Mercredi 12 mars 2014

P7_TA(2014)0230

Programme de surveillance de la NSA, organismes de surveillance dans divers États membres et incidences sur les droits fondamentaux des citoyens européens

Résolution du Parlement européen du 12 mars 2014 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))

(2017/C 378/14)

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 de Vienne sur les relations diplomatiques, en particulier ses articles 24, 27 et 40,

— 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, remis le 17 mai 2010 ([2]),

— vu la communication de la Commission intitulée «Politique et gouvernance de l'internet: le rôle de l'Europe à l'avenir» (COM(2014)0072),

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

— 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,

([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 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 ([5]), et en particulier son titre III,

— vu la décision 2000/520/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)0196) et du 20 octobre 2004 (SEC(2004)1323),

— vu la communication de la Commission du 27 novembre 2013 sur le fonctionnement de la «sphère de sécurité» du point de vue des citoyens européens et des entreprises établies dans l'Union (COM(2013)0847) 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)0846),

— vu sa résolution du 5 juillet 2000 sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la «sphère de sécurité» et les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis ([6]), qui a estimé que la pertinence du système ne pouvait être confirmée, ainsi que les avis du groupe de travail «Article 29», en particulier l'avis 4/2000 du 16 mai 2000 ([7]),

— vu les accords conclus entre les États-Unis d'Amérique et l'Union européenne en 2004, 2007 ([8]) et 2012 ([9]) 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 ([10]) accompagnant le rapport de la Commission au Parlement européen et au Conseil sur l'examen conjoint (COM(2013)0844),

---

([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.
([6]) JO C 121 du 24.4.2001, p. 152.
([7]) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32fr.pdf.
([8]) JO L 204 du 4.8.2007, p. 18.
([9]) JO L 215 du 11.8.2012, p. 5.
([10]) SEC(2013)0630 du 27.11.2013.

Mercredi 12 mars 2014

— 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 ([1]);

— 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) ([2]), 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 ([3]),

— 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'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 tiers, ainsi que des actions fondées sur elle ou en découlant ([4]),

— 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 la directive présidentielle n° 28 (Presidential Policy Directive — PPD-28) sur le renseignement d'origine électromagnétique promulguée par Barack Obama, président des États-Unis, le 17 janvier 2014,

— vu les propositions législatives en cours d'examen par le Congrès américain, dont le projet de loi sur la liberté (US Freedom Act) ou le projet de loi sur le contrôle du renseignement et la réforme de la surveillance, entre autres,

— 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, ainsi que la décision du tribunal de district des États-Unis pour le district sud de New York, ACLU e.a./James R. Clapper e.a, action civile n° 13-3994 du 11 juin 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 ([5]),

---

([1]) Avis de l'avocat général Cruz Villalón du 12 décembre 2013 dans l'affaire C-293/12.
([2]) JO L 195 du 27.7.2010, p. 3.
([3]) JO L 181 du 19.7.2003, p. 34.
([4]) JO L 309 du 29.11.1996, p. 1.
([5]) Document du Conseil 16987/2013.

— vu ses résolutions du 5 septembre 2001 ([1]) et du 7 novembre 2002 ([2]) 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 ([4]), dans laquelle il chargeait sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur cette question,

— vu le document de travail n° 1 sur les programmes de surveillance des États-Unis et de l'Union européenne et leur impact sur les droits fondamentaux des citoyens de l'Union,

— vu le document de travail n° 3 sur la 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,

— vu le document de travail n° 4 relatif aux activités de surveillance des États-Unis à l'égard des données de l'Union européenne et à leurs implications juridiques éventuelles sur les accords et la coopération transatlantiques,

— vu le document de travail n° 5 sur le contrôle démocratique des services de renseignement des États membres et des organes de renseignement de l'Union européenne,

— vu le document de travail de la commission des affaires étrangères sur les aspects de politique étrangère de l'enquête sur la surveillance électronique de masse des citoyens de l'Union européenne;

— vu sa résolution du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux: recommandations sur des actions et des initiatives à entreprendre ([5]),

— 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 ([6]),

— vu sa résolution du 10 décembre 2013 sur l'exploitation du potentiel de l'informatique en nuage en Europe ([7]),

— 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 ([8]),

— 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 (A7-0139/2014),

Les incidences de la surveillance de masse

A. considérant que la protection des données et la vie privée sont des droits fondamentaux; considérant que les mesures de sécurité, notamment dans le cadre de la lutte contre le terrorisme, doivent donc s'inscrire dans l'état de droit et respecter les obligations en matière de droits de l'homme, y compris celles qui ont trait à la vie privée et à la protection des données;

([1]) JO C 72 E du 21.3.2002, p. 221.
([2]) JO C 16 E du 22.1.2004, p. 88.
([3]) Textes adoptés de cette date, P7_TA(2013)0203.
([4]) Textes adoptés de cette date, P7_TA(2013)0322.
([5]) Textes adoptés de cette date, P7_TA(2013)0444.
([6]) Textes adoptés de cette date, P7_TA(2013)0449.
([7]) Textes adoptés de cette date, P7_TA(2013)0535.
([8]) JO C 353 E du 3.12.2013, p. 156.

B. considérant que les flux d'information et les données, qui dominent aujourd'hui la vie quotidienne et font partie de l'intégrité de toute personne, doivent être aussi sûrs que les domiciles devant les intrusions;

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

D. considérant que la coopération entre les États-Unis et l'Union européenne et ses États membres dans le domaine de la lutte contre le terrorisme restent d'une importance cruciale pour la sécurité et la sûreté des deux partenaires;

E. considérant que la confiance et la compréhension mutuelles constituent des facteurs clés dans le dialogue et le partenariat transatlantiques;

F. considérant qu'après le 11 septembre 2001, la lutte contre le terrorisme est devenue l'une des grandes priorités de la plupart des gouvernements; considérant que les révélations fondées sur les documents divulgués par Edward Snowden, ancien consultant de la NSA, ont contraint les dirigeants politiques à faire face aux défis de la supervision et du contrôle des agences de renseignement dans le cadre de leurs activités de surveillance et à évaluer les incidences de leurs activités sur les droits fondamentaux et l'état de droit dans la société démocratique;

G. 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;

— la violation des normes juridiques et des droits fondamentaux de l'Union européenne ainsi que des normes européennes en matière de 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 manque de contrôle et de surveillance effective 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 au sens strict, par exemple à des fins d'espionnage économique et industriel ou de profilage pour des motifs politiques;

— l'atteinte à la liberté de la presse et aux communications des membres des professions soumises au secret professionnel, dont les avocats et les médecins;

— 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 les activités répressives et les activités de renseignement, avec pour effet que chaque citoyen est traité comme un suspect et fait l'objet d'une surveillance;

— les menaces relatives à la vie privée à l'heure du numérique et l'incidence de la surveillance de masse sur les citoyens et les sociétés;

H. 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 des parlements nationaux des États membres ainsi que de leurs autorités judiciaires;

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

J. considérant que M. Obama a récemment annoncé une réforme de la NSA et de ses programmes de surveillance;

K. considérant qu'en comparaison des mesures prises par les institutions européennes et par certains États membres, le Parlement européen a pris très au sérieux son obligation de faire la lumière sur les révélations des pratiques non sélectives de surveillance de masse des citoyens européens et, par sa résolution du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine, les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, a chargé sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur la question;

L. 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

M. 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]); qu'en revanche, le tribunal de district pour le district sud de New York a jugé que cette collecte était légale dans sa décision du 27 décembre 2013;

N. considérant qu'une décision du tribunal de district de la région orientale de l'État du 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 ([2]);

O. considérant que dans son rapport du 12 décembre 2013, le groupe d'étude du président sur la révision des renseignements et des technologies propose 46 recommandations au président des États-Unis; que ces recommandations soulignent la nécessité de protéger à la fois la sécurité nationale et la vie privée et les libertés civiles; 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 la cour dite FISC (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 à 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;

P. considérant que, selon un mémorandum public remis à M. Obama par les anciens hauts responsables de la NSA (Veteran Intelligence Professionals for Sanity) le 7 janvier 2014 ([3]), la collecte massive de données ne renforce pas la capacité de la NSA à prévenir de futures attaques terroristes; que les auteurs soulignent que la surveillance de masse réalisée par la NSA n'a prévenu aucune attaque et que des milliards de dollars ont été dépensés dans des programmes moins efficaces et considérablement plus irrespectueux de la vie privée des citoyens qu'une technologie baptisée THINTHREAD développée en interne en 2001;

Q. 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 le principe fondamental 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; que ces recommandations ne préconisent pas d'octroyer aux ressortissants non américains les mêmes droits et protections qu'aux ressortissants américains;

([1]) Klayman e.a./Obama e.a.., action civile n° 13-0851, 16 décembre 2013.
([2]) ACLU/NSA n° 06-CV-10204, 17 août 2006.
([3]) http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

