Choisissez la langue de votre document :

bg - български
es - español
cs - čeština
da - dansk
de - Deutsch
et - eesti keel
el - ελληνικά
en - English
fr - français
ga - Gaeilge
hr - hrvatski
it - italiano
lv - latviešu valoda
lt - lietuvių kalba
hu - magyar
mt - Malti
nl - Nederlands
pl - polski
pt - português
ro - română
sk - slovenčina
sl - slovenščina
fi - suomi
sv - svenska

Procédure : 2016/3018(RSP) Cycle de vie en séance

Cycle relatif au document : B8-0235/2017

Textes déposés :	Débats :	Votes :	Textes adoptés :
B8-0235/2017	PV 05/04/2017 - 19 CRE 05/04/2017 - 19	PV 06/04/2017 - 7.7 CRE 06/04/2017 - 7.7	P8_TA(2017)0131

Textes adoptés 293k

Jeudi 6 avril 2017 - Strasbourg Edition provisoire

Adéquation de la protection offerte par le bouclier de protection des données UE-États-Unis

P8_TA-PROV(2017)0131 B8-0235/2017

Résolution du Parlement européen du 6 avril 2017 sur l'adéquation de la protection offerte par le bouclier de protection des données UE-États-Unis (2016/3018(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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données («directive sur la protection des données») [1],

– vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[2],

– 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)[3] 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[4],

– 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[5],

– vu la communication de la Commission au Parlement européen et au Conseil du 6 novembre 2015 concernant le transfert transatlantique de données à caractère personnel conformément à la directive 95/46/CE faisant suite à l'arrêt de la Cour de justice dans l'affaire C-362/14 (Schrems) (COM(2015)0566),

– vu la communication de la Commission au Parlement européen et au Conseil du 10 janvier 2017 intitulée «Exchanging and Protecting Personal Data in a Globalised World» (Échange et protection des données à caractère personnel à l'ère de la mondialisation) (COM(2017)0007),

– 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.[6],

– 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[7],

– 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[8],

– vu l'avis du groupe de travail «article 29» sur la protection des données du 13 avril 2016 sur le bouclier de protection des données UE-États-Unis[9] et la déclaration du groupe de travail «article 29» du 26 juillet 2016[10],

– vu sa résolution du 26 mai 2016 sur les flux de données transatlantiques[11],

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

A. considérant que la Cour de justice de l'Union européenne (CJUE), 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/CE lue à la lumière de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte de l'UE», et qu'il est donc urgent de conclure les négociations relatives au bouclier de protection des données UE-États-Unis 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, sans y être limité, 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, et 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 de l'UE;

D. considérant que le CEPD a formulé plusieurs inquiétudes sur le projet de bouclier de protection des données dans son avis 4/2016; que le CEPD salue dans ce même avis 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;

E. 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 importantes 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;

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

G. considérant que le bouclier de protection des données UE-États-Unis est assorti de plusieurs lettres et déclarations unilatérales de la part du gouvernement américain, 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 personnelles et traiter ces dernières;

H. 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 en 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 personnelles (collecte de masse);

1. salue les efforts de la Commission et du gouvernement américain pour prendre des mesures suite aux inquiétudes soulevées par la CJUE, les États membres, le Parlement européen, les autorités de protection des données (APD) et les parties prenantes, de manière à permettre à la Commission d'adopter la décision d'exécution constatant l'adéquation du bouclier de protection des données UE-États-Unis;

2. reconnaît que le bouclier de protection des données UE-États-Unis comporte des améliorations notables vis-à-vis de clarté des normes par rapport à l'ancien régime de la sphère de sécurité entre l'Union et les États-Unis, et que les organisations américaines déclarant elles-mêmes leur adhésion au bouclier de protection des données UE-États-Unis devront respecter des normes de protection des données plus claires que dans le cadre de la sphère de sécurité;

3. note qu'au 23 mars 2017, 1 893 organisations américaines participent au bouclier de protection des données UE-États-Unis; déplore que le bouclier de protection des données se fonde sur une autocertification volontaire et ne s'applique par conséquent qu'aux organisations américaines qui y participent volontairement, de sorte que de nombreuses entreprises ne sont ainsi pas soumises à ces

règles;

4. admet que le bouclier de protection des données UE-États-Unis facilite le transfert des données des PME et des entreprises de l'Union vers les États-Unis;

