



Document de séance

B8-0633/2016

23.5.2016

PROPOSITION DE RÉSOLUTION

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

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

sur les flux de données transatlantiques
(2016/2727(RSP))

Ignazio Corrao, Laura Ferrara, Beatrix von Storch
au nom du groupe EFDD

**Résolution du Parlement européen sur les flux de données transatlantiques
(2016/2727(RSP))**

Le Parlement européen,

- vu le cadre juridique établi par le traité sur l'Union européenne (traité UE), notamment ses articles 2, 3, 4, 5, 6, 7, 10 et 21, la charte des droits fondamentaux de l'Union européenne, notamment ses articles premier, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 et 52, la convention européenne des droits de l'homme, notamment ses articles 6, 8, 9, 10 et 13, et la jurisprudence des juridictions européennes en matière de sécurité, de respect de la vie privée et de liberté d'expression,
- 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 données¹ (ci-après "directive sur la protection des données"),
- 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 pénale²,
- vu le règlement (UE) n° 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 Conseil⁴,
- vu la décision 2000/520/CE de la Commission du 26 juillet 2000 (décision sur la sphère de sécurité),
- vu la communication de la Commission au Parlement européen et au Conseil du 27 novembre 2013 intitulée "Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique" (COM(2013)0846) et la communication de la Commission au Parlement européen et au Conseil du 27 novembre 2013 relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire (communication sur la sphère de sécurité) (COM(2013)0847),

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.

- 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* (EU:C:2015:650),
 - 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 déclaration du groupe de travail "Article 29" du 3 février 2016 sur les conséquences de l'arrêt Schrems,
 - vu le *Judicial Redress Act* (loi sur le recours juridictionnel) de 2015, promulgué par le président Obama le 24 février 2016 (H.R.1428),
 - vu le *USA Freedom Act* de 2015¹,
 - vu les réformes des activités de renseignement d'origine électromagnétique des États-Unis inscrites dans la directive présidentielle n° 28 (PPD-28)² et la communication de la Commission au Parlement européen et au Conseil du 29 février 2016 intitulée "Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides" (COM(2016)0117),
 - vu l'avis 01/2016 du 13 avril 2016 du groupe de travail "Article 29" sur le projet de décision concernant le caractère adéquat du "bouclier de protection des données UE-États-Unis",
 - vu l'article 123, paragraphe 2, de son règlement,
- A. considérant que la Cour de justice de l'Union européenne a invalidé la décision concernant la sphère de sécurité dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems* contre *Data Protection Commissioner*;
- B. considérant que la Cour de justice de l'Union européenne a insisté sur les éléments ci-après dans son arrêt dans l'affaire C-362/14:
- i. le droit fondamental à la protection des données à caractère personnel est essentiel, y compris lorsque les données sont transférées en dehors de l'Union européenne;
 - ii. la décision de la Commission concernant la sphère de sécurité ne contient pas les constatations suffisantes quant aux limitations en ce qui concerne l'accès des autorités publiques américaines aux données transférées en vertu de ladite décision et à l'existence d'une protection juridique efficace contre des ingérences de cette nature,
 - iii. les exigences américaines relatives à la sécurité nationale, à l'intérêt public et à l'application de la loi prévalent sur les principes de la sphère de sécurité, et les

¹ <https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf>

² <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

entreprises américaines sont donc tenues d'écarter les règles de protection de la sphère de sécurité lorsqu'elles entrent en conflit avec ces exigences;