Mercredi 12 mars 2014

R. considérant que, dans sa directive présidentielle sur le renseignement électromagnétique (Presidential Policy Directive on Signals Intelligence Activties) du 17 janvier 2014 et le discours associé, le président Barack Obama a déclaré que la surveillance électronique de masse était nécessaire pour permettre aux États-Unis d'assurer la sécurité nationale, de protéger leurs citoyens et les citoyens de leurs alliés et partenaires, ainsi que de promouvoir leurs intérêts en matière de politique étrangère; considérant que cette directive comporte certains principes relatifs au recueil, à l'utilisation et au partage des renseignements électromagnétiques et étend certaines garanties à des citoyens non américains, en accordant en partie un traitement équivalent à celui dont bénéficient les ressortissants américains, dont des garanties concernant les informations personnelles de tous, indépendamment de la nationalité ou du lieu de résidence; considérant cependant que le président Obama n'a préconisé aucune proposition concrète, en particulier en ce qui concerne l'interdiction des activités de surveillance de masse et l'instauration de voies de recours administratives et juridictionnelles pour les ressortissants non américains;

Cadre juridique

Droits fondamentaux

S. 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 permis d'établir les faits relatifs aux programmes de surveillance américains; 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 américaines des questions ayant trait à la sécurité nationale;

T. considérant que les droits fondamentaux, notamment les libertés 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; considérant que la surveillance de masse des êtres humains est incompatible avec celles-ci;

U. considérant que dans tous les États membres, le droit protège contre la divulgation d'informations communiquées à titre confidentiel entre un avocat et son client, principe reconnu par la Cour de justice de l'Union européenne ([1]);

V. considérant que dans sa résolution du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux, il invite la Commission à présenter une proposition législative visant à mettre en place un programme européen efficace et complet de protection des lanceurs d'alerte afin de protéger les intérêts financiers de l'Union européenne et à examiner s'il convient d'étendre ces futures dispositions à d'autres domaines de compétence de l'Union;

Compétences de l'Union dans le domaine de la sécurité

W. considérant qu'en vertu de l'article 67, paragraphe 3, du traité FUE, l'Union européenne «œuvre pour assurer un niveau élevé de sécurité»; que les dispositions du traité (notamment l'article 4, paragraphe 2, du traité UE, ainsi que les articles 72 et 73 du traité FUE) signifient que l'Union européenne est dotée de certaines compétences sur les questions ayant trait à la sécurité collective de l'Union; que l'Union est compétente dans les domaines relatifs à la sécurité intérieure (article 4, paragraphe 2, point j), du traité FUE) et exerce cette compétence 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;

X. considérant que le traité sur le fonctionnement de l'Union européenne dispose qu'«il est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale» (article 73 du traité FUE);

Y. considérant que l'article 276 du traité sur le fonctionnement de l'Union européenne dispose que «dans l'exercice de ses attributions concernant les dispositions des chapitres 4 et 5 du titre V, de la troisième partie, relatives à l'espace de liberté, de sécurité et de justice, la Cour de justice de l'Union européenne n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un État membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure»;

([1]) Arrêt du 18 mai 1982 dans l'affaire C-155/79, AM & S Europe Limited/Commission des Communautés européennes.

Z. considérant que les notions de «sécurité nationale», de «sécurité intérieure», de «sécurité intérieure de l'Union» et de «sécurité internationale» se recoupent; 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;

AA. considérant que les traités européens assignent à la Commission le rôle de «gardienne des traités» et donc, que la Commission est légalement tenue d'enquêter sur toute violation éventuelle du droit de l'Union;

AB. considérant que, conformément à l'article 6 du traité sur l'Union européenne, où il est fait référence à la charte des droits fondamentaux de l'Union européenne et à la CEDH, les agences des États membres et même les parties privées agissant dans le domaine de la sécurité nationale sont aussi tenues de respecter les droits consacrés par les dispositions de ces deux textes, tant à l'égard de leurs propres citoyens ou que des citoyens des autres États;

Extraterritorialité

AC. 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; que, dans ces circonstances, il est nécessaire d'entreprendre une action au niveau de l'Union afin de garantir le respect sur son territoire des valeurs de l'Union consacrées par l'article 2 du traité UE, par la charte des droits fondamentaux et par la CEDH concernant les droits fondamentaux, la démocratie et l'état de droit, et des droits des personnes physiques ou morales consacrés dans la législation dérivée appliquant ces principes fondamentaux, 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

AD. considérant que le transfert de données à caractère personnel par les institutions, organes ou organismes 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, organe ou organisme 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;

AE. considérant que le transfert de données n'est pas limité sur le plan géographique et que, notamment eu égard au développement de la mondialisation et des communications à l'échelle mondiale, le législateur européen fait face à de nouveaux défis en matière de protection des données et des communications à caractère personnel; qu'il est donc de la plus grande importance de promouvoir les cadres juridiques établissant des règles communes;

AF. considérant que la collecte massive de données à caractère personnel à des fins commerciales et au nom de la lutte contre le terrorisme et contre la grande criminalité transnationale met à mal les droits des citoyens de l'Union en matière de vie privée et de protection des données à caractère personnel;

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

AG. 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;

AH. 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 2000/520/CE, a déclaré adéquate 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»;

([1]) Voir notamment les affaires jointes C-6/90 et C-9/90, Francovich e.a./Italie, arrêt du 19 novembre 1991.

AI. considérant que dans sa résolution du 5 juillet 2000, il 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;

AJ. considérant que, dans le document de travail n° 4 du Parlement européen du 12 décembre 2013 relatif aux activités de surveillance des États-Unis à l'égard des données de l'Union européenne et à leurs implications juridiques éventuelles sur les accords et la coopération transatlantiques, les rapporteurs ont manifesté leurs doutes et leurs inquiétudes quant au caractère approprié de la «sphère de sécurité» et ont demandé à la Commission d'abroger la décision sur la pertinence de la «sphère de sécurité» et de trouver de nouvelles solutions juridiques;

AK. considérant qu'en vertu de la décision 2000/520/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;

AL. considérant que la décision 2000/520/CE de la Commission précise 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 des mesures à prendre en vue d'abroger ou de suspendre ladite décision ou d'en limiter la portée;

AM. 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 une série de recommandations aux autorités américaines en vue de corriger ces lacunes;

AN. 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; 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; 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»;

AO. considérant que du 28 au 31 octobre 2013, une délégation de la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE) du Parlement européen a rencontré, à Washington D.C., le ministère américain du commerce et la commission fédérale du commerce des États-Unis; que le ministère du commerce a reconnu l'existence d'organisations ayant déclaré adhérer 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; 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;

AP. 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»; 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; que le champ d'application de cette dérogation aurait dû être précisé par les États-Unis et l'Union européenne, et en particulier par la Commission, afin d'éviter toute interprétation ou application invalidant en substance le droit fondamental à la vie privée et à la protection des données, entre autres; que, par conséquent, une telle dérogation ne doit pas être utilisée d'une manière qui nuirait à ou invaliderait la protection apportée par la charte des droits fondamentaux, la CEDH, la législation de l'Union européenne sur la protection des données et les principes de la «sphère de sécurité»; qu'en cas d'invocation de la dérogation à des fins de sécurité nationale, il est impératif de préciser en vertu du droit national de quel pays;

AQ. 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; 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

AR. considérant que selon les informations communiquées et les conclusions de l'enquête réalisée par la commission LIBE, les services nationaux de sécurité néozélandais, canadiens et australiens ont été impliqués 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 eux des données à caractère personnel de citoyens européens transférées depuis l'Union européenne;

AS. considérant que les décisions 2013/65/UE ([1]) et 2002/2/CE ([2]) de la Commission ont déclaré adéquat le niveau de protection garanti respectivement par la loi néozélandaise sur le respect de la vie privée et la loi canadienne relative à la protection des informations à caractère personnel et aux documents électroniques; 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; que la Commission ne s'est pas penchée sur cet aspect;

Transferts fondés sur des clauses contractuelles et d'autres instruments

AT. 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;

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

AV. considérant que la directive 95/46/CE permet à la Commission de décider que certaines clauses contractuelles types présentent 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;

AW. 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 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;

AX. 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; 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; que les REC applicables aux sous-traitants pour le traitement des données ont été rejetées dans le rapport de la commission LIBE relatif au règlement général sur la protection des données, étant donné qu'elles auraient enlevé au responsable du traitement des données et à la personne concernée tout contrôle sur la juridiction dans laquelle leurs données sont traitées;

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

Mercredi 12 mars 2014

AY. considérant qu'en vertu de la compétence qui lui est attribuée par l'article 218 du traité FUE, le Parlement européen a pour responsabilité de contrôler en permanence la valeur des accords internationaux qu'il a approuvés;

Transferts basés sur les accords TFTP et PNR

AZ. considérant que dans sa résolution du 23 octobre 2013, il 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 TFTP, et notamment à son article premier;

BA. considérant que la surveillance du financement du terrorisme est un outil essentiel dans la lutte contre le financement du terrorisme et la grande criminalité qui permet aux enquêteurs antiterroristes de mettre au jour des liens entre les personnes ciblées par leurs enquêtes et d'autres suspects potentiels en rapport avec des réseaux terroristes plus larges suspectés de financer le terrorisme;