5. constate que, conformément à l'arrêt de la CJUE dans l'affaire Schrems, les pouvoirs des APD européennes ne sont pas modifiés par la décision d'adéquation et qu'elles peuvent, par conséquent, les exercer, y compris la suspension ou l'interdiction des transferts de données vers une organisation enregistrée dans le bouclier de protection des données UE-États-Unis; se félicite en ce sens du rôle de premier plan qu'offre le cadre du bouclier de protection des données aux autorités de protection des données des États membres pour examiner et enquêter sur les plaintes relatives à la protection des droits à la vie privée et à la vie familiale en vertu de la charte de l'UE et pour suspendre les transferts de données, ainsi que de l'obligation pour le ministère américain du commerce de résoudre ces plaintes;

6. relève que, dans le cadre du bouclier «vie privée», les ressortissants de l'Union disposent de plusieurs moyens d'introduire des recours en justice aux États-Unis: premièrement, les plaintes peuvent être déposées directement auprès de l'entreprise ou par l'intermédiaire du ministère du commerce après consultation d'une APD ou d'un organisme indépendant de règlement des litiges; deuxièmement, pour ce qui est des atteintes aux droits fondamentaux pour des motifs de sécurité nationale, une action civile peut être intentée devant un tribunal des États-Unis et des plaintes similaires peuvent également être traitées par le médiateur indépendant nouvellement institué; enfin, les plaintes concernant des atteintes aux droits fondamentaux à des fins d'application de la loi ou d'intérêt public peuvent être traitées par des motions contestant des assignations; encourage la Commission et les APD à fournir davantage d'orientations afin de rendre tous ces recours juridiques plus facilement accessibles et disponibles;

7. reconnaît l'engagement clair du département américain du commerce de surveiller étroitement l'application, par les organisations américaines, des principes du bouclier de protection des données UE-États-Unis et son intention de prendre des mesures coercitives contre les structures qui ne seraient pas en conformité;

8. invite à nouveau la Commission à demander des clarifications à propos du statut juridique des «assurances écrites» fournies par les États-Unis et à veiller à ce que tout engagement ou arrangement prévu au titre du bouclier de protection des données soit maintenu à la suite de l'entrée en fonction d'un nouveau gouvernement aux États-Unis;

9. estime que, malgré les engagements et les assurances apportés par le gouvernement américain dans les lettres annexées à l'accord sur le bouclier de protection des données, d'importantes questions demeurent en ce qui concerne certains aspects commerciaux, la sécurité nationale et la répression;

10. relève en particulier la différence importante entre la protection prévue par l'article 7 de la directive 95/46/CE et les principes «Notification» et «Choix» des dispositions du bouclier de protection des données, ainsi que les différences considérables entre l'article 6 de cette même directive et le principe «Intégrité des données et limitation des finalités» des dispositions du bouclier de protection des données; fait observer qu'au lieu d'établir une base juridique (comme le consentement ou un engagement contractuel) qui s'appliquerait à toutes les opérations de traitement des données, les principes du bouclier de protection des données ne prévoient pour les personnes concernées que des droits qui s'appliquent à deux types très particuliers d'opérations de traitement (divulgation et changement de finalité) et ne prévoient qu'un droit d'opposition («clause d'exemption»);

11. estime que ces nombreuses inquiétudes pourraient conduire, à l'avenir, à une nouvelle contestation de la décision d'adéquation de la protection devant les tribunaux; insiste sur les conséquences préjudiciables tant pour le respect des droits fondamentaux que pour la sécurité juridique nécessaire des acteurs concernés;

12. constate, entre autres, l'absence de règles spécifiques sur la prise de décision automatisée et sur un droit général d'opposition, ainsi que le manque de principes clairs sur les modalités d'application du bouclier de protection des données aux sous-traitants (agents);

13. constate que, bien que les individus puissent s'opposer, vis-à-vis du responsable européen de traitement des données, à tout transfert de leurs données personnelles vers les États-Unis ainsi qu'à tout traitement supplémentaire de ces données aux États-Unis, où l'entreprise ayant adhéré au bouclier de protection des données est chargée du traitement des données au nom du responsable européen, le bouclier de protection des données ne contient pas de règles spécifiques à propos d'un droit général de s'opposer vis-à-vis de l'entreprise américaine autocertifiée;

14. constate que seule une petite partie des organisations américaines qui ont souscrit au bouclier de protection des données ont choisi de

faire appel à une APD européenne pour le mécanisme de règlement des litiges; s'inquiète du fait que cela représente un désavantage pour les citoyens de l'Union qui chercheraient à faire valoir leurs droits;

