Parlement européen
2014-2019

Document de séance

B8-0305/2018

26.6.2018

PROPOSITION DE RÉSOLUTION

déposée à la suite d'une déclaration de la Commission

conformément à l'article 123, paragraphe 2, du règlement intérieur

sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis
(2018/2645(RSP))

Claude Moraes
au nom de la commission des libertés civiles, de la justice et des affaires intérieures

B8-0305/2018

Résolution du Parlement européen sur l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis
(2018/2645(RSP))

Le Parlement européen,

– vu le traité sur l'Union européenne (traité UE), le traité sur le fonctionnement de l'Union européenne (traité FUE) et les articles 6, 7, 8, 11, 16, 47 et 52 de la charte des droits fondamentaux de l'Union européenne,

– vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1] et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[2],

– vu l'arrêt rendu par la Cour de justice de l'Union européenne le 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems contre Data Protection Commissioner*[3],

– vu l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 dans les affaires C-203/15 – *Tele2 Sverige AB contre Post- och telestyrelsen* et C-698/15 – *Secretary of State for the Home Department contre Tom Watson e.a.*[4],

– vu la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis[5],

– vu l'avis 4/2016 du Contrôleur européen de la protection des données (CEPD) sur le projet de décision d'adéquation relative au bouclier de protection des données UE-États-Unis[6],

– vu l'avis 01/2016 du groupe de travail «article 29» sur la protection des données du 13 avril 2016 sur le projet de décision d'adéquation relative au bouclier de protection

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 119 du 4.5.2016, p. 89.
[3] UE:C:2015:650.
[4] UE:C:2016:970.
[5] JO L 207 du 1.8.2016, p.1.
[6] JO C 257 du 15.7.2016, p.8.

des données UE-États-Unis[1] et sa déclaration du 26 juillet 2016[2],

– vu le rapport de la Commission au Parlement européen et au Conseil sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis[3] et le document de travail des services de la Commission accompagnant le document[4],

– vu le document du groupe de travail «article 29» sur la protection des données (ci-après, «le groupe de travail «article 29»») du 28 novembre 2017 intitulé «EU-US Privacy Shield – First Annual Joint Review»[5],

– vu la lettre de réaction du groupe de travail «article 29» du 11 avril 2018 à la réautorisation de la section 702 du Foreign Intelligence Surveillance Act (FISA) américain,

– vu sa résolution du 6 avril 2017 sur l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis[6];

– vu l'article 123, paragraphe 2, de son règlement intérieur,

A. considérant que la Cour de justice de l'Union européenne, dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems contre Data Protection Commissioner*, a invalidé la décision concernant la sphère de sécurité et a précisé qu'un niveau de protection adéquat dans un pays tiers s'entend comme «substantiellement équivalent» à la protection garantie dans l'Union en vertu de la directive 95/46 lue à la lumière de la charte, et qu'il est donc urgent de conclure les négociations relatives à un nouveau dispositif afin de garantir la sécurité juridique sur les modalités de transfert des données à caractère personnel de l'Union vers les États-Unis;

B. considérant que, lors de l'examen du niveau de protection offert par un pays tiers, la Commission est tenue d'apprécier le contenu des règles applicables dans ce pays résultant de la législation interne ou des engagements internationaux de celui-ci, ainsi que la pratique visant à assurer le respect de ces règles, dès lors qu'elle doit, conformément à l'article 25, paragraphe 2, de la directive 95/46/CE, prendre en compte toutes les circonstances relatives à un transfert de données à caractère personnel vers un pays tiers; que cet examen ne doit pas seulement se rapporter à la législation et aux pratiques relatives à la protection des données à caractère personnel à des fins commerciales et privées, mais doit également couvrir tous les aspects du cadre applicable à ce pays ou secteur, à savoir, en particulier, mais pas uniquement, la répression, la sécurité nationale et le respect des droits fondamentaux;

C. considérant que les transferts de données à caractère personnel entre les organisations commerciales de l'UE et des États-Unis constituent un élément important des relations transatlantiques, au vu de la numérisation toujours croissante de l'économie mondiale;