BB. considérant qu'il a demandé à la Commission de suspendre l'accord et a réclamé un accès immédiat à toutes les informations et documents utiles pour ses délibérations; que la Commission n'a accédé à aucune de ces demandes;

BC. 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; 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; qu'il n'est pas certain que les autorités américaines aient contourné l'accord en accédant à ces données par d'autres moyens, tel qu'indiqué dans la lettre du 18 septembre 2013 des autorités américaines ([1]);

BD. 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; 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; 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; que le 18 décembre 2013, M. Glenn Greenwald a déclaré dans le cadre de l'enquête menée par la commission LIBE que la NSA et le GCHQ avaient ciblé les réseaux SWIFT;

BE. 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 ([2]);

BF. considérant que selon 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 précises de l'accord;

BG. 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; que cette absence de droits judiciaires ou administratifs annule les protections prévues pour les citoyens de l'Union dans l'accord PNR existant;

([1]) La lettre mentionne que le gouvernement des États-Unis recherche et obtient des informations financières […] (qui) sont collectées via des voies réglementaires, des mesures d'application de la loi, des voies diplomatiques et des activités de renseignement ainsi que des échanges avec des partenaires étrangers […] le gouvernement américain a recours au TFTP pour obtenir des données SWIFT que nous ne pouvons obtenir par d'autres sources.

([2]) 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

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

BH. considérant que l'accord entre l'Union européenne et les États-Unis sur l'entraide judiciaire en matière pénale du 6 juin 2003 ([1]) 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»)

BI. 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; que les négociations ont été autorisées par le Conseil le 2 décembre 2010; que cet accord revêt une importance primordiale et contribuerait à faciliter les transferts de données dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale;

BJ. 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 sur le plan judiciaire à leurs données à caractère personnel aux États-Unis, et de les rectifier et de les effacer, ainsi que le droit à des moyens de recours judiciaire ou administratif efficaces pour les citoyens de l'Union aux États-Unis et à une surveillance indépendante des activités de traitement de données;

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

BL. 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

BM. 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; que la Commission a présenté en janvier 2012 un ensemble de propositions législatives: un règlement général sur la protection des données ([2]), qui remplacera la directive 95/46/CE et établira une législation uniforme dans toute l'Union, et une directive ([3]) 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;

BN. 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;

BO. 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 toujours pas parvenu, après deux années de délibérations, à définir une approche globale concernant le règlement général sur la protection des données et la directive ([4]);

([1]) JO L 181 du 19.7.2003, p. 25.
([2]) COM(2012)0011 du 25.1.2012.
([3]) COM(2012)0010 du 25.1.2012.
([4]) http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/ec/139210.pdf

Mercredi 12 mars 2014

Sécurité informatique et informatique en nuage

BP. considérant que sa résolution du 10 décembre 2013 mentionnée ci-dessus souligne le potentiel économique offert par l'informatique en nuage pour la croissance et l'emploi; que, selon les prévisions, la valeur économique globale du marché de l'informatique en nuage équivaut à 207 milliards de dollars américains par an d'ici à 2016, soit le double de sa valeur en 2012;

BQ. 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; que le droit de l'Union en matière de protection des données, neutre sur le plan technologique, s'applique déjà pleinement aux services d'informatique en nuage actifs dans l'Union européenne;

BR. considérant que les activités de surveillance de masse donnent aux agences de renseignement l'accès aux données à caractère personnel stockées ou autrement traitées 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; que les services de renseignement américains ont accédé à des données à caractère personnel stockées ou autrement traitées dans des serveurs localisés sur le sol européen en exploitant les réseaux internes de Yahoo et Google; que de telles activités constituent une violation des obligations internationales et des normes européennes en matière de droits fondamentaux, dont font partie le droit à la vie privée et familiale, la confidentialité des communications, la présomption d'innocence, la liberté d'expression, la liberté d'information, la liberté de réunion et d'association et la liberté d'entreprise; 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;

BS. considérant que les services de renseignement américains appliquent une politique de sape systématique des protocoles et produits cryptographiques afin d'être en mesure d'intercepter même les communications cryptées; que l'agence de sécurité nationale des États-Unis a collecté un grand nombre de «vulnérabilités jour zéro» — à savoir des vulnérabilités informatiques en matière de sécurité dont le public et le fournisseur du produit n'ont pas encore connaissance; que de telles activités mettent considérablement à mal les efforts mondiaux visant à améliorer la sécurité informatique;

BT. considérant que le fait que les agences de renseignement aient eu accès aux données à caractère personnel des utilisateurs de services en ligne a fortement dégradé la confiance des citoyens dans ces services, ce qui a donc un effet néfaste sur les entreprises investissant dans le développement de nouveaux services qui ont recours aux «données massives» et de nouvelles applications, telles que l'internet des objets;

BU. considérant que les fournisseurs de technologies de l'information proposent souvent des produits dont la sécurité informatique n'a pas été convenablement testée ou qui parfois disposent de portes dérobées intégrées à dessein par le fournisseur; que l'absence de règles en matière de responsabilité des fournisseurs de logiciels a conduit à une telle situation, qui est exploitée par les services de renseignement, mais qui ouvre aussi la voie au risque d'attaques d'autres entités;

BV. considérant qu'il est essentiel que les entreprises fournissant ce type de nouveaux services et de nouvelles applications respectent les règles relatives à la protection des données et à la vie privée des utilisateurs dont les données sont collectées, traitées et analysées, afin de maintenir la confiance des citoyens à un niveau élevé;

Contrôle démocratique des services de renseignement

BW. considérant que, dans les sociétés démocratiques, les services de renseignement sont dotés de pouvoirs et moyens spéciaux pour protéger les droits fondamentaux, la démocratie et l'état de droit, les droits des citoyens et l'État contre les menaces intérieures et extérieures, et font l'objet d'un contrôle démocratique et judiciaire; qu'ils jouissent de capacités et de pouvoirs spéciaux uniquement à cet effet; que ces pouvoirs doivent être employés dans les limites du cadre juridique imposé par les droits fondamentaux, la démocratie et l'état de droit et que leur application doit être strictement contrôlée, sans quoi ils perdent leur légitimité et risquent de porter atteinte à la démocratie;

BX. considérant que, si un certain degré de confidentialité est accordé aux 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, cette confidentialité ne peut outrepasser ou exclure les règles relatives au contrôle et à l'examen démocratiques et judiciaires de leurs activités, ainsi que les règles de transparence, notamment en ce qui concerne le respect des droits fondamentaux et de l'état de droit, qui sont autant d'éléments essentiels des sociétés démocratiques;

BY. 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 rapides progrès technologiques et évolutions politiques de la décennie écoulée, qui ont conduit les services de renseignements à coopérer davantage à l'échelle internationale, notamment par l'échange à grande échelle de données à caractère personnel, ce qui crée souvent une confusion des genres entre renseignement et répression;

BZ. considérant que le contrôle démocratique des services de renseignement est toujours effectué uniquement 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; 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;

CA. considérant que les organes de contrôle nationaux n'ont souvent pas pleinement accès aux renseignements reçus des services étrangers, ce qui est susceptible de créer un «entre-deux» où les échanges internationaux d'informations peuvent avoir lieu sans contrôle approprié; que ce problème est aggravé par la règle dite du «tiers service» ou le principe du «contrôle par l'entité d'origine», qui vise à permettre à l'entité dont émanent les informations de décider de la diffusion ou non de ses informations sensibles à d'autres entités mais qui est parfois malheureusement interprétée en ce sens qu'elle s'applique aussi au contrôle des services destinataires;

CB. considérant que les initiatives de réforme en matière de transparence des secteurs public et privé sont essentielles pour donner confiance au public dans les activités des services de renseignement; que les systèmes juridiques ne devraient pas empêcher les entreprises de rendre publique la façon dont elle traite tous les types de requêtes des gouvernements et d'injonctions des tribunaux demandant l'accès aux données de leurs utilisateurs, y compris la divulgation d'informations globales sur le nombre de requêtes et d'injonctions acceptées et rejetées;

Conclusions principales

1. estime que les récentes révélations faites dans la presse par des lanceurs d'alerte et des journalistes, ainsi que les témoignages d'experts recueillis pendant cette enquête, les aveux des autorités et l'insuffisance de la réaction face à ces allégations, 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 de communication, y compris les données de contenu, et les données et métadonnées de localisation des citoyens du monde entier, à une échelle sans précédent, sans aucun discernement et sans se baser sur des soupçons;

2. appelle plus particulièrement l'attention sur les programmes de renseignement de la NSA permettant la surveillance de masse des citoyens de l'Union européenne grâce à l'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), et à l'accès aux réseaux informatiques et téléphoniques et aux données de localisation, mais aussi sur les systèmes de l'agence de renseignement britannique GCHQ, notamment son activité de surveillance en amont (programme Tempora) et son programme de décryptage (Edgehill), les attaques ciblées «de l'homme du milieu» sur des systèmes informatiques (programmes Quantum et Foxacid) et la collecte et la conservation de quelque 200 millions de SMS par jour (programme Dishfire);

