|  |  |
| --- | --- |
| Parlement européen  2019-2024 | EP logo RGB_Mute |

{LIBE}Commission des libertés civiles, de la justice et des affaires intérieures

<NoDocSe>2020/2789(RSP)</NoDocSe>

<Date>{13/01/2021}13.1.2021</Date>

<TitreType>PROJET DE PROPOSITION DE RÉSOLUTION</TitreType>

<TitreSuite>déposée à la suite d’une déclaration de la Commission</TitreSuite>

<TitreRecueil>conformément à l’article 132, paragraphe 2, du règlement intérieur</TitreRecueil>

<Titre>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»)</Titre>

<DocRef>(2020/2789(RSP))</DocRef>

<RepeatBlock-By><Depute>Juan Fernando López Aguilar</Depute>

<Commission>{LIBE}au nom de la commission des libertés civiles, de la justice et des affaires intérieures</Commission>

</RepeatBlock-By>

B9-0000/2021

Résolution du Parlement européen 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»)

(2020/2789(RSP))

*Le Parlement européen*,

– vu la charte des droits fondamentaux de l’Union européenne, en particulier ses articles 7, 8, 47 et 52,

– 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[[1]](#footnote-1) (ci-après «arrêt Schrems II»),

– 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[[2]](#footnote-2) (ci‑après «arrêt Schrems I»),

– vu l’arrêt rendu par la Cour de justice de l’Union européenne le 6 octobre 2020 dans l’affaire C-623/17, Privacy International contre Secretary of State for Foreign and Commonwealth Affairs[[3]](#footnote-3),

– vu sa résolution du 5 juillet 2018 sur l’adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis[[4]](#footnote-4),

– vu sa résolution du 25 octobre 2018 sur l’exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données[[5]](#footnote-5),

– vu sa résolution du 23 novembre 2020 sur l’examen de la politique commerciale de l’Union[[6]](#footnote-6),

– vu le règlement (UE) 2016/679, règlement général sur la protection des données (RGPD)[[7]](#footnote-7),

– 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’UE et les recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance[[8]](#footnote-8),

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

A. considérant que la Cour de justice de l’Union européenne (ci-après «la Cour»), dans l’arrêt Schrems I, a fait observer que l’accès indiscriminé, par les services de renseignement, au contenu des communications électroniques porte atteinte au contenu essentiel du droit à la confidentialité des communications consacré à l’article 7 de la charte des droits fondamentaux de l’Union européenne (ci-après «la charte»);

B. considérant que la Cour, dans l’arrêt Schrems II, a fait observer que les États-Unis ne prévoient 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 dans sa résolution du 25 octobre 2018, le Parlement européen demandait déjà à la Commission de suspendre le bouclier de protection des données;

***OBSERVATIONS GÉNÉRALES***

1. prend acte de l’arrêt de la Cour du 16 juillet 2020, dans lequel la Cour confirme la validité de la décision 2010/87 relative aux clauses contractuelles types, estimant que ces dernières constituent un mécanisme efficace pour veiller à la conformité avec le niveau de protection prévu dans le droit de l’Union; prend acte, en outre, de l’annulation par la Cour de la décision 2016/1250 de la Commission relative à l’adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis;

2. est convaincu que l’arrêt de la Cour a des implications significatives pour les décisions relatives à l’adéquation de la protection des données dans des pays tiers; réaffirme qu’une clarté et une sécurité juridiques sont indispensables;

3. se dit préoccupé par le fait que l’affaire Schrems II ait été portée devant la Cour par le commissaire irlandais à la protection des données, alors qu’il aurait pu prendre une décision dans le cadre des pouvoirs que lui confère l’article 58 du RGPD; se dit fortement préoccupé par le fait que le commissaire irlandais à la protection des données n’ait pas encore tranché sur plusieurs réclamations qui lui ont été présentées le 25 mai 2018 concernant des infractions au RGPD, alors qu’il est l’autorité compétente au premier chef pour ces affaires; condamne fermement la tentative de l’autorité irlandaise de protection des données de faire supporter à Maximilian Schrems les coûts de la procédure judiciaire, ce qui aurait eu un effet dissuasif généralisé; demande à la Commission d’engager une procédure en manquement à l’encontre de l’Irlande pour absence de contrôle satisfaisant de l’application du RGPD;

4. invite instamment la Commission à publier davantage d’orientations sur les transferts de données internationaux à l’intention des entreprises, en particulier des PME, qui portent entre autres sur les garanties supplémentaires exigées dans le cadre des transferts s’appuyant sur les clauses contractuelles types;

***CLAUSES CONTRACTUELLES TYPES***

5. prend acte du projet de décision d’exécution de la Commission et du projet de clauses contractuelles types; salue le fait que la Commission consulte actuellement les parties prenantes au sujet de ce projet;

6. prend acte des 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’UE; se dit préoccupé par les potentielles dissonances entre ces recommandations et la proposition de la Commission relative aux clauses contractuelles types; estime que le comité européen de la protection des données doit publier des orientations plus détaillées;

7. estime crucial que les entreprises de l’Union puissent s’appuyer sur des mécanismes solides conformes à l’arrêt de la Cour; estime, à cet égard, que la proposition de la Commission relative à un modèle de clauses contractuelles types devrait prendre dûment en compte l’ensemble des recommandations pertinentes; se dit favorable à une boîte à outils de mesures supplémentaires, comme une certification de sécurité ou des garanties en matière de chiffrement, acceptées par les autorités de réglementation;