[1] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
[2] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf
[3] COM(2017)0611 du 18.10.2017.
[4] SWD(2017)0344 du 18.10.2017.
[5] WP 255, disponible à l'adresse http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621
[6] Textes adoptés de cette date, P8_TA(2017)0131.

que ces transferts devraient être menés dans le strict respect du droit à la protection des données à caractère personnel et du droit au respect de la vie privée; que l'un des objectifs fondamentaux de l'Union est la protection des droits fondamentaux consacrés dans la charte;

D. considérant que Facebook, signataire du bouclier de protection des données, a confirmé que les données de 2,7 millions de citoyens de l'UE figuraient parmi les données utilisées de manière abusive par le consultant politique Cambridge Analytica;

E. considérant que le CEPD a formulé plusieurs inquiétudes sur le projet de bouclier de protection des données dans son avis 4/2016; que dans ce même avis, le CEPD salue les efforts déployés par toutes les parties pour apporter une solution aux problèmes relatifs aux transferts de données à caractère personnel à des fins commerciales de l'Union vers les États-Unis dans le cadre d'un système d'autocertification;

F. considérant que, dans son avis 01/2016 sur le projet de décision d'adéquation du bouclier de protection des données UE-États-Unis, le groupe de travail «article 29» s'est félicité des améliorations apportées par le bouclier de protection des données par rapport à la décision relative à la sphère de sécurité, tout en faisant part de vives inquiétudes concernant à la fois les aspects commerciaux et l'accès des autorités publiques aux données transférées au titre du bouclier de protection des données;

G. considérant que, le 12 juillet 2016, à la suite de nouvelles discussions avec l'administration américaine, la Commission a adopté sa décision d'exécution (UE) 2016/1250, constatant le niveau adéquat de protection des données à caractère personnel transférées de l'Union à des organisations aux États-Unis au titre du bouclier de protection des données UE-États-Unis;

H. considérant que le bouclier de protection des données UE-États-Unis est assorti de plusieurs engagements et assurances unilatéraux de la part de l'administration américaine, explicitant, entre autres, les principes de la protection des données, le fonctionnement de la surveillance, de la mise en application de la loi et des voies de recours, et les protections et garanties en vertu desquelles les agences de sécurité peuvent avoir accès aux données à caractère personnel et traiter ces dernières;

I. considérant que, dans sa déclaration du 26 juillet 2016, le groupe de travail «article 29» salue les améliorations apportées par le mécanisme du bouclier de protection des données UE-États-Unis par comparaison avec la décision relative à la sphère de sécurité, et félicite la Commission et les autorités américaines d'avoir tenu compte de ses inquiétudes; que le groupe de travail «article 29» fait néanmoins état d'un certain nombre d'inquiétudes concernant à la fois les aspects commerciaux et l'accès des autorités publiques américaines aux données transférées depuis l'Union, comme l'absence de règles spécifiques sur les décisions automatisées et d'un droit général de s'opposer, le besoin de garanties plus strictes sur l'indépendance et les pouvoirs du médiateur, ou le manque d'assurances concrètes sur l'absence de collecte massive et indifférenciée des données à caractère personnel (collecte de masse);

J. considérant que, dans sa résolution du 6 avril 2017, le Parlement européen, tout en reconnaissant que le bouclier de protection des données UE-États-Unis comporte des améliorations notables en termes de clarté des normes par rapport à l'ancien régime de

la sphère de sécurité entre l'Union et les États-Unis, estime également que d'importantes questions demeurent en ce qui concerne certains aspects commerciaux, la sécurité nationale et la répression; qu'il demande à la Commission de réaliser, lors du premier examen annuel conjoint, un examen complet et approfondi de tous les défauts et faiblesses et de montrer comment ils ont été traités afin d'assurer l'application de la charte de l'UE et de la législation de l'Union, et d'évaluer attentivement l'efficacité et la faisabilité des mécanismes et garanties mentionnés dans les assurances et clarifications de l'administration américaine;