3. prend note des allégations de piratage ou d'exploitation des systèmes de Belgacom par l'agence de renseignement britannique GCHQ; constate que Belgacom a indiqué ne pas être en mesure de confirmer ou d'infirmer que les institutions de l'Union européenne étaient ciblées ou touchées, et a affirmé que les logiciels malveillants utilisés étaient des logiciels extrêmement complexes dont le développement et l'utilisation ont nécessité d'importants moyens financiers et humains dont n'auraient pas pu disposer des entités privées ou des pirates;

4. souligne que la confiance a été profondément mise à mal, à savoir la confiance entre les deux partenaires transatlantiques, la confiance entre les citoyens et leurs gouvernements, la confiance dans le fonctionnement des institutions démocratiques des deux côtés de l'Atlantique, la confiance à l'égard du respect de l'état de droit et la confiance dans la sécurité des services et des communications informatiques; pense que pour restaurer la confiance à tous ces égards, il est indispensable d'adopter un plan d'intervention immédiat et global prévoyant un ensemble de mesures soumises au contrôle des citoyens;

5. note que plusieurs gouvernements affirment que ces programmes de surveillance de masse sont nécessaires à la lutte contre le terrorisme; dénonce fermement le terrorisme, mais est convaincu que la lutte contre le terrorisme ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, secrets, voire illégaux; estime que de tels programmes sont incompatibles avec les principes de nécessité et de proportionnalité en vigueur dans les sociétés démocratiques;

6. réaffirme la ferme conviction de l'Union selon laquelle il convient d'établir un juste équilibre entre les mesures de sécurité et la protection des libertés civiles et des droits fondamentaux, tout en veillant au respect le plus strict de la vie privée et de la protection des données;

7. considère que, face à une collecte de données d'une telle ampleur, on peut sérieusement douter que ces mesures ne soient motivées que par la seule lutte contre le terrorisme, étant donné qu'elles supposent le recueil de toutes les données possibles de l'ensemble des citoyens; signale par conséquent l'existence possible d'autres motifs, notamment l'espionnage politique et économique, qu'il faut entièrement dissiper;

8. 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 sur le fonctionnement de l'Union européenne; réaffirme le principe de coopération loyale établi à l'article 4, paragraphe 3, du traité sur l'Union européenne 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»;

9. relève 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;

10. condamne 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 les systèmes de surveillance de masse sans discernement mis en place par les services de renseignement constituent 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 de toute 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, ainsi que sur la liberté de réunion et d'association, 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 donnent également 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;

11. juge capital de protéger le secret professionnel des avocats, des journalistes, des médecins et des autres professions réglementées contre les activités de surveillance de masse; souligne en particulier que toute incertitude concernant la confidentialité des communications entres les avocats et leurs clients pourrait avoir des incidences négatives sur le droit d'accès des citoyens de l'Union européenne à l'assistance juridique et à la justice, ainsi que le droit à un procès équitable;

12. estime que les programmes de surveillance constituent une nouvelle étape vers la mise en place d'un État «ultrapréventif», s'éloignant du modèle établi du droit pénal en vigueur dans les sociétés démocratiques, selon lequel toute atteinte aux droits fondamentaux d'un suspect nécessite l'autorisation d'un juge ou d'un procureur, en l'existence de soupçons raisonnables, et doit impérativement être régie par la loi, pour y substituer un mélange d'activités de répression et de renseignement avec des garanties juridiques floues et affaiblies, allant bien souvent à l'encontre des freins et contrepoids démocratiques et 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;

13. est convaincu que les législations et tribunaux secrets constituent une violation de l'état de droit; souligne que les arrêts des cours ou tribunaux et les décisions d'autorités administratives d'un pays tiers autorisant, directement ou indirectement, le transfert de données personnelles, ne doivent en aucun cas être reconnus ou appliqués, sauf si un traité d'entraide judiciaire ou un accord international est en vigueur entre le pays tiers demandeur et l'Union ou un État membre, et sous réserve de l'accord préalable de l'autorité de contrôle compétente; rappelle que les arrêts rendus par des cours ou tribunaux secrets et les décisions émises par des autorités administratives de pays non membres de l'Union autorisant de manière confidentielle, directement ou indirectement, des activités de surveillance, ne doivent ni être reconnus, ni appliqués;

([1]) N° 1 BvR 518/02 du 4 avril 2006.

14. souligne que les préoccupations susmentionnées sont exacerbées par la rapidité des évolutions technologiques et sociétales, les appareils internet et mobiles étant omniprésents dans la vie quotidienne moderne («informatique ubiquitaire») et le modèle commercial de la plupart des entreprises du secteur de l'internet reposant sur le traitement de données à caractère personnel; estime que l'ampleur de ce problème est sans précédent; constate que l'on pourrait assister à une utilisation abusive des infrastructures de collecte massive et de traitement des données en cas de changement de régime politique;

15. observe qu'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 attaques d'intrus bien équipés («pas de sécurité informatique à 100 %»); note que pour pouvoir jouir d'une sécurité informatique maximale, les Européens doivent accepter de consacrer suffisamment de moyens, humains et financiers, à la préservation de l'indépendance et de l'autosuffisance de l'Europe dans le domaine des technologies de l'information;

16. rejette vivement l'idée selon laquelle toutes les questions liées aux programmes de surveillance de masse relèveraient strictement de la sécurité nationale et, dès lors, de l'unique compétence des États membres; réaffirme que les États membres doivent respecter pleinement la législation de l'Union et la convention européenne des droits de l'homme lorsqu'ils agissent pour assurer leur sécurité nationale; 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 qu'il y va de la protection de la vie privée de tous les citoyens de l'Union européenne, de même que de la sécurité et de la fiabilité de tous les réseaux de communication de l'Union; pense par conséquent qu'une discussion et une action au niveau de l'Union européenne ne sont pas seulement légitimes, mais nécessaires pour l'autonomie de l'Union;

17. 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;

18. 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 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;

19. compte demander à la nouvelle Commission qui sera désignée après les élections européennes de mai 2014 de prendre des engagements politiques forts en vue de mettre en œuvre les propositions et recommandations de l'enquête;

Recommandations

20. demande aux autorités américaines et aux États membres de l'Union européenne d'interdire les activités de surveillance de masse aveugle, s'ils ne l'ont pas déjà fait;

21. exhorte tous les États membres de l'Union, en particulier ceux qui participent aux programmes «9-eyes» et «14-eyes» ([2]), à procéder à un examen complet, et à la révision au besoin, de leurs législations et pratiques régissant les activités des services de renseignement afin de s'assurer qu'elles font l'objet d'un contrôle parlementaire et judiciaire et sont soumises à la vigilance des citoyens, qu'elles respectent les principes de légalité, de nécessité, de proportionnalité, de traitement équitable, d'information de l'utilisateur et de transparence, notamment en s'appuyant sur le recueil de bonnes pratiques des Nations unies et sur les recommandations de la Commission de Venise, et qu'elles sont conformes aux normes de la convention européenne des droits de l'homme et aux obligations des États membres en matière de droits fondamentaux, notamment en ce qui concerne la protection des données, le respect de la vie privée et la présomption d'innocence;

([1]) Arrêt du 4 juin 2013 dans l'affaire C-300/11, ZZ contre Secretary of State for the Home Department.

([2]) Le «programme "9-eyes» englobe les États-Unis, le Royaume-Uni, le Canada, l'Australie, la Nouvelle-Zélande, le Danemark, la France, la Norvège et les Pays-Bas; le programme «14-eyes» comprend aussi, outre ces pays, l'Allemagne, la Belgique, l'Italie, l'Espagne et la Suède.