15. constate l'absence de principes explicites sur la manière dont les principes du bouclier de protection des données s'appliquent aux sous-traitants (agents), tout en reconnaissant que tous les principes s'appliquent au traitement des données à caractère personnel par toute entreprise américaine autocertifiée «sauf indication contraire» et que tout transfert à des fins de traitement exige l'établissement d'un contrat avec le responsable européen du traitement, qui déterminera les finalités et les moyens du traitement et décidera notamment si le sous-traitant est autorisé à poursuivre les transferts (par exemple pour la sous-traitance ultérieure);

16. souligne que, en ce qui concerne la sécurité nationale et la surveillance, nonobstant les clarifications apportées par le bureau du directeur des services de renseignement intérieur (Office of the Director of National Intelligence, ODNI) dans les lettres annexées au cadre du bouclier de protection des données, la «surveillance de masse», malgré la terminologie différente utilisée par les autorités américaines, reste possible; regrette que la notion de «surveillance de masse» ne soit pas définie de manière uniforme et que la terminologie américaine ait été reprise, et demande donc une définition uniforme de la «surveillance de masse», reflétant la compréhension européenne de ce terme et garantissant que l'évaluation des données soit indépendante de leur sélection; souligne que toute forme de «surveillance de masse» est contraire à la charte de l'UE;

17. rappelle qu'il ressort de l'annexe VI (lettre de Robert S. Litt, bureau du directeur des services de renseignement intérieur) qu'en vertu de la directive présidentielle n° 28, la collecte de masse des données et communications à caractère personnel relatives à des ressortissants non américains reste autorisée dans six cas; souligne qu'une telle collecte de masse doit uniquement être «aussi ciblée que possible» et «raisonnable», des exigences qui ne satisfont pas aux critères plus stricts de nécessité et de proportionnalité définis par la charte de l'UE;

18. constate avec une profonde inquiétude qu'au sein du Conseil de surveillance de la vie privée et des libertés civiles, mentionné à l'annexe VI (lettre de Robert S. Litt, ODNI) en tant qu'organe indépendant établi par voie législative chargé d'analyser et de contrôler les programmes et politiques de contre-terrorisme, y compris le recours au renseignement d'origine électromagnétique, afin de garantir qu'ils protègent de manière adéquate la vie privée et les libertés civiles, le quorum n'est plus atteint depuis le 7 janvier 2017, et que cette situation perdurera jusqu'à la nomination de nouveaux membres au conseil d'administration par le président des États-Unis et leur confirmation par le Sénat; souligne que l'absence de quorum limite les pouvoirs du Conseil de surveillance de la vie privée et des libertés civiles, qui ne peut entreprendre certaines actions qui requièrent l'aval des membres du conseil d'administration, telles que le lancement de projets de surveillance ou la formulation de recommandations en matière de surveillance, situation qui compromet gravement les garanties et assurances en matière de conformité et de contrôle données par les autorités américaines à cet égard;

19. déplore le fait que le bouclier de protection des données UE-États-Unis n'interdit pas la collecte de données en masse à des fins répressives;

20. souligne que, dans son arrêt du 21 décembre 2016, la CJUE a clairement expliqué que la charte de l'UE «doit être [interprétée] en ce sens qu'[elle] s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique»; fait observer que, dès lors, la surveillance de masse aux États-Unis ne fournit pas un niveau essentiellement équivalent de protection des données et communications à caractère personnel;

21. s'inquiète vivement des récentes révélations relatives à des activités de surveillance exercées par prestataire américain de services de communication électronique sur tous les courriels ayant transité par ses serveurs, à la demande de la l'Agence de sécurité nationale (NSA) et du Bureau fédéral d'enquête (FBI), en 2015 encore, soit un an après l'adoption de la directive présidentielle nº 28 et pendant les négociations du bouclier de protection des données UE-États-Unis; invite instamment la Commission à demander aux autorités américaines qu'elles fournissent une clarification totale et mettent leurs réponses à la disposition du Conseil, du Parlement et des autorités nationales de protection des données; considère qu'il y a là un motif de douter fortement des assurances fournies par le bureau du directeur des services de renseignement intérieur; est conscient du fait que le bouclier de protection des données UE-États-Unis repose sur la directive présidentielle (presidential policy directive) n° 28 (PPD-28), prise par le président américain et pouvant tout autant être abrogée par un futur président sans l'accord du Congrès des États-Unis;