K. considérant que le rapport de la Commission au Parlement européen et au Conseil sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis et le document de travail des services de la Commission accompagnant ce document, tout en reconnaissant que les autorités américaines ont mis en place les structures et procédures nécessaires pour assurer le bon fonctionnement du bouclier de protection des données et en concluant que les États-Unis continuent de garantir un niveau suffisant de protection des données à caractère personnel transférées au titre du bouclier, ont formulé dix recommandations aux autorités américaines afin d'aborder des questions qui ne concernent pas seulement les missions et activités du ministère américain du commerce (DoC) en tant qu'administrateur responsable du suivi de la certification des organisations au titre du bouclier de protection des données et de l'application effective des principes, mais également les questions de sécurité nationale telles que la réautorisation de la section 702 du Foreign Intelligence Surveillance Act (FISA), ou la nomination d'un médiateur permanent, et le fait que les membres du Privacy Civil Liberties Oversight Board (PCLOB) ne sont toujours pas en fonction;

L. considérant que l'avis du groupe de travail «article 29» du 28 novembre 2017 intitulé «EU-US Privacy Shield – First Annual Joint Review», rendu dans la foulée du premier examen annuel conjoint, prend acte des progrès du bouclier de protection des données par rapport à la décision, invalidée, relative à la sphère de sécurité; que le groupe de travail «article 29» prend acte des efforts consentis par les autorités américaines et la Commission afin de mettre en œuvre le bouclier de protection des données;

M. considérant que le groupe de travail «article 29» a recensé un certain nombre de questions en suspens, importantes et très préoccupantes, concernant à la fois le commerce et l'accès des autorités publiques américaines aux données transférées aux États-Unis au titre du bouclier de protection des données (que ce soit à des fins de répression ou de sécurité nationale), qui doivent être abordées aussi bien par la Commission que par les autorités américaines; qu'il a demandé la mise en place immédiate d'un plan d'action pour démontrer que toutes ces questions seront abordées, au plus tard lors du deuxième examen conjoint;

N. considérant que, si aucune réponse n'est apportée aux inquiétudes du groupe de travail «article 29» dans les délais impartis, les membres de ce groupe prendront des mesures appropriées, y compris en portant la décision relative à l'adéquation du bouclier de protection des données devant les juridictions nationales afin qu'elles saisissent la Cour de justice de l'Union européenne d'une demande de décision préjudicielle;

O. considérant qu'un recours en annulation (affaire T-738/16 *La Quadrature du Net et autres contre Commission*) et une saisine de la Haute cour d'Irlande dans l'affaire

opposant le commissaire à la protection des données d'Irlande et Facebook Ireland Limited et Maximilian Schrems (affaire *Schrems II*) ont été portés devant la Cour de justice européenne; que la saisine constate que la surveillance de masse perdure et examine si une solution effective se trouve dans la loi américaine pour les citoyens européens dont les données à caractère personnel sont transférées au États-Unis;

P. considérant que le 11 janvier 2018, le Congrès américain a modifié et réautorisé pour six ans la section 702 du FISA sans répondre aux préoccupations que la Commission exprime dans son rapport d'examen conjoint et de l'avis du groupe de travail «article 29» ;

Q. considérant que, dans le cadre de la législation budgétaire générale promulguée le 23 mars 2018, le Congrès américain a promulgué le «Clarifying Overseas Use of Data ('CLOUD') Act», qui facilite l'accès à des fins répressives au contenu des communications et autres données liées en permettant aux autorités répressives des États-Unis d'imposer la production de données de communication même si elles sont stockées en dehors des États-Unis, et en permettant à certains pays étrangers de conclure des accords exécutifs avec les États-Unis de manière à permettre aux fournisseurs de services américains de répondre à certaines décisions de justice étrangères réclamant un accès à des données de communication;

R. considérant que Facebook Inc., Cambridge Analytica and SCL Elections Ltd sont des entreprises certifiées dans le cadre du bouclier de protection des données et qu'en tant que telles, elles ont bénéficié de la décision d'adéquation comme base juridique pour le transfert, en vue du traitement ultérieur, de données à caractère personnel de l'Union européenne vers les États-Unis;

S. considérant qu'en vertu de l'article 45, paragraphe 5, du règlement général sur la protection des données, lorsque les informations disponibles révèlent qu'un pays tiers n'assure plus un niveau de protection adéquat, la Commission abroge, modifie ou suspend sa décision d'adéquation;