22. invite tous les États membres de l'Union européenne et en particulier, compte tenu de sa résolution du 4 juillet 2013 et de ses auditions d'enquête, le Royaume-Uni, la France, l'Allemagne, la Suède, les Pays-Bas et la Pologne à veiller à ce que leur cadre législatif et leurs mécanismes de contrôle, actuels et à venir, applicables aux activités des services de renseignement soient conformes aux normes de la convention européenne des droits de l'homme et au droit de l'Union européenne en matière de protection des données; invite ces États membres à faire la lumière sur les allégations concernant des activités de surveillance massive, y compris la surveillance massive des communications transfrontalières, la surveillance non ciblée des communications par câble, les accords éventuels passés entre les services de renseignement et des entreprises de télécommunications concernant l'accès aux données personnelles et leur échange et l'accès aux câbles transatlantiques, la présence sur le territoire de l'Union européenne de personnels et d'équipements de renseignement américains sans contrôle sur les opérations de surveillance, et leur compatibilité avec la législation de l'Union; invite les parlements nationaux desdits pays à intensifier la coopération de leurs organes de surveillance des services de renseignement au niveau européen;

23. invite le Royaume-Uni, en particulier, compte tenu des nombreuses informations fournies par les médias faisant état d'une surveillance de masse par le service de renseignement GHCQ, à réviser son cadre juridique actuel consistant en l'«interaction complexe» de 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;

24. prend acte de la révision de la loi néerlandaise de 2002 sur le renseignement et la sécurité (rapport de la commission Dessens du 2 décembre 2013); soutient les recommandations de la commission de révision visant à augmenter la transparence du fonctionnement des services de renseignement néerlandais et à renforcer le contrôle et la supervision à l'égard de ces derniers; prie les Pays-Bas de s'abstenir d'étendre les pouvoirs des services de renseignement de façon à permettre de procéder également à une surveillance systématique et à grande échelle des communications par câble de citoyens innocents, en particulier compte tenu du fait que l'un des plus importants points d'échange internet (AMS-IX) se situe à Amsterdam; appelle à la prudence quant à la définition du mandat et des capacités de la nouvelle unité commune pour le renseignement d'origine électronique et informatique, ainsi qu'à l'égard de la présence et des activités de membres des services de renseignement américains sur le territoire des Pays-Bas;

25. invite les États membres, y compris lorsqu'ils sont représentés par leurs services de renseignement, 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;

26. demande que tous les services secrets cessent d'intercepter massivement et d'exploiter les images de webcams; invite les États membres à mener une enquête approfondie pour savoir si, comment et dans quelle mesure leurs services secrets respectifs ont pris part à la collecte et au traitement des images de webcams et à supprimer toutes les images enregistrées dans le cadre des programmes de surveillance de masse;

27. 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 ou par leurs propres services de renseignement et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers;

28. invite le secrétaire général du Conseil de l'Europe à lancer la procédure au titre de l'article 52 qui prévoit que «[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»;

29. 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 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);

30. invite les États membres à mettre en place des mécanismes efficaces par lesquels les personnes responsables des programmes de surveillance (de masse) qui enfreignent l'État de droit et les droits fondamentaux des citoyens doivent répondre des abus de pouvoir qu'ils ont commis;

31. 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, à mettre les droits des citoyens de l'Union sur un pied d'égalité avec ceux des citoyens américains et à signer le protocole optionnel permettant aux particuliers de soumettre des plaintes au titre du PIDCP;

32. salue, à cet égard, les observations et la directive présidentielle de Barack Obama, président des États-Unis, du 17 janvier 2014, y voyant un progrès vers la limitation des autorisations d'utiliser la surveillance et le traitement de données pour des motifs de sécurité nationale, et vers le traitement égal par la communauté américaine du renseignement des informations personnelles de tous, sans distinction liée à la nationalité ou au lieu de résidence; attend néanmoins que d'autres mesures plus spécifiques soient prises dans le cadre de la relation entre l'Union et les États-Unis, principalement en vue de consolider la confiance à l'égard des transferts de données transatlantiques et de fournir des garanties contraignantes concernant les droits opposables des ressortissants de l'Union, comme la présente résolution l'expose en détail;

33. souligne ses vives inquiétudes face aux travaux en cours au sein du comité de la convention cybercriminalité du Conseil de l'Europe sur l'interprétation de l'article 32 de la convention cybercriminalité du 23 novembre 2001 (convention de Budapest) concernant l'accès transfrontalier à des données informatiques stockées avec autorisation ou lorsque le public peut les consulter, et s'oppose à la conclusion de tout protocole additionnel et à la formulation de toute orientation visant à élargir le champ d'application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception de taille au principe de territorialité, en ce qu'il pourrait donner aux autorités répressives la possibilité d'accéder librement à distance aux serveurs et aux systèmes informatiques situés dans d'autres juridictions sans avoir recours aux accords multilatéraux et aux autres instruments de coopération judiciaire mis en place pour garantir les droits fondamentaux des personnes physiques, y compris la protection des données et l'application régulière de la loi, et notamment la convention n° 108 du Conseil de l'Europe;

34. 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;

35. demande à l'Agence des droits fondamentaux d'effectuer des recherches approfondies sur la protection des droits fondamentaux dans le contexte de la surveillance, et notamment sur l'actuelle situation juridique des citoyens de l'Union européenne pour ce qui touche aux voies de recours juridictionnelles dont ils disposent à l'égard de ces pratiques;

Transferts internationaux de données

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

36. 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 affirmé adhérer 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 (par exemple Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); est préoccupé par le fait que ces entreprises n'ont pas crypté les flux d'informations et de communications entre leurs centres de données, ce qui a permis aux services de renseignement d'intercepter les informations; salue les déclarations de certaines entreprises américaines faites en réponse à ces révélations, selon lesquelles elles accélèreraient les projets de mise en œuvre de cryptage des flux de données circulant entre leurs centres de données mondiaux;

37. 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 aux critères de dérogation visés au point «sûreté de l'État»;

38. 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, à condition que ces instruments présentent des garanties et des protections spécifiques et ne soient pas contournés par d'autres cadres juridiques;

39. est d'avis que la Commission n'a pas pris les mesures nécessaires pour remédier aux faiblesses bien connues dont souffre actuellement la mise en œuvre de la «sphère de sécurité»;

40. invite la Commission à présenter des mesures prévoyant la suspension immédiate de sa 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; invite par conséquent les autorités des États-Unis à présenter une proposition de nouveau cadre pour les transferts de données à caractère personnel de l'Union européenne vers les États-Unis, qui respecte les exigences de protection des données de la législation de l'Union et garantisse un degré de protection adéquat;

41. invite les autorités compétentes des États membres, en particulier 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 nécessaires en ce qui concerne la protection de la vie privée et les droits et libertés fondamentaux des individus;

42. invite la Commission à présenter d'ici décembre 2014 une évaluation complète du cadre américain en matière de respect de la vie privée, portant sur les activités commerciales, policières et de renseignement, ainsi que des recommandations concrètes en l'absence de loi générale sur la protection des données aux États-Unis; encourage la Commission à travailler de concert avec les autorités des États-Unis afin d'établir un cadre juridique garantissant un degré élevé de protection des personnes eu égard à la protection de leurs données à caractère personnel lorsqu'elles sont transférées aux États-Unis et à veiller à l'équivalence des cadres européen et américain de respect de la vie privée;

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

43. rappelle que la directive 95/46/CE dispose 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;

44. rappelle que la directive 95/46/CE précise également 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 de données ou à une catégorie de telles opérations; 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;

45. 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 doit engager des négociations en vue de remédier à cette situation;

46. invite la Commission et les États membres à déterminer sans tarder si le niveau de protection adéquat assuré par la loi de Nouvelle-Zélande sur la vie privée et par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, tel que déclaré par les décisions 2013/65/UE et 2002/2/CE de la Commission, a été affecté par la participation des agences nationales de renseignement de ces pays 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; invite également la Commission à examiner la situation d'autres pays ayant fait l'objet d'une évaluation du caractère adéquat du niveau de protection assuré; attend de la Commission qu'elle rende compte au Parlement de ses observations sur les pays mentionnés plus haut avant décembre 2014;

Transferts fondés sur des clauses contractuelles et d'autres instruments

47. 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 formulées 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;

48. invite les États membres à interdire ou à suspendre les flux de données vers des pays tiers, fondés sur des clauses contractuelles types, des clauses contractuelles ou des règles d'entreprise contraignantes autorisées par les autorités nationales compétentes lorsqu'il est probable que la loi à laquelle les destinataires de données sont soumis leur impose des obligations qui vont au-delà des restrictions strictement nécessaires, adéquates et proportionnées dans une société démocratique et qui risquent d'avoir un effet contraire 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 de dommages graves pour les personnes dont les données sont traitées;

49. 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;

50. invite la Commission à examiner sans plus attendre les clauses contractuelles types qu'elle a établies en 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

51. 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; demande également au Conseil et à la Commission d'évaluer les accords bilatéraux entre les États membres et les États-Unis afin de veiller à ce qu'ils soient en adéquation avec ceux que l'Union a mis ou décide de mettre en place avec les États-Unis;

Entraide judiciaire européenne en matière pénale

52. 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

53. 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,

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

55. invite la Commission 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»)

56. 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;

57. demande une reprise immédiate des négociations avec les États-Unis sur l'accord-cadre, en vue de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis; souligne en outre que l'accord devrait de plus permettre à tous les citoyens de l'Union d'introduire des recours administratifs et judiciaires efficaces et exécutoires aux États-Unis sans aucune discrimination;

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

59. 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

60. invite la présidence du Conseil et les États membres 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'un niveau élevé de protection des données dans un avenir très proche; souligne qu'un engagement réel et un soutien sans faille de la part du Conseil sont une condition nécessaire pour prouver la crédibilité et la fermeté de l'Union à l'égard des pays tiers;

61. 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 qu'ils 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; souligne qu'il n'adoptera des mesures de coopération en matière répressive que lorsque le Conseil aura entamé les négociations avec le Parlement et la Commission au sujet du paquet relatif à la protection des données;