8. fait observer que, pour les responsables du traitement de données qui relèvent du champ d’application de la loi américaine sur la surveillance et le renseignement étranger (loi FISA), un transfert de données à caractère personnel en provenance de l’Union n’est pas possible dans le cadre de ces clauses contractuelles types, en raison du risque élevé de surveillance de masse; estime que seule une réforme en profondeur des pratiques de surveillance aux États-Unis peut contribuer à résoudre ce problème et à apporter une sécurité juridique aux entreprises et aux personnes dont les données sont traitées;

9. rappelle qu’un grand nombre de PME ont recours à des clauses contractuelles types; souligne que les entreprises et les PME ont un besoin urgent de lignes directrices claires et d’aide à l’application et à l’interprétation de l’arrêt de la Cour;

10. souligne que les PME européennes disposent d’un pouvoir de négociation et de capacités juridiques limités, alors qu’on attend d’elles qu’elles évaluent elles-mêmes l’adéquation de la protection des données dans des pays tiers, ce qui implique d’évaluer des cadres juridiques complexes de divers pays tiers; invite instamment la Commission et le comité européen de la protection des données à examiner de manière approfondie la nécessité et la faisabilité de toute mesure supplémentaire exigée, en particulier pour les PME;

11. invite instamment, dans ces cas, les autorités de contrôle nationales à exercer les pouvoirs visés à l’article 3 du projet de décision d’exécution ainsi que ceux que leur confère l’article 58 du RGPD;

***BOUCLIER DE PROTECTION DES DONNÉES***

12. relève que, malgré l’amélioration que représente le bouclier de protection des données par rapport à la sphère de sécurité, la Cour a constaté que le bouclier de protection des données UE-États-Unis ne garantit pas un niveau adéquat de protection essentiellement équivalent à celui qui est garanti par le RGPD et la charte, notamment en raison des conditions prévues en ce qui concerne l’accès des pouvoirs publics des États-Unis aux données à caractère personnel transférées dans le cadre du bouclier de protection des données, ainsi qu’en raison de l’absence, pour les personnes de l’Union dont les données sont traitées, de droits opposables aux autorités américaines devant les tribunaux des États-Unis;

13. rappelle sa résolution de 2018 sur le bouclier de protection des données, dans laquelle il insistait sur le risque de voir le bouclier désavoué par la Cour;

***SURVEILLANCE DE MASSE ET CADRE JURIDIQUE***

14. encourage la Commission à continuer de suivre de près l’utilisation de technologies de surveillance de masse au Royaume-Uni;

15. souligne que ni la loi californienne sur la protection de la vie privée des consommateurs ni aucun des projets de loi au niveau fédéral présentés jusqu’à présent aux États-Unis ne répondent aux critères du RGPD en matière de niveau adéquat de protection; encourage le législateur fédéral américain à adopter une loi nationale instaurant un cadre robuste et complet en matière de respect de la vie privée et de protection des données qui réponde à ces critères;

16. souligne qu’une telle législation en matière de protection des données et de la vie privée des consommateurs ne suffira pas à elle seule à résoudre les problèmes fondamentaux constatés par la Cour concernant la surveillance de masse menée par les services de renseignement des États-Unis ni l’accès insuffisant aux voies de recours; encourage le législateur fédéral américain à envisager de nouveau de modifier la section 702 de la loi FISA, le décret présidentiel nº 12333 et la directive présidentielle nº 28, en particulier en vue d’accorder le même niveau de protection aux citoyens de l’Union et des États-Unis;

***DÉCISIONS RELATIVES À L’ADÉQUATION***

17. demande à la Commission de prendre toutes les mesures qui s’imposent pour faire en sorte que tout accord à venir avec les États-Unis soit pleinement conforme au règlement (UE) 2016/679, à la charte et à tous les aspects de l’arrêt de la Cour;

18. rappelle que la Commission est tenue de réexaminer toutes les décisions relatives à l’adéquation adoptées au titre de la directive 95/46/CE en appliquant les conclusions des arrêts Schrems I et II pour évaluer si un niveau adéquat de protection essentiellement équivalent est garanti;

19. demande à la Commission de n’adopter aucune nouvelle décision constatant l’adéquation de la protection des données aux États-Unis, sauf si des réformes substantielles de la législation et de la pratique dans le domaine de l’accès aux informations par les pouvoirs publics ont lieu, en particulier en ce qui concerne l’accès à des fins de renseignement et de sécurité nationale;

20. demande à la Commission de publier une liste mise à jour des critères qu’elle prend en compte lorsqu’elle évalue si un pays tiers peut bénéficier d’une décision constatant l’adéquation de la protection des données;

21. charge son Président de transmettre la présente résolution à la Commission, au Conseil européen, au Conseil, au comité européen de la protection des données et aux parlements nationaux.

1. [https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62018CA0311&qid=1610640279033](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62018CA0311&qid=1610640279033) [↑](#footnote-ref-1)
2. [https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62014CJ0362](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62014CJ0362) [↑](#footnote-ref-2)
3. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62017CJ0623> [↑](#footnote-ref-3)
4. P8\_TA(2018)0315, <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_FR.html>. [↑](#footnote-ref-4)
5. P8\_TA(2018)0433, <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_FR.html>. [↑](#footnote-ref-5)
6. P9\_TA(2020)0337, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0337\_FR.html. [↑](#footnote-ref-6)
7. 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), JO L 119 du 4.5.2016, p. 1-88, [http://data.europa.eu/eli/reg/2016/679/oj](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679). [↑](#footnote-ref-7)
8. <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_fr>

   <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_fr> [↑](#footnote-ref-8)