1. insiste sur les faiblesses persistantes du bouclier de protection des données en ce qui concerne le respect des droits fondamentaux des personnes concernées; souligne le risque croissant que la Cour de justice de l'Union européenne puisse invalider la décision d'exécution (UE) 2016/1250 de la Commission sur le bouclier de protection des données;

2. prend acte des améliorations par rapport à l'accord concernant la sphère de sécurité, avec l'insertion de définitions clés, des obligations plus strictes en matière de conservation des données et de transferts ultérieurs vers des pays tiers, la création d'un médiateur pour garantir des recours individuels et un contrôle indépendant, des garde-fous garantissant les droits des personnes concernées (PCLOB), des contrôles de conformité externes et internes, une documentation et un suivi plus réguliers et rigoureux, la disponibilité de plusieurs voies de recours juridiques et le rôle proéminent des APD nationales dans l'examen des plaintes;

3. rappelle que le groupe de travail «article 29» a fixé le délai du 25 mai 2018 pour résoudre les questions en suspens, faute de quoi il pourrait décider de porter la question du bouclier de protection des données devant les juridictions nationales afin qu'elles

saisissent la Cour de justice de l'Union européenne d'une demande de décision préjudicielle[1];

Aspects institutionnels / Nominations

4. regrette qu'il ait fallu tant de temps pour désigner les deux membres supplémentaires qu'implique la nomination du président du PCLOB et demande instamment au Sénat d'examiner leurs profils afin de ratifier leur désignation de manière à rétablir le quorum de l'agence indépendante et lui permettre de remplir ses missions de prévention du terrorisme et de protection de la vie privée et des libertés civiles;

5. est préoccupé par le fait que l'absence d'un président et d'un quorum ait limité la capacité du PCLOB à agir et à remplir ses obligations; souligne que, tant que le quorum n'est pas atteint, le PCLOB ne peut lancer de nouveaux projets de conseil ou de contrôle ni engager du personnel; rappelle que le PCLOB n'a toujours pas publié son rapport tant attendu sur la conduite des opérations de surveillance prévues par le décret présidentiel 12333 ni fourni des informations sur les modalités concrètes de fonctionnement dudit décret, pas plus que sur la nécessité du décret d'intervenir dans la protection des données ou sur le caractère proportionné d'une telle ingérence; note que ce rapport est hautement souhaitable compte tenu de l'incertitude et de l'imprévisibilité entourant la mise en œuvre du décret présidentiel 12333; regrette que le PCLOB n'ait pas publié un nouveau rapport sur la section 702 du FISA avant sa réactivation en janvier 2018; considère que l'absence de quorum compromet sérieusement les garanties et les assurances de conformité et de surveillance données par les autorités américaines; invite donc instamment les autorités américaines à nommer sans délai les nouveaux membres du conseil d'administration et à les confirmer dans leurs fonctions;

6. sachant que la directive présidentielle 28 (DPP 28) est l'un des éléments centraux sur lesquels repose le bouclier de protection des données, demande la publication du rapport du PCLOB sur la DPP 28, qui continue d'être assujetti au privilège de l'exécutif et qui, partant, n'est toujours pas paru;

7. rappelle sa position, selon laquelle le mécanisme du médiateur mis en place par le département d'État américain n'est pas suffisamment indépendant et n'est pas doté de pouvoirs effectifs suffisants pour mener à bien ses missions et offrir aux ressortissants de l'Union des voies de recours efficaces; souligne que les pouvoirs exacts du mécanisme du médiateur doivent être clarifiés, notamment en ce qui concerne ses pouvoirs vis-à-vis de la communauté du renseignement et l'efficacité réelle des recours contre ses décisions; regrette que le médiateur ne puisse que demander certaines mesures ou des informations aux organes gouvernementaux américains et qu'il ne puisse pas ordonner aux autorités de cesser ou de mettre fin à la surveillance illégale ou à la destruction définitive d'informations; souligne que, bien qu'il existe un médiateur faisant fonction, l'administration américaine n'a toujours pas nommé à ce jour un nouveau médiateur à titre permanent, ce qui ne favorise pas la confiance mutuelle; estime qu'en l'absence de nomination d'un médiateur indépendant, expérimenté et doté de pouvoirs suffisants, les assurances des États-Unis selon lesquelles les citoyens de l'UE se voient proposer des voies de recours efficaces n'ont aucun sens;