- iv. l'accès généralisé au contenu des communications électroniques par les autorités publiques porte atteinte au droit fondamental au respect de la vie privée;
 - v. l'existence d'une décision de la Commission constatant qu'un pays tiers assure un niveau de protection adéquat des données à caractère personnel transférées ne saurait annihiler ou réduire les pouvoirs des autorités nationales de contrôle de vérifier indépendamment si les transferts de données à caractère personnel vers un pays tiers respectent les exigences fixées par la directive relative à la protection des données;
- C. considérant qu'en l'absence de décision sur la sphère de sécurité, les entreprises qui transfèrent des données de l'Union européenne vers les États-Unis sont confrontées à une insécurité juridique et à d'éventuelles mesures de mise en conformité et d'application des États membres, mais peuvent recourir à d'autres instruments pour transférer des données vers les États-Unis, par exemple des clauses contractuelles types (la Commission propose des modèles de clauses contractuelles aux entreprises en relation avec des responsables du traitement des données à l'étranger) et des règles d'entreprise contraignantes (ensemble de règles définissant les politiques des entreprises en matière de transferts internationaux de données à caractère personnel au sein d'un même groupe d'entreprises);
- D. considérant que si l'accord entre l'Union européenne et les États-Unis sur le bouclier de protection des données a été largement salué par les représentants du monde des affaires, il n'est pas encore certain que le nouveau cadre procurera une sécurité juridique à long terme aux entreprises qui transfèrent des données de l'Union européenne vers les États-Unis;
1. salue les efforts déployés par la Commission et le gouvernement des États-Unis pour apporter des améliorations substantielles au bouclier de protection des données UE-États-Unis par rapport à la décision concernant la sphère de sécurité, et met l'accent sur l'importance des échanges et de la coopération transatlantiques;
 2. insiste sur le fait qu'une relation saine entre l'Union et les États-Unis reste absolument indispensable pour les deux parties; souligne, dans ce contexte, qu'une solution négociée entre les États-Unis et l'Union européenne dans son ensemble, respectueuse du droit à la protection des données et du droit à la vie privée, doit être trouvée;
 3. prend acte des conséquences de l'arrêt C-362/14 de la Cour de justice de l'Union européenne et de la réglementation de l'Union sur le droit à l'oubli tel que décrit dans l'arrêt C-131/12 de la Cour du 13 mai 2014 (*Google Spain SL, Google Inc. contre AEPD*) et à l'article 17 du règlement général sur la protection des données, qui entrera en vigueur en 2018, qui creusent déjà un profond fossé juridique, économique et culturel entre les partenaires commerciaux européens et américains;
 4. rappelle que la décision concernant le caractère adéquat du bouclier de protection des données et les annexes y afférentes doivent être conformes aux exigences de l'arrêt C-362/14 en imposant des "obligations strictes aux entreprises qui traitent des

données à caractère personnel européennes, et un contrôle rigoureux", "un accès par les autorités américaines étroitement encadré et transparent" et "une protection effective des droits des citoyens de l'Union et plusieurs voies de recours";

5. invite la Commission à mettre en œuvre pleinement les recommandations formulées par le groupe de travail "Article 29" dans son avis 01/2016 sur le projet de décision concernant le caractère adéquat du bouclier de protection des données UE-États-Unis;
6. s'inquiète du fait que le dispositif du bouclier de protection des données puisse ne pas entièrement satisfaire aux exigences de la charte des droits fondamentaux de l'Union européenne, de la directive sur la protection des données, du règlement général sur la protection des données et des arrêts rendus en la matière par la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme;
7. demande à la Commission de ne pas outrepasser ses compétences d'exécution en décidant que le bouclier de protection des données assure un niveau adéquat de protection des données aux États-Unis sans réaliser d'analyse approfondie du système américain ni tenir compte des aspects mis en lumière dans la présente résolution;
8. insiste sur la nécessité de prévoir, à tout le moins, une clause limitant à deux ans la validité de la décision concernant le caractère adéquat du dispositif et d'entamer de nouvelles négociations avec les États-Unis sur un cadre amélioré fondé sur le règlement général sur la protection des données;
9. charge son Président de transmettre la présente résolution au Conseil, à la Commission, aux gouvernements et aux parlements des États membres, ainsi qu'au gouvernement et au Congrès des États-Unis d'Amérique.