62. rappelle que les notions de «prise en compte du respect de la vie privée dès la conception» et de «respect de la vie privée par défaut» participent au renforcement de la protection des données et devraient avoir le statut de norme pour tous les produits, services et systèmes proposés sur l'internet;

63. estime que l'amélioration de la transparence et des normes de sécurité pour les télécommunications et les communications en ligne est un principe nécessaire pour un meilleur régime de protection des données; demande dès lors à la Commission de présenter une proposition législative relative à des conditions générales normalisées pour les télécommunications et les communications en ligne et de charger une autorité de contrôle de vérifier le respect de ces conditions générales;

Informatique en nuage

64. 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 de services en nuage et de solutions informatiques au niveau européen 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;

65. invite tous les organismes publics dans l'Union à ne pas utiliser de services en nuage qui pourraient être soumis à une législation autre que la législation européenne;

66. 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;

67. déplore qu'un tel accès soit habituellement obtenu via 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;

68. demande à la Commission et aux États membres d'accélérer les travaux relatifs au partenariat européen de l'informatique en nuage, en associant pleinement la société civile et la communauté technique, comme l'IETF (Internet Engineering Task Force), et en intégrant les aspects liés à la protection des données;

69. invite instamment la Commission, lors de la négociation d'accords internationaux concernant le traitement de données à caractère personnel, à accorder une attention particulière aux risques et aux défis que l'informatique en nuage comporte pour les droits fondamentaux, et en particulier — sans s'y limiter toutefois — pour le droit à la vie privée et à la protection des données à caractère personnel, consacrés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne; invite en outre instamment la Commission à prendre acte des dispositions nationales des partenaires de négociation régissant l'accès des forces de l'ordre et des services de renseignement aux données à caractère personnel traitées par des services d'informatique en nuage, en particulier en exigeant que l'accès ne puisse être accordé qu'au terme d'une procédure régulière fondée sur une base juridique sans ambiguïté, et qu'à condition qu'il soit exigé de spécifier les conditions exactes d'accès, la finalité de cet accès, les mesures de sécurité mises en place lors du transfert des données, les droits des particuliers, ainsi que les règles relatives à la surveillance et à un mécanisme de recours efficace;

70. 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 et souligne qu'il importe de disposer de sanctions administratives effectives, proportionnées et dissuasives à l'encontre des fournisseurs de services d'informatique en nuage qui ne respectent pas les normes de l'Union en matière de protection des données;

71. demande à la Commission et aux autorités compétentes des États membres d'évaluer dans quelle mesure les règles européennes en matière de vie privée et de protection des données ont été enfreintes grâce à la coopération d'entités juridiques de l'Union européenne avec les services secrets ou l'acceptation de mandats délivrés par un tribunal d'un pays tiers pour demander des données à caractère personnel de citoyens de l'Union, à l'encontre de la législation européenne en matière de protection des données;

72. demande aux entreprises fournissant de nouveaux services utilisant des «données massives» et de nouvelles applications, telles que l'«internet des objets», d'intégrer dès la phase de développement des mesures de protection des données de manière à maintenir un degré élevé de confiance chez les citoyens;

Partenariat transatlantique de commerce et d'investissement (TTIP)

73. 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 la croissance économique;

74. 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 l'approbation du TTIP final par le Parlement européen pourrait être menacée tant que les activités de surveillance de masse aveugle et l'interception des communications au sein des institutions et des représentations diplomatiques de l'Union européenne n'auront pas été complètement abandonnées et qu'une solution adéquate n'aura pas été trouvée en ce qui concerne les droits des citoyens de l'Union européenne en matière de confidentialité des données, notamment un recours administratif et un recours judiciaire;

souligne que le Parlement européen ne peut approuver le TTIP final qu'à condition que l'accord respecte pleinement, entre autres, 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; souligne que la législation européenne en matière de protection des données ne saurait être vue comme une «discrimination arbitraire ou injustifiable» au sens de l'article XIV de l'AGCS;

Contrôle démocratique des services de renseignement

75. souligne que, bien que le contrôle des activités des services de renseignement doive 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;

76. 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, notamment le droit d'effectuer des visites sur place, nécessaires pour pouvoir contrôler efficacement les services de renseignement;

77. demande la création d'un groupe de députés et d'experts qui examinerait, de manière transparente et en collaboration avec les parlements nationaux, des recommandations pour améliorer le contrôle démocratique, y compris le contrôle parlementaire, des services de renseignement et pour renforcer la collaboration dans l'Union en matière de contrôle, en particulier en ce qui concerne la dimension transfrontière de cette collaboration; invite ce groupe à envisager la possibilité de 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.); y compris sur la question des organes de contrôle considérés comme un tiers au titre de la règle du «tiers service», ou sur le principe du «contrôle par l'entité d'origine», sur le contrôle et la responsabilité des services de renseignement de pays étrangers des critères de transparence renforcée, fondés sur le principe général d'accès à l'information et sur les principes dits «de Tshwane» ([1]), ainsi que les principes concernant les limites de la durée et de la portée de la surveillance, en veillant à ce qu'elles soient proportionnées et limitées à leur objectif;

78. demande à ce groupe de préparer un rapport et de collaborer à l'organisation d'une conférence à l'initiative du Parlement avec les organes de contrôle nationaux, qu'ils soient parlementaires ou indépendants, avant le début de l'année 2015;

79. 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;

80. 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);

81. invite instamment la VP/HR à rendre régulièrement compte des activités du centre d'analyse du renseignement de l'Union (IntCen), qui fait partie du Service européen pour l'action extérieure, aux organes compétents du Parlement, y compris sur son respect plein et entier des droits fondamentaux et des règles de l'Union applicables en matière de confidentialité des données, de façon à permettre au Parlement d'exercer un meilleur contrôle sur la dimension extérieure des politiques de l'Union; invite instamment la Commission et la VP/HR à présenter une proposition de base juridique pour les activités de l'IntCen, dans l'éventualité où seraient envisagées des opérations ou compétences futures en matière de dispositifs de renseignement ou de collecte de données qui lui soient propres pouvant avoir une incidence sur la stratégie de sécurité intérieure de l'Union;

([1]) «The Global Principles on National Security and the Right to Information», juin 2013.

82. invite la Commission à présenter, avant décembre 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 personnel en fonction de leur nationalité;

83. rappelle les dispositions de l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement 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

84. 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; estime qu'Europol ne devrait pas traiter les informations et les données obtenues en violation des droits fondamentaux protégés par la charte des droits fondamentaux;

85. invite Europol à se prévaloir pleinement de son mandat pour demander aux autorités compétentes des États membres à lancer des enquêtes criminelles au sujet des cyberattaques majeures et des atteintes informatiques ayant un impact transfrontalier potentiel; est convaincu que le mandat d'Europol devrait être renforcé pour lui permettre de lancer sa propre enquête à la suite d'une suspicion d'attaque malveillante sur le réseau et les systèmes informatiques de deux États membres ou organes de l'Union ou davantage ([1]); demande à la Commission de passer en revue les activités du centre européen de lutte contre la cybercriminalité (EC3) et de présenter, le cas échéant, une proposition de cadre général visant au renforcement des compétences de ce dernier;

Liberté d'expression

86. 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»;

87. prend acte de la détention de David Miranda et de la saisie du matériel en sa possession par les autorités du Royaume-Uni 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), et fait part de ses préoccupations au vu de ce que ceci constitue une potentielle grave atteinte au droit à la liberté d'expression et à la liberté des médias, reconnue par l'article 10 de la CEDH et l'article 11 de la charte de l'Union européenne, et que la législation visant à lutter contre le terrorisme pourrait faire l'objet d'abus dans de tels cas;

88. attire l'attention sur la situation difficile des lanceurs d'alerte et de leurs soutiens, y compris des journalistes, à la suite de leurs révélations; invite la Commission à examiner si une future proposition législative établissant un programme européen efficace et global de protection des lanceurs d'alerte, tel que l'a déjà demandé le Parlement dans sa résolution du 23 octobre 2013, devrait inclure également d'autres domaines de la compétence de l'Union, avec une attention toute particulière portée à la complexité du lancement d'alertes dans le domaine du renseignement; demande aux États membres d'examiner de manière approfondie la possibilité d'octroyer aux lanceurs d'alerte une protection internationale contre les poursuites;

([1]) Position du Parlement européen du 25 février 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) (Textes adoptés de cette date, P7_TA(2014)0121).