[1] https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

8. prend acte de la récente confirmation par le Sénat d'un nouveau président de la FTC et de quatre commissaires; déplore que, jusqu'à cette confirmation, quatre des cinq sièges de la FTC sont restés vacants, alors que la FTC est l'agence chargée de faire respecter les principes du bouclier de protection des données par la contrepartie américaine;

9. souligne que les récentes révélations concernant les pratiques de Facebook et de Cambridge Analytica mettent en exergue la nécessité d'une surveillance en amont ainsi que de mesures d'exécution qui ne se fondent pas exclusivement sur des plaintes et qui prévoient des contrôles systématiques de la conformité pratique des politiques de protection de la vie privée avec les principes du bouclier de protection des données tout au long de la durée de vie de la certification; invite les autorités compétentes de l'Union en matière de protection des données à prendre des mesures appropriées et à suspendre les transferts en cas d'absence de conformité;

Aspects commerciaux

10. estime que, afin d'assurer la transparence et d'éviter les fausses déclarations de certification, le ministère du commerce ne devrait pas tolérer que les entreprises américaines fassent des déclarations publiques sur leur certification avant d'avoir finalisé le processus de certification et de les avoir inscrites sur la liste des entités du bouclier de protection des données; est préoccupé par le fait que le ministère du commerce n'ait pas fait usage de la possibilité prévue dans le bouclier de protection des données de demander une copie des clauses contractuelles utilisées par les entreprises certifiées dans leurs contrats avec des tiers pour vérifier le respect de la conformité; considère dans ces conditions qu'il n'existe pas de contrôle efficace permettant de savoir si les entreprises certifiées respectent effectivement les obligations prévues par le bouclier de protection des données; invite le ministère du commerce à entreprendre de manière proactive et régulière des examens automatiques de conformité afin de vérifier le respect effectif des règles et des exigences du bouclier de protection des données par les entreprises;

11. estime que les différentes procédures de recours offertes aux citoyens de l'Union européenne peuvent s'avérer trop complexes, difficiles à utiliser et, partant, moins efficaces; note que, comme le soulignent les entreprises qui proposent des mécanismes de recours indépendants (IRM), la plupart des plaintes sont déposées directement auprès des entreprises par des personnes cherchant des informations générales sur le bouclier des données et le traitement de leurs données; plaide donc pour que les autorités américaines donnent, sur le site Internet du bouclier de protection des données, des informations plus concrètes sur les divers droits et les voies de recours existantes, et ce sous une forme accessible et facilement compréhensible;

12. invite, eu égard aux récentes révélations d'utilisation abusive de données à caractère personnel par des entreprises certifiées participant au bouclier de protection des données, notamment Facebook et Cambridge Analytica, les autorités américaines chargées de faire respecter le bouclier de protection des données à réagir à ces révélations sans délai et dans le plein respect des assurances et engagements donnés pour maintenir dans sa forme actuelle le bouclier de protection des données et, le cas échéant, à retirer ces entreprises de la liste du bouclier de protection des données; demande également aux autorités de l'Union européenne en charge de la protection des

données à enquêter sur ces révélations et, le cas échéant, à suspendre ou à interdire les transferts de données au titre du bouclier de protection des données; estime que ces révélations montrent clairement que le mécanisme du bouclier de protection des données n'assure pas une protection appropriée du droit à la protection des données;

13. est vivement préoccupé par les conséquences de la révision des conditions d'utilisation de Facebook pour les utilisateurs de pays tiers résidant hors des États-Unis et du Canada, qui ont jusqu'à présent bénéficié des droits octroyés par la législation européenne sur la protection des données, et qui doivent désormais accepter que le responsable du traitement des données ne soit plus Facebook Irlande mais Facebook États-Unis; considère que cette pratique constitue un transfert de données à caractère personnel d'environ 1,5 milliard d'utilisateurs vers un pays tiers; doute sérieusement qu'une telle limitation à grande échelle et sans précédent des droits fondamentaux des utilisateurs d'une plate-forme, de fait monopolistique, corresponde au but recherché par le bouclier de protection des données; invite les autorités de protection des données de l'UE à enquêter sur cette question;

