me] Berndsen-Jansen, Voorzitter Vaste Kamer Commissie voor Binnenlandse Zaken Tweede Kamer der Staten-Generaal, Pays-Bas
- M. Rob Bertholee, directeur, Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Suède

- M. Ingvar Åkesson, National Defence Radio Establishment
  (Försvarets radioanstalt, FRA)