Parlement européen
2019-2024

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

2023/2501(RSP)

14.2.2023

PROJET DE PROPOSITION DE RÉSOLUTION

déposée à la suite d'une déclaration de la Commission

conformément à l'article 132, paragraphe 2, du règlement intérieur

sur l'adéquation de la protection assurée par le cadre de protection des données UE–États-Unis
(2023/2501(RSP))

Juan Fernando López Aguilar
au nom de la commission des libertés civiles, de la justice et des affaires intérieures

B9-0000/2023

Résolution du Parlement européen sur l'adéquation de la protection assurée par le cadre de protection des données UE–États-Unis
(2023/2501(RSP))

Le Parlement européen,

– vu la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), en particulier ses articles 7, 8, 16 et 47 ainsi que son article 52,

– 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 (ci-après l'«arrêt Schrems I»)[1],

– vu l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems (ci-après l'«arrêt Schrems II»)[2],

– vu son enquête sur les révélations faites par Edward Snowden concernant la surveillance électronique de masse des citoyens de l'Union, y compris les conclusions de sa résolution 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[3],

– vu sa résolution du 26 mai 2016 sur les flux de données transatlantiques[4],

– vu sa résolution du 6 avril 2017 sur l'adéquation de la protection offerte par le bouclier de protection des données UE-États-Unis[5],

– vu sa résolution du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis[6],

– vu sa résolution du 20 mai 2021 sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems («arrêt Schrems II»)[7],

– vu le projet de décision d'exécution de la Commission conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection

[1] Arrêt de la Cour de justice du 6 octobre 2015, Maximillian Schrems contre Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.
[2] Arrêt de la Cour de justice du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.
[3] JO C 378 du 9.11.2017, p. 104.
[4] JO C 76 du 28.2.2018, p. 82.
[5] JO C 298 du 23.8.2018, p. 73.
[6] JO C 118 du 8.4.2020, p. 133.
[7] JO C 15 du 12.1.2022, p. 176.

des données UE–États-Unis,

– vu le décret 14086 du Président des États-Unis du 7 octobre 2022 sur le renforcement des garanties applicables aux activités de renseignement d'origine électromagnétique menées par les États-Unis,

– vu le règlement relatif à la Cour de révision de la protection des données émis par le procureur général des États-Unis (le «règlement du procureur général»),

– 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 (ci-après le «RGPD»)[8], et notamment son chapitre V,

– vu la proposition de la Commission du 10 janvier 2017 relative à un règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques») (COM(2017)0010), vu la décision d'engager des négociations interinstitutionnelles confirmée par la plénière du Parlement le 25 octobre 2017 et vu l'orientation générale du Conseil adoptée le 10 février 2021 (6087/21),

– vu les recommandations 01/2020 du comité européen de la protection des données sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'Union et les recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance,

– vu l'avis du comité européen de la protection des données du [à ajouter],

– vu l'article 132, paragraphe 2, de son règlement intérieur,

A. considérant que la Cour de justice de l'Union européenne, dans l'arrêt «Schrems I», a invalidé la décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de 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 d'Amérique[9], et a souligné que l'accès indifférencié, par les autorités de renseignement, au contenu des communications électroniques, porte atteinte au contenu essentiel du droit fondamental à la confidentialité des communications consacré à l'article 7 de la charte;

B. considérant que la Cour de justice, dans l'arrêt «Schrems II», a invalidé 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[10] et a conclu

[8] JO L 119 du 4.5.2016, p. 1.
[9] JO L 215 du 25.8.2000, p. 7.
[10] JO L 207 du 1.8.2016, p. 1.

qu’il ne prévoyait pas suffisamment de voies de recours judiciaires pour les non-ressortissants contre la surveillance de masse, ce qui porte atteinte au contenu essentiel du droit à un recours effectif consacré à l’article 47 de la charte;

C. considérant que le 7 octobre 2022, le Président des États-Unis a signé le décret 14086 sur le renforcement des garanties applicables aux activités de renseignement d’origine électromagnétique menées par les États-Unis,

D. considérant que le 13 décembre 2022, la Commission a lancé le processus d’adoption d’une décision d’adéquation concernant le cadre de protection des données UE-États-Unis;

E. 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;

F. considérant que la possibilité de transférer des données à caractère personnel par-delà les frontières peut être un moteur essentiel d’innovation, de productivité et de compétitivité économique; considérant que ces transferts devraient être effectués dans le strict respect du droit à la protection des données à caractère personnel et du droit au respect de la vie privée; considérant que l’un des objectifs fondamentaux de l’Union est la protection des droits fondamentaux consacrés par la charte;

G. considérant que le règlement général sur la protection des données (RGPD) s’applique à l’ensemble des entreprises qui traitent des données à caractère personnel de personnes concernées qui se trouvent dans l’Union, lorsque les activités de traitement sont liées à l’offre de biens ou de services à ces personnes dans l’Union, ou au suivi de leur comportement, dans la mesure où celui-ci a lieu au sein de l’Union;

H. considérant que la surveillance de masse et la collecte massive des données par des acteurs étatiques nuisent à la confiance des entreprises et des citoyens européens à l’égard des services numériques et, par extension, de l’économie numérique;

I. considérant que les responsables du traitement devraient toujours rendre des comptes quant au respect des obligations en matière de protection des données, notamment en prouvant la conformité de tout traitement des données, quels que soient la nature, la portée, le contexte, les finalités et les risques pour les personnes dont les données sont traitées;

J. considérant qu’il n’existe pas de législation fédérale sur la protection des données et le respect de la vie privée aux États-Unis; considérant que l’Union européenne et les États-Unis ont des définitions divergentes des concepts clés en matière de protection des données, tels que les principes de nécessité et de proportionnalité;