14. se déclare vivement préoccupé par le fait que, si elles ne sont pas traitées, de telles utilisations abusives des données à caractère personnel par diverses entités cherchant à manipuler l'opinion publique ou à influencer son vote peuvent menacer le processus démocratique et la conviction implicite que les électeurs sont à même de prendre des décisions éclairées fondées sur des éléments factuels;

15. accueille favorablement et soutient les appels lancés au législateur américain pour qu'il s'oriente vers une loi omnibus sur la protection de la vie privée et des données;

16. rappelle ses préoccupations quant à l'absence de règles et de garanties spécifiques, dans le bouclier de protection des données, concernant les décisions fondées sur le traitement automatisé ou le profilage, qui produisent des effets juridiques ou affectent de manière significative l'individu; prend acte de l'intention de la Commission de commander une étude visant à recueillir des preuves factuelles et à mieux évaluer, dans le cadre du bouclier de protection des données, la pertinence du processus décisionnel automatisé qui s'applique au transfert de données; invite la Commission à prévoir des règles spécifiques concernant le processus décisionnel automatisé afin de proposer des garanties suffisantes si l'étude le recommande; relève à cet égard les informations contenues dans le réexamen conjoint, selon lesquelles la prise de décision automatisée ne peut s'effectuer sur la base de données à caractère personnel, transférées dans le cadre du bouclier de protection des données; déplore, comme le constate en substance le groupe de travail «article 29», que les réactions des entreprises sont restées très générales, sans préciser si ces affirmations correspondent à la réalité de toutes les entreprises qui adhèrent au bouclier de protection des données; souligne en outre qu'aux termes de son article 3, paragraphe 2, le RGPD s'applique;

17. souligne que des améliorations supplémentaires devraient être apportées en ce qui concerne l'interprétation et le traitement des données liées aux ressources humaines en raison de l'interprétation différente de la notion de «données liées aux ressources humaines » par le gouvernement américain, d'une part, et par la Commission et le groupe de travail «article 29», d'autre part; approuve pleinement l'appel lancé par le groupe de travail «article 29» à la Commission en vue d'engager des négociations avec

les autorités américaines dans l'optique de modifier le mécanisme de protection des données sur ce point;

18. se dit une nouvelle fois préoccupé par le fait que les principes du bouclier de protection des données ne sont pas conformes au modèle européen de traitement fondé sur le consentement dans la mesure où ils ne permettent un droit d'opposition (clause d'exemption) que dans des situations bien précises; invite donc instamment le ministère du commerce, à la lumière du réexamen conjoint, à coopérer avec les autorités européennes de protection des données afin de préciser les notions essentielles du bouclier de protection des données que sont notamment le principe du choix, le principe de la communication, les transferts ultérieurs, la relation entre le responsable du traitement et le sous-traitant et, enfin, l'accès, qui sont beaucoup plus en phase avec les droits de la personne concernée au sens du règlement (UE) 2016/679;

19. réitère ses préoccupations concernant le rejet par le Congrès, en mars 2017, du texte proposé par la commission fédérale des communications relatif à la «protection de la vie privée des clients des services à haut débit et autres services de télécommunications», ce qui en pratique supprime, dans le domaine du haut débit, les règles de protection de la vie privée qui auraient obligé les fournisseurs de services Internet à obtenir le consentement explicite des consommateurs avant de vendre ou de partager des données de navigation Web et d'autres informations privées avec les annonceurs et diverses autres entreprises; considère qu'il s'agit là d'une nouvelle menace pour la protection de la vie privée aux États-Unis;

Application de la loi et sécurité nationale

20. estime que la définition de l'expression «sécurité nationale» dans le mécanisme du bouclier de protection des données n'est pas suffisamment circonscrite pour s'assurer que les violations de la protection des données peuvent être effectivement examinées par les tribunaux sur la base d'un contrôle strict de ce qui est nécessaire et proportionné; demande par conséquent une définition claire de la «sécurité nationale».