89. demande aux États membres de faire en sorte que leur législation, notamment dans le domaine de la sécurité nationale, prévoie une alternative sûre au silence pour divulguer ou signaler les actes répréhensibles, y compris la corruption, les infractions pénales, les violations d'obligations juridiques, les erreurs judiciaires et les abus d'autorité, ce qui est également conforme aux dispositions des différents instruments internationaux (Nations unies et Conseil de l'Europe) de lutte contre la corruption, aux principes établis dans la résolution de l'Assemblée parlementaire du Conseil de l'Europe 1729 (2010), les principes de Tshwane, etc.;

Sécurité informatique dans l'Union européenne

90. 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 et malveillants; 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; 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; souligne que le renforcement de la capacité et de la sécurité informatiques de l'Union atténue également la vulnérabilité de l'Union par rapport aux graves cyberattaques provenant de grandes organisations criminelles ou de groupes terroristes;

91. 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, en tant que mesure stratégique prioritaire, une capacité autonome de ressources informatiques clés; souligne que pour regagner la confiance, une telle capacité informatique européenne devrait se fonder autant que possible sur des normes ouvertes, des logiciels et, si possible, du matériel ouverts, rendant toute la chaîne d'approvisionnement transparente et contrôlable, de l'architecture de processeur jusqu'à la couche application; fait observer que pour regagner en compétitivité dans le secteur stratégique des services informatiques, il convient de mettre en place un «*new deal* numérique» accompagné d'efforts conjoints et à grande échelle dans l'Union européenne de la part des institutions, des États membres, des instituts de recherche, de l'industrie et de la société civile; 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; exhorte par conséquent la Commission à réexaminer les pratiques actuelles de passation de marchés publics eu égard au traitement des données afin d'envisager de limiter les procédures d'appels d'offres aux entreprises certifiées, et éventuellement aux entreprises de l'Union européenne, lorsque des questions de sécurité ou autres intérêts vitaux sont en jeu;

92. condamne vivement le fait que des services de renseignement cherchent à assouplir les normes de sécurité informatique et à installer des «portes dérobées» («backdoors») dans toute une série de systèmes informatiques; demande à la Commission de présenter une proposition législative visant à interdire le recours aux portes dérobées par les services répressifs; recommande en conséquence le recours aux logiciels ouverts à chaque fois que la sécurité informatique est un enjeu important;

93. invite l'ensemble des États membres, la Commission, le Conseil et le Conseil européen à soutenir sans réserve, y compris au moyen de financements dans le domaine de la recherche et du développement, le développement des capacités innovatrices et technologiques européennes en matière d'outils, de sociétés et de fournisseurs dans le secteur de l'informatique (matériel, logiciels, services et réseau), notamment aux fins de la cybersécurité et des capacités de cryptage et cryptographiques; invite toutes les institutions compétentes de l'Union et les États membres à investir dans des technologies indépendantes et locales européennes, et à développer massivement et à renforcer les capacités de détection;

94. invite la Commission, les organes de normalisation et l'ENISA à définir, avant décembre 2014, des normes et des règles minimales de sécurité et de respect de 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 et l'intégrité de tous les systèmes informatiques; estime que ces normes pourraient devenir la référence en vue de nouvelles normes mondiales et devraient 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; soutient les récentes décisions de l'IETF (Internet Engineering Task Force) visant à inclure les gouvernements dans le modèle de menace pour la sécurité de l'internet;

95. indique que les régulateurs des télécommunications européens et nationaux, et dans certains cas les sociétés de télécommunications également, 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 de bout en bout des communications;

96. 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; souligne la nécessité de renforcer la sécurité et la résilience des systèmes informatiques;

97. 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);

98. invite la Commission à affecter, dans le cadre du prochain programme de travail du programme Horizon 2020, des moyens supplémentaires 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, les meilleures solutions de sécurité possibles, y compris les solutions de sécurité ouvertes, et d'autres services de la société de l'information, et à promouvoir également le marché intérieur des logiciels et matériels européens et des moyens et infrastructures de communication cryptés, y compris en développant une stratégie industrielle globale de l'Union européenne dans le domaine de l'industrie informatique; estime que les petites et moyennes entreprises jouent un rôle particulier dans la recherche; souligne qu'aucun financement de l'Union ne devrait être accordé aux projets dont l'unique objectif est de développer des outils permettant d'accéder illégalement à des systèmes informatiques;

99. invite la Commission à établir les responsabilités actuelles et à examiner, avant décembre 2014, la nécessité d'un mandat élargi, d'une meilleure coordination et/ou de ressources et de capacités techniques supplémentaires pour l'ENISA, le centre de lutte contre la cybercriminalité d'Europol et d'autres centres de l'Union disposant d'expertises spécialisées, la CERT-EU et le CEPD afin de leur permettre de jouer un rôle essentiel dans la sécurisation des systèmes européens de communication, de prévenir et 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; invite en particulier la Commission à envisager de renforcer le rôle de l'ENISA de défense des systèmes internes au sein des institutions de l'Union et à établir au sein de la structure de l'ENISA une équipe d'intervention en cas d'urgence informatique (CERT) pour l'Union européenne et ses États membres;

100. demande à la Commission d'évaluer la nécessité d'une académie informatique européenne, qui rassemblerait les meilleurs experts européens et internationaux indépendants dans tous les domaines connexes et 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;

101. invite les services compétents du secrétariat du Parlement européen, sous la responsabilité du Président du Parlement, à effectuer, avant juin 2015, avec un rapport intermédiaire avant décembre 2014, un examen et une évaluation complets de la fiabilité du Parlement 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 Parlement; 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 de 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 s'appuyant sur les meilleures pratiques, y compris la possibilité d'une condition relative à des logiciels ouverts («open source») en tant que condition d'achat, ou de la condition pour les entreprises européennes de participer aux appels d'offres lorsque ceux-ci concernent des domaines sensibles liés à la sécurité;

— la liste des sociétés sous contrat avec le Parlement européen dans les domaines de l'informatique et des télécommunications, en prenant en considération toute information révélée au sujet de leur coopération avec des agences de renseignement (telles que 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), y compris la faisabilité que ces mêmes services soient fournis par d'autres entreprises, de préférence européennes;

— la fiabilité et la résilience des logiciels, et en particulier des logiciels commerciaux prêts à l'emploi, utilisés par les institutions de l'Union dans leurs systèmes informatiques en ce qui concerne les pénétrations et les intrusions par les autorités policières et de renseignement européennes et non européennes, compte tenu également des normes internationales applicables, des principes de gestion des risques pour la sécurité conformément aux meilleures pratiques et du respect des normes de sécurité des informations des réseaux de l'Union européenne en matière de violations de la sécurité;

— le recours accru aux systèmes ouverts;

— les démarches et mesures à prendre pour faire face au recours accru aux outils mobiles (comme les smartphones, les tablettes, qu'ils soient professionnels ou personnels) et à ses conséquences sur la sécurité informatique du système;

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

— l'utilisation et l'emplacement des serveurs et des centres informatiques pour les systèmes informatiques du Parlement 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 de services d'informatique et de stockage en nuage par le Parlement, y compris la nature des données stockées en nuage, la manière dont le contenu et l'accès à celui-ci sont protégés et le lieu où les serveurs de nuages sont situés, en précisant le régime juridique applicable en matière de protection des données et de renseignement, ainsi qu'en évaluant les possibilités d'utiliser uniquement les serveurs de nuages basés sur le territoire de l'Union;

— un plan permettant l'utilisation de technologies cryptographiques supplémentaires, notamment le cryptage authentifié de bout en bout pour l'ensemble des services informatiques 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;

— un plan pour l'utilisation d'une norme de cryptage par défaut pour les courriers électroniques, comme le GNU Privacy Guard, 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, permettant une communication sécurisée, où le serveur ne verrait que du contenu crypté;

102. invite les institutions et les agences de l'Union européenne à réaliser une démarche similaire en coopération avec l'ENISA, Europol et les CERT, avant juin 2015, avec un rapport intermédiaire 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;

103. 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;

104. 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 tels qu'un ESTA de l'Union, doivent être développés et exploités de sorte à éviter que les données ne soient compromises à la suite des demandes émises par des autorités de pays tiers; invite l'eu-LISA à rendre compte au Parlement de la fiabilité des systèmes en place avant fin 2014;

105. 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, 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, tout en évitant de faciliter le contrôle ou la censure par l'État ou la «balkanisation» et la fragmentation de l'internet;

106. demande à l'Union européenne de se poser en chef de file pour façonner l'architecture et la gouvernance de l'internet afin de parer aux risques liés aux flux de données et à leur stockage, en privilégiant le renforcement de la minimisation des données et de la transparence et la réduction du stockage de masse centralisé de données brutes, et pour le réacheminement du trafic internet ou le cryptage complet de bout en bout de l'ensemble du trafic internet afin de parer aux risques actuels liés à 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;

107. invite à promouvoir:

— les moteurs de recherche et les réseaux sociaux de l'Union, un pas important vers l'indépendance informatique de l'Union;

— les fournisseurs de services informatiques européens;

— le cryptage des communications en général, y compris les courriels et les SMS;

— l'élaboration au niveau européen d'éléments informatiques cruciaux, par exemple les solutions pour système d'exploitation client-serveur, en utilisant les normes ouvertes et en développant des éléments européens pour le couplage de réseaux, par exemple des routeurs;

108. invite la Commission à présenter une proposition législative de système d'acheminement de l'Union, permettant notamment le traitement au niveau de l'Union des statistiques d'appel, ayant vocation à constituer une sous-structure de l'internet existant et à ne pas s'étendre au-delà des frontières de l'Union européenne; relève que toutes les données d'acheminement et statistiques d'appel devraient être traitées conformément aux cadres juridiques de l'Union;