22. constate avec inquiétude que le Sénat américain et la Chambre des représentants ont voté, les 23 et 28 mars 2017 respectivement, en faveur du rejet de la règle introduite par la Commission fédérale des communications relative à «la protection de la vie privée des clients de services à haut débit et d'autres services de télécommunications», ce qui, en pratique, élimine les règles de protection de la vie privée dans les services à haut débit qui imposent aux fournisseurs d'accès à internet d'obtenir le consentement exprès des consommateurs avant

de pouvoir vendre aux annonceurs et à d'autres sociétés des données de navigation sur internet et d'autres informations privées ou de les partager avec ces derniers; considère que ce vote fait peser une nouvelle menace sur la protection de la vie privée aux États-Unis;

23. exprime sa vive inquiétude quant à la publication des procédures relatives à la mise à disposition et à la diffusion de données brutes sur le renseignement d'origine électromagnétique au titre de la section 2.3 du décret présidentiel nº 12333 («Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333»), approuvées par le procureur général le 3 janvier 2017 et permettant à la NSA de partager une grande quantité de données privées collectées sans mandat, ni ordonnance du tribunal, ni autorisation du Congrès, avec 16 autres agences, dont le FBI, l'Agence américaine de lutte contre la drogue (DEA) et le ministère de la sécurité intérieure; invite la Commission à évaluer immédiatement la compatibilité de ces nouvelles règles avec les engagements pris par les autorités américaines en vertu du bouclier de protection des données ainsi que leur incidence sur le niveau de protection des données à caractère personnel aux États-Unis;

24. rappelle que si les personnes physiques, notamment les ressortissants de l'Union, disposent d'un certain nombre de voies de recours lorsqu'elles ont fait l'objet d'une surveillance (électronique) illégale au nom de la sécurité nationale des États-Unis, certains fondements juridiques au moins pouvant être utilisés par les services de renseignement américains (comme le décret 12333) ne sont cependant pas couverts; souligne en outre que même lorsque des possibilités de recours juridictionnel existent en principe pour les personnes non américaines, dans le cas d'une surveillance en vertu du Foreign Intelligence Surveillance Act, par exemple, les moyens d'action sont limités et les réclamations introduites par des personnes physiques (même américaines) seront déclarées irrecevables lorsque celles-ci ne peuvent démontrer leur qualité pour agir, ce qui restreint l'accès aux tribunaux ordinaires;

25. invite la Commission à déterminer l'incidence du décret du 25 janvier 2017 sur le renforcement de la sécurité publique sur le territoire des États-Unis (Enhancing Public Safety in the Interior of the United States), et en particulier de sa section 14 concernant l'exclusion des ressortissants étrangers de la protection octroyée par le Privacy act au regard des informations à caractère personnel, laquelle est contraire aux garanties données par écrit sur l'existence de voies de recours judiciaires pour les personnes physiques en cas d'accès à des données par les autorités américaines; demande à la Commission de transmettre une analyse juridique détaillée des répercussions des dispositions de ce décret sur les voies et droits de recours des ressortissants européens aux États-Unis;

26. déplore le fait 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 dont les données personnelles sont transférées à une organisation américaine conformément aux principes du bouclier de protection des données et consultées et traitées par les autorités publiques américaines à des fins d'application de la loi et d'intérêt public, droits mis en exergue par la CJUE dans son arrêt du 6 octobre 2015 en ce qu'ils constituent l'essence du droit fondamental prévu à l'article 47 de la charte de l'UE;

27. rappelle sa résolution du 26 mai 2016, selon laquelle le médiateur mis en place par le département d'État américain n'est pas suffisamment indépendant et n'est pas pourvu de pouvoirs effectifs suffisants pour mener à bien ses missions et offrir aux ressortissants de l'Union des voies de recours efficaces; fait observer qu'à ce jour, la future administration des États-Unis n'a pas nommé de nouveau médiateur pour prendre la relève de la sous-secrétaire d'État américaine à la croissance économique, à l'énergie et à l'environnement, désignée pour remplir cette fonction en juillet 2016, à la fin de son mandat; estime que tant qu'aucun médiateur indépendant et disposant de suffisamment de pouvoirs n'aura été désigné, les garanties données par les États-Unis concernant l'existence d'un mécanisme de recours efficace pour les citoyens de l'Union seront considérées comme nulles et non avenues; exprime son inquiétude quant au fait qu'une personne concernée par le non-respect de la protection de ses données puisse uniquement demander un accès aux données et leur suppression, ou bien la cessation de leur traitement, mais ne puisse pas obtenir réparation du préjudice subi;