21. prend note que le nombre d'objectifs visés par l'article 702 de la FISA a augmenté en raison de l'évolution tant des techniques et des modes de communication que des nouvelles formes de menace;

22. regrette que les États-Unis n'aient pas saisi l'occasion de la récente réactivation de la section 702 de la FISA pour inclure les garanties prévues dans la PPD 28; demande des preuves et des engagements juridiquement contraignants garantissant que la collecte de données fondée sur la section 702 de la FISA ne se fasse pas sans discernement et que l'accès ne soit pas généralisé (collecte en vrac), sous peine de méconnaître la charte des droits fondamentaux de l'UE; prend note de l'explication apportée par la Commission dans le document de travail de ses services, selon laquelle la surveillance fondée sur la section 702 de la FISA se base toujours sur des mots-clés (sélecteurs) et ne permet donc pas la collecte en vrac; se joint donc à la demande du groupe de travail «article 29» qui souhaite un rapport actualisé du PCLOB sur la définition des «cibles», sur le «choix des mots-clés» et sur le processus concret d'utilisation des mots-clés dans le cadre du programme UPSTREAM afin de clarifier et d'évaluer s'il y a, dans ce contexte, un accès en vrac aux données à caractère personnel; déplore que les citoyens de l'UE soient exclus de la protection supplémentaire que permet la réactivation de la section 702 de la

FISA; regrette, comme l'a déjà fait observer le groupe de travail «article 29», que la réactivation de la section 702 contienne plusieurs modifications qui ne sont que d'ordre procédural et qui ne s'attaquent pas aux aspects les plus problématiques; invite la Commission à prendre au sérieux l'analyse à venir du groupe de travail «article 29» sur la section 702 de la FISA et à agir en conséquence;

23. fait observer que la réactivation de l'article 702 de la loi FISA pour six ans de plus remet en question la légalité du bouclier de protection des données;

24. réitère ses préoccupations concernant le décret présidentiel 12333, qui permet à la NSA de partager de vastes quantités de données privées, recueillies sans mandat, ordonnance de justice ou autorisation du Congrès, avec 16 autres organismes, dont le FBI, l'agence de lutte contre la drogue et le ministère de la sécurité intérieure; regrette l'absence de tout contrôle juridictionnel des activités de surveillance fondées sur le décret présidentiel 12333;

25. souligne les obstacles persistants concernant la réparation pour les citoyens non américains soumis à une mesure de surveillance fondée sur la section 702 du FISA ou le décret présidentiel 12333 en raison des exigences procédurales de «qualité pour agir», au sens de l'interprétation actuellement faite par les tribunaux américains, ce qui empêche les citoyens non américains d'intenter des actions en justice devant les tribunaux américains contre les décisions qui les affectent;

26. exprime sa préoccupation sur les conséquences du décret présidentiel 13768 portant renforcement de la sécurité publique à l'intérieur des États-Unis sur les recours juridictionnels et administratifs dont peuvent se prévaloir les justiciables aux États-Unis dans la mesure où les garanties prévues par la loi sur la protection des données ne s'appliquent plus aux citoyens non américains; prend note de la position de la Commission selon laquelle l'évaluation du caractère adéquat ne se fonde pas sur les garanties contenues dans la loi sur la protection de la vie privée et que, dans ces conditions, ce décret présidentiel ne porte pas atteinte au bouclier de protection des données; considère que le décret présidentiel 13768 reflète toutefois l'intention de l'exécutif américain d'annuler les garanties de protection des données précédemment accordées aux citoyens de l'UE et de s'affranchir des engagements pris à l'égard de l'UE pendant la présidence Obama;

27. exprime ses vives préoccupations concernant l'adoption récente de la loi CLOUD [Clarifying Lawful Overseas Use of Data Act] (H.R. 4943) visant à clarifier les règles relatives aux réquisitions des autorités américaines sur les données stockées en dehors de leur territoire, qui étend les compétences des services répressifs américains et étrangers en leur permettant de cibler et d'accéder aux données des personnes au-delà des frontières internationales sans recourir aux instruments d'entraide judiciaire (MLAT), qui eux prévoient des garanties appropriées et respectent les compétences judiciaires des pays sur le territoire desquels l'information est stockée; fait observer que la loi CLOUD pourrait avoir de graves conséquences pour l'UE car elle a une grande portée et est source de conflit potentiel avec la législation de l'UE sur la protection des données;