109. 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 développer une culture de la sécurité et 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 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»;

110. invite la Commission à présenter, avant décembre 2014, des propositions législatives pour encourager les fabricants de logiciels et de matériel à renforcer la sécurité et la vie privée au moyen de fonctions dès la conception et par défaut dans leurs produits, y compris en proposant des mesures pour décourager la collecte excessive et disproportionnée de données à caractère personnel en masse et en introduisant une responsabilité légale pour les fabricants pour les vulnérabilités connues non corrigées, les produits défectueux ou non sûrs, ou l'installation de portes dérobées secrètes permettant d'accéder sans autorisation aux données et de les traiter; à cet égard, demande à la Commission d'évaluer la possibilité de mettre en place un système de certification ou de validation pour le matériel informatique, y compris des procédures de test au niveau de l'Union européenne pour garantir l'intégrité et la sécurité des produits;

Rétablissement de la confiance

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

Mercredi 12 mars 2014

112. 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 des droits fondamentaux, de la démocratie et de l'état de droit, ainsi qu'à la crédibilité des garanties et du contrôle démocratiques, judiciaires et parlementaires, dans une société numérique;

Entre l'Union européenne et les États-Unis

113. 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;

114. estime que les activités de surveillance de masse des citoyens et d'espionnage des dirigeants politiques menées par les 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;

115. 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 sur une nouvelle base de confiance s'appuyant sur un véritable respect commun de l'état de droit et le rejet de toutes les pratiques de surveillance de masse systématique; affirme par conséquent 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;

116. est disposé à engager le 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, le droit à la vie privée et autres droits des citoyens et des résidents de l'Union et des autres personnes protégées par le droit de l'Union, ainsi que les droits à l'information et au respect de la vie privée équivalents dans les tribunaux des États-Unis soient garantis au moyen, par exemple, d'une révision du *Privacy Act* et de l'*Electronic Communications Privacy Act* et de la ratification du premier protocole additionnel du Pacte international relatif aux droits civils et politiques (PIDCP), de façon à mettre un terme à la discrimination actuelle;

117. 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 proportionné et limité à des situations bien définies et lié à des soupçons raisonnables ou à une cause probable d'activité terroriste; souligne que ces activités doivent, dans ce cas, faire l'objet d'un contrôle judiciaire transparent;

118. 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;

119. 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;

120. 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;

121. 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

122. estime également que la participation et les activités des États membres de l'Union européenne ont produit une perte de confiance, y compris entre États membres ainsi qu'entre les citoyens et leurs autorités nationales; 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, y compris l'arrêt des activités de surveillance de masse et le renforcement du système de contrôle judiciaire et parlementaire, pourront rétablir la confiance perdue; rappelle les difficultés que présente l'élaboration de politiques globales de sécurité de l'Union lorsque de telles activités de surveillance de masse sont pratiquées, et souligne que le principe européen de sincère coopération requiert que les États membres s'abstiennent de mener des activités de renseignement sur le territoire d'autres États membres;

123. observe 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 et le cadre législatif de l'Union dans son ensemble; juge ces accords bilatéraux contreproductifs et inappropriés, étant donnée la nécessité d'une approche européenne de ce problème; demande au Conseil d'informer le Parlement de l'évolution des discussions menées par les États membres au sujet d'un accord mutuel de non-espionnage pour toute l'Union;

124. estime que ces accords ne doivent pas violer les traités de l'Union, 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; décide de réexaminer tous accords de ce type eu égard à leur compatibilité avec le droit européen et 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 les principes fondamentaux de l'Union sur lesquels elle s'appuie;

125. demande aux États membres de consentir tous les efforts possibles pour favoriser une meilleure coopération afin de fournir des garanties contre l'espionnage, en coopération avec les organes et agences pertinents de l'Union européenne, en vue de la protection des citoyens et des institutions de l'Union, des entreprises européennes, de l'industrie de l'Union, des infrastructures et réseaux informatiques, ainsi que de la recherche européenne; considère que la participation active des parties concernées européennes est une condition *sine qua non* d'un bon échange d'informations; souligne que les menaces de sécurité sont devenues davantage internationales, diffuses et complexes, et qu'elles requièrent une coopération européenne renforcée; est convaincu que cette évolution devrait mieux se refléter dans les traités, et demande dès lors une révision des traités pour renforcer la notion de coopération loyale entre les États membres et l'Union en ce qui concerne l'objectif de création d'un espace de sécurité, et de prévenir l'espionnage mutuel entre États membres au sein de l'Union;

126. estime que des structures de communication non piratables (courrier électronique et télécommunications, y compris lignes terrestres et téléphones portables) et des salles de réunion ne pouvant être placées sur écoute sont absolument nécessaires dans toutes les institutions et délégations de l'Union européenne; demande par conséquent la mise en place d'un système de courrier électronique interne crypté;

127. invite le Conseil et la Commission à approuver sans délai la proposition, adoptée par le Parlement européen le 23 mai 2012, de règlement du Parlement européen relatif aux modalités d'exercice du droit d'enquête du Parlement européen et abrogeant la décision 95/167/CE, Euratom, CECA du Parlement européen, du Conseil et de la Commission, présentée sur la base de l'article 226 du traité FUE; demande une révision du traité pour étendre ces pouvoirs d'enquête afin de couvrir, sans restrictions ni exceptions, tous les domaines de compétence ou d'activité de l'Union et d'inclure la possibilité d'interroger sous serment;

Sur le plan international

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

129. 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 no 16 de la commission des droits de l'homme 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»; invite les États membres à prévoir dans cet exercice de plaider en faveur de l'attribution, à une agence internationale des Nations unies, d'un mandat consistant en particulier à surveiller l'apparition d'instruments de surveillance et à réglementer et examiner les utilisations qui en sont faites; demande à la haute représentante/vice-présidente de la Commission et au Service européen pour l'action extérieure d'adopter des mesures proactives;

130. 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, et à œuvrer davantage pour la défense du droit fondamental à la vie privée et à la protection des données au niveau international tout en évitant de faciliter le contrôle ou la censure par l'État ou la fragmentation de l'internet, notamment au moyen d'une initiative en faveur d'un traité international interdisant les activités de surveillance de masse et via la création d'une agence pour en assurer le contrôle;

Plan prioritaire: un habeas corpus numérique européen — protéger les droits fondamentaux à l'ère numérique

131. 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; invite la Commission et les autres institutions, organes, bureaux et agences de l'Union visés dans la présente résolution, conformément à l'article 265 du traité FUE, à agir selon les recommandations et demandes formulées dans la présente résolution;

132. décide de lancer un habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique fondé sur les huit actions suivantes, dont il surveillera la mise en œuvre:

— 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 garantissant le droit fondamental des citoyens au respect de la vie privée et à la protection des données et assurant des mécanismes de recours adéquats aux citoyens européens, y compris 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 2013;

— Action 5: évaluer tout accord, mécanisme ou échange avec les pays tiers concernant des données à caractère personnel pour s'assurer que le droit au respect de la vie privée et à la protection des données à caractère personnel n'est pas violé en raison des activités de surveillance et prendre les mesures adéquates nécessaires;

— Action 6: protéger l'état de droit et les droits fondamentaux des citoyens de l'Union (y compris contre les menaces qui pèsent sur la liberté de la presse), le droit de la population à recevoir des informations impartiales et la confidentialité professionnelle (y compris dans les relations entre l'avocat et son client), et renforcer la protection des lanceurs d'alerte;

— Action 7: développer une stratégie européenne en vue d'une plus grande indépendance informatique (un «*new deal* numérique», comprenant l'affectation de ressources adéquates au niveau national et de l'Union) pour dynamiser l'industrie informatique et permettre aux entreprises européennes d'exploiter l'avantage compétitif de l'Union en termes de protection de la vie privée;

— Action 8: faire de l'Union européenne un exemple en matière de gouvernance démocratique et neutre de l'internet;

133. invite les institutions et les États membres de l'Union à promouvoir l'habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique; s'engage à se faire le défenseur du respect des droits des citoyens de l'Union, en s'appuyant sur le calendrier ci-après pour suivre la mise en œuvre:

— avril 2014 — mars 2015: un groupe de contrôle basé sur la commission d'enquête LIBE responsable de la surveillance de nouvelles révélations éventuelles 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 demande formelle au Conseil européen d'intégrer l'habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique 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 protégeant les droits fondamentaux à l'ère numérique et les recommandations connexes serviront de critères déterminants pour l'approbation de la prochaine Commission;

— 2014: 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;

— 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;

o

o o

134. 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;

135. charge sa commission des libertés civiles, de la justice et des affaires intérieures à s'adresser au Parlement en plénière sur le sujet un an après l'adoption de la présente résolution; considère qu'il est essentiel d'évaluer la mesure dans laquelle les recommandations adoptées par le Parlement ont été suivies et d'analyser tous les cas où de telles recommandations n'ont pas été suivies.