28. observe avec inquiétude qu'au 30 mars 2017, la commission américaine du commerce (FTC), qui fait appliquer les principes du bouclier de protection des données, avait trois de ses cinq sièges vacants;

29. regrette que la procédure d'adoption de la décision d'adéquation ne prévoie pas de consultation formelle des acteurs concernés, tels que les entreprises, et en particulier les organisations représentatives des PME;

30. regrette que la Commission ait suivi la procédure d'adoption de sa décision d'exécution d'une manière qui, de facto, n'a pas permis au Parlement d'exercer de manière efficace son droit de regard sur le projet d'acte d'exécution;

31. invite la Commission à prendre toutes les mesures nécessaires pour garantir que le bouclier de protection des données sera entièrement conforme à la charte de l'UE et au règlement (UE) 2016/679, applicable à partir du 16 mai 2018;

32. invite la Commission à garantir, en particulier, que les données à caractère personnel transférées vers les États-Unis en vertu du bouclier de protection des données ne peuvent être transférées vers un autre pays tiers que si ce transfert est compatible avec la finalité dans laquelle les données ont été collectées en premier lieu et si les mêmes règles en matière d'accès spécifique et ciblé à des fins répressives s'appliquent dans le pays tiers concerné;

33. invite la Commission à veiller à ce que les données à caractère personnel qui ne sont plus nécessaires eu égard à la finalité dans laquelle elles ont été collectées en premier lieu soient supprimées, y compris par les services répressifs;

34. invite la Commission à contrôler de près le bouclier de protection des données pour déterminer s'il permet aux APD d'exercer pleinement leurs pouvoirs et, sinon, d'identifier les dispositions qui les en empêchent;

35. demande à la Commission de réaliser, lors du premier réexamen annuel conjoint, un examen complet et approfondi de tous les défauts et faiblesses mentionnés dans la présente résolution et dans la résolution du 26 mai 2016 sur les flux de données transatlantiques, ainsi que ceux identifiés par le groupe de travail «article 29», le CEPD et les parties prenantes, 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 du gouvernement américain;

36. invite la Commission à veiller à ce que, lors de la conduite du réexamen annuel conjoint, tous les membres de l'équipe aient un accès total et sans restriction à l'ensemble des documents et locaux nécessaires à l'exercice de leur mission, y compris aux éléments permettant d'évaluer correctement la nécessité et la proportionnalité de la collecte des données transférées par les autorités publiques et de l'accès à ces données, à des fins d'application de la loi ou de sécurité nationale;

37. souligne qu'il convient de garantir l'indépendance de tous les membres de l'équipe chargée du réexamen commun dans l'exercice de leurs missions ainsi que leur droit d'exprimer leurs propres opinions dissidentes dans le rapport final du réexamen conjoint qui sera rendu public et annexé au rapport conjoint;

38. demande aux autorités européennes de protection des données de surveiller le fonctionnement du bouclier de protection des données UE-États-Unis et d'exercer leurs pouvoirs, y compris de procéder à la suspension ou à l'interdiction définitive des transferts de données personnelles vers une organisation dans le cadre du bouclier européen de protection des données si elles estiment que les droits fondamentaux tels que le droit à la vie privée et la protection des données personnelles ne sont pas garantis;

39. souligne que le Parlement devrait avoir pleinement accès à tout document pertinent en lien avec le réexamen annuel conjoint;

40. charge son Président de transmettre la présente résolution à la Commission, au Conseil, aux gouvernements et aux parlements des États membres, ainsi qu'au gouvernement et au Congrès américains.

---

(1) JO L 281 du 23.11.1995, p. 31.
(2) JO L 350 du 30.12.2008, p. 60.
(3) JO L 119 du 4.5.2016, p. 1.
(4) JO L 119 du 4.5.2016, p. 89.
(5) ECLI:EU:C:2015:650.
(6) ECLI:EU:C:2016:970.
(7) JO L 207 du 1.8.2016, p. 1.
(8) JO C 257 du 15.7.2016, p. 8.
(9) ***http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf***

(10)***http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf***

(11)Textes adoptés de cette date, **P8_TA(2016)0233**.