28. estime qu'une solution plus équilibrée aurait été de renforcer le système international existant de traités d'entraide judiciaire (MLAT) en vue d'encourager la coopération

internationale et judiciaire; réaffirme que, comme prévu à l'article 48 du règlement (UE) 679/2016 (règlement général sur la protection des données), l'entraide judiciaire et les accords internationaux divers constituent le mécanisme privilégié pour accéder, à l'étranger, aux données à caractère personnel;

29. déplore que les autorités américaines n'aient pas respecté de manière proactive l'engagement qu'elles ont pris de fournir en temps utile à la Commission des informations complètes sur toutes les évolutions qui pourraient être pertinentes dans le cadre du bouclier de protection des données, notamment en omettant de notifier à la Commission les changements apportés au cadre juridique américain du fait, par exemple, du décret 13768 du président Trump sur le renforcement de la sécurité publique sur le territoire des États-Unis ou de l'abrogation des règles de protection de la vie privée pour les fournisseurs de services Internet;

30. rappelle, comme déjà dans sa résolution du 6 avril 2017, que ni les principes du bouclier de protection des données ni les lettres du gouvernement américain apportant des clarifications et des assurances ne démontrent l'existence de droits de recours effectifs pour les particuliers européens en cas d'utilisation de leurs données à caractère personnel par les autorités américaines à des fins d'application de la loi et d'intérêt public, droits mis en exergue par la Cour de justice de l'Union européenne dans son arrêt du 6 octobre 2015 en ce qu'ils constituent l'essence du droit fondamental visé à l'article 47 de la charte des droits fondamentaux de l'Union européenne;

Conclusions

31. invite la Commission à prendre toutes les mesures nécessaires pour garantir que le bouclier de protection des données sera entièrement conforme au règlement (UE) 2016/679, applicable à partir du 25 mai 2018, et à la charte des droits fondamentaux de l'UE pour éviter ainsi que les critères d'adéquation ne se traduisent par des lacunes ou par un avantage concurrentiel pour les entreprises américaines;

32. déplore que la Commission et les autorités américaines compétentes n'aient pas relancé les discussions sur le bouclier de protection des données et n'aient pas établi de plan d'action afin de remédier dans les meilleurs délais aux déficiences identifiées, comme l'a demandé le groupe de travail «article 29» dans son rapport de décembre sur le réexamen conjoint; invite la Commission et les autorités américaines compétentes à le faire sans plus tarder;

33. rappelle que la protection des données et de la vie privée sont des droits fondamentaux juridiquement contraignants, consacrés par les traités, par la charte des droits fondamentaux et par la convention européenne des droits de l'homme, ainsi que par le droit et la jurisprudence; souligne qu'ils doivent être appliqués d'une manière qui n'entrave pas inutilement le commerce ou les relations internationales, mais qu'ils ne peuvent pas être «mis en balance» avec les intérêts commerciaux ou politiques;

34. est d'avis que l'actuel bouclier de protection des données n'offre pas le niveau de protection adéquat requis par le droit de l'Union en matière de protection des données et par la charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la Cour de justice de l'Union européenne;

35. estime que la Commission n’a pas agi conformément à l’article 45, paragraphe 5, du RGPD, à moins que les États-Unis ne se conforment pleinement à leurs obligations d’ici au 1er septembre 2018; demande par conséquent à la Commission de suspendre le bouclier de protection des données jusqu’à ce que les autorités américaines se conforment aux dispositions de l’accord;

36. charge sa commission des libertés civiles, de la justice et des affaires intérieures de continuer à suivre l’évolution de la situation dans ce domaine, notamment les affaires examinées par la Cour de justice, et de veiller au suivi des recommandations formulées dans la présente résolution;

37. charge son Président de transmettre la présente résolution au Conseil, à la Commission, ainsi qu’aux gouvernements et aux parlements des États membres et au Conseil de l’Europe.