1. rappelle que la protection des données et le respect de la vie privée sont des droits fondamentaux juridiquement contraignants consacrés par les traités, la charte et la Convention européenne des droits de l’homme, ainsi que par le droit et la jurisprudence; insiste sur le fait qu’ils doivent être appliqués d’une manière qui n’entrave pas inutilement le commerce ou les relations internationales, mais qu’ils peuvent

uniquement être «mis en balance» avec d'autres droits fondamentaux et non avec des intérêts commerciaux ou politiques;

2. prend acte des efforts accomplis dans le décret pour fixer des limites aux activités de renseignement d'origine électromagnétique menées par les États-Unis, en se référant aux principes de proportionnalité et de nécessité, et en dressant une liste des objectifs légitimes de ces activités; souligne, cependant, que ces principes sont des éléments essentiels qui s'inscrivent de longue date dans le régime de protection des données de l'Union européenne et que leurs définitions précises dans le décret ne sont pas conformes à leurs définitions dans le droit de l'Union ni à leur interprétation par la Cour de justice; souligne, en outre, qu'aux fins du cadre de protection des données UE-États-Unis, ces principes seront interprétés uniquement en considération du droit et des traditions juridiques des États-Unis; souligne qu'en vertu du décret, le renseignement d'origine électromagnétique doit être effectué de manière proportionnée à la «priorité validée en matière de renseignement», ce qui semble être une interprétation large de la proportionnalité;

3. déplore que le décret n'interdise pas la collecte massive de données par le renseignement d'origine électromagnétique, y compris le contenu des communications; note que la liste des objectifs légitimes de sécurité nationale peut être élargie par le Président des États-Unis, qui peut décider de ne pas rendre publiques les mises à jour pertinentes;

4. souligne que le décret ne s'applique pas aux données auxquelles les autorités publiques accèdent par d'autres moyens, par exemple grâce à la loi américaine sur l'informatique en nuage (Cloud Act) ou à la loi antiterroriste (Patriot Act), à l'achat de données commerciales ou à des accords de partage volontaire des données;

5. souligne que les décisions de la Cour de révision de la protection des données seront classifiées et ne seront pas rendues publiques ni mises à la disposition du plaignant; souligne que la Cour de révision de la protection des données relève du pouvoir exécutif et non du pouvoir judiciaire; souligne qu'un plaignant sera représenté par un «avocat spécial» désigné par la Cour de révision de la protection des données, pour laquelle il n'existe aucune exigence d'indépendance; souligne que la procédure de recours prévue par le décret est fondée sur le secret et ne prévoit pas l'obligation d'informer le plaignant que ses données à caractère personnel ont été traitées, ce qui porte atteinte à son droit d'accéder à ses données ou de les rectifier; relève que la procédure de recours proposée ne prévoit pas de voie de recours devant une cour fédérale et, partant, ne prévoit pas, entre autres, la possibilité pour le plaignant de réclamer des dommages et intérêts; conclut que la Cour de révision de la protection des données ne respecte pas les normes d'indépendance et d'impartialité énoncées à l'article 47 de la charte;

6. constate que, si les États-Unis ont prévu un nouveau mécanisme de recours pour les questions liées à l'accès des autorités publiques aux données, les voies de recours disponibles en matière commerciale en vertu de la décision d'adéquation sont insuffisantes; note que ces questions sont largement laissées à l'appréciation des entreprises, qui peuvent choisir d'autres voies de recours, telles que les mécanismes de règlement des litiges ou le recours aux programmes de protection de la vie privée proposés par les entreprises;

7. constate que les entreprises européennes ont besoin de sécurité juridique et méritent d'en bénéficier; met l'accent sur le fait que les mécanismes successifs de transfert de données, qui ont ensuite été abrogés par la Cour de justice, ont entraîné des coûts supplémentaires pour les entreprises européennes; constate que l'incertitude persistante et la nécessité de s'adapter aux nouvelles solutions juridiques sont particulièrement contraignantes pour les micro, petites et moyennes entreprises;

8. souligne que, contrairement à tous les autres pays tiers qui ont reçu une décision d'adéquation au titre du RGPD, les États-Unis ne disposent toujours pas d'une loi fédérale sur la protection des données; souligne que le décret n'est pas clair, précis, ni prévisible dans son application, étant donné qu'il peut être modifié à tout moment par le Président des États-Unis; s'inquiète dès lors de l'absence d'une clause de caducité en vertu de laquelle la décision pourrait expirer automatiquement quatre ans après son entrée en vigueur;

9. insiste sur le fait que les décisions d'adéquation doivent inclure des mécanismes clairs et stricts de suivi et de réexamen afin de garantir que les décisions sont adaptées aux évolutions futures et que le droit fondamental des citoyens de l'Union à la protection des données est garanti;

Conclusions

10. rappelle que, dans sa résolution du 20 mai 2021, le Parlement a invité la Commission à ne pas adopter de nouvelle décision d'adéquation à l'égard des États-Unis, à moins que des réformes significatives ne soient mises en place, en particulier à des fins de sécurité nationale et de renseignement;

11. conclut que le cadre de protection des données UE–États-Unis ne crée pas de réelle équivalence du niveau de protection; invite la Commission à poursuivre les négociations avec ses homologues américains dans le but de créer un mécanisme qui garantirait cette équivalence et assurerait le niveau de protection adéquat requis par le droit de l'Union en matière de protection des données et la charte telle qu'interprétée par la Cour de justice; demande instamment à la Commission de ne pas adopter le constat d'adéquation;

°

° °

12. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission, ainsi qu'au Président et au Congrès des États-Unis d'Amérique.