Parlement européen
2019-2024

TEXTES ADOPTÉS

P9_TA(2021)0256

Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems («Schrems II») - Affaire C-311/18

Résolution du Parlement européen 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») (2020/2789(RSP))

Le Parlement européen,

– vu la charte des droits fondamentaux de l'Union européenne, et en particulier ses articles 7, 8, 16, 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* (ci-après «arrêt Schrems II»)[1],

– 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 «arrêt Schrems I»)[2],

– 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],

– 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 assurée par le bouclier de protection des données UE-États-Unis [5],

---

1 Arrêt de la Cour de justice du 16 juillet 2020, *Data Protection Commissioner*/*Facebook Ireland Ltd et Maximillian Schrems* C-311/18, ECLI:EU:C:2020:559.
2 Arrêt de la Cour de justice du 6 octobre 2015, *Maximillian Schrems*/*Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
3 Arrêt de la Cour de justice du 6 octobre 2020, *Privacy International*/*Secretary of State for Foreign and Commonwealth Affairs e.a.*, C-623/17, ECLI:EU:C:2020:790.
4 JO C 76 du 28.2.2018, p. 82.
5 JO C 298 du 23.8.2018, p. 73.

– vu sa résolution du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis[1],

– 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[2],

– vu la décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (notifiée sous le numéro C(2010) 593)[3],

– 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 (notifiée sous le numéro C(2016) 4176)[4],

– vu sa résolution du 26 novembre 2020 sur l'examen de la politique commerciale de l'Union[5],

– 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)[6], et notamment son article 45, paragraphe 3,

– vu la proposition de règlement de la Commission relative à la vie privée et aux 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, ainsi que la déclaration du comité européen de la protection des données du 19 novembre 2020 sur le règlement «vie privée et communications électroniques» et le rôle futur des autorités de contrôle et du comité européen de la protection des données,

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

A. 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

---

1 JO C 118 du 8.4.2020, p. 133.
2 JO C 345 du 16.10.2020, p. 58.
3 JO L 39 du 12.2.2010, p. 5.
4 JO L 207 du 1.8.2016, p. 1.
5 Textes adoptés de cette date, P9_TA(2020)0337.
6 JO L 119 du 4.5.2016, p. 1.

compétitivité économique; que ces transferts sont d'autant plus importants dans le contexte de la pandémie actuelle de COVID-19, puisqu'ils sont indispensables pour assurer la continuité des activités des entreprises et des pouvoirs publics, ainsi que des interactions sociales; qu'ils peuvent également soutenir des stratégies de sortie de la pandémie et contribuer à la relance économique;

B. considérant que la Cour de justice de l'Union européenne (ci-après «la Cour»), dans l'arrêt Schrems I, a invalidé la décision «sphère de sécurité» de la Commission en se fondant sur ses conclusions, et a argué 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»);

C. considérant que la Cour, dans l'arrêt Schrems II, a établi 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;

D. 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;

E. considérant que les données des citoyens européens stockées et transférées par les opérateurs de télécommunication et les entreprises constituent une ressource essentielle qui concourt aux intérêts stratégiques de l'Union;

F. considérant que la surveillance de masse et systématique par des acteurs étatiques nuit à la confiance des citoyens, des gouvernements et des entreprises d'Europe à l'égard des services numériques et, par extension, de l'économie numérique;

G. considérant que les organisations de défense des consommateurs et de la société civile disposent de ressources limitées et que l'application des droits et obligations en matière de données ne peuvent pas dépendre de leurs actions; que l'Union fait face à une mosaïque de procédures et pratiques nationales qui mettent à rude épreuve le mécanisme de coopération prévu dans le RGPD pour les plaintes transfrontières; qu'elle est confrontée à une lenteur générale des procédures, à un manque de ressources suffisantes pour les autorités de contrôle et, dans certains cas, à un manque de volonté ou d'utilisation efficace des ressources déjà allouées, que les plaintes s'accumulent concernant des infractions présumées commises par de grandes entreprises technologiques traitées par une autorité nationale unique, ce qui a généré un goulot d'étranglement en matière d'application;

H. considérant que les procédures qui ont conduit à cet arrêt de la Cour montrent également les difficultés que rencontrent les personnes dont les données sont traitées et les consommateurs au moment de défendre leurs droits, ce qui a un effet dissuasif sur leur capacité à défendre leurs droits devant l'autorité irlandaise de protection des données;

I. considérant que dans sa résolution du 25 octobre 2018, le Parlement européen,

soulignant que les États-Unis n'ont pas respecté le délai du 1er septembre 2018 pour se mettre en totale conformité avec le bouclier de protection des données, demandait déjà à la Commission de suspendre le bouclier de protection des données jusqu'à ce que les autorités des États-Unis respectent les dispositions de l'accord;

J. considérant que les droits des personnes dont les données sont traitées, garantis par la législation européenne sur la protection des données, devraient être respectés quel que soit le niveau de risque encouru dans le cadre du traitement des données à caractère personnel, notamment le transfert de ces données vers un pays tiers; que les responsables du traitement des données 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 et les finalités de ce traitement et les risques pour les personnes dont les données sont traitées;

K. considérant qu'à ce jour, malgré l'évolution considérable de la jurisprudence de la Cour au cours des cinq dernières années et l'application effective du RGPD depuis le 25 mai 2018, les autorités de contrôle n'ont pris aucune décision pour imposer des mesures correctives en matière de transferts de données à caractère personnel conformément au mécanisme de contrôle de la cohérence du RGPD; qu'aucune décision significative n'a été adoptée par les autorités de contrôle au niveau national pour imposer des mesures correctives ou des amendes en lien avec le transfert de données à caractère personnel vers des pays tiers;

L. considérant que, le jour même de sa prise de fonction, le président américain Joe Biden a désigné, au sein du ministère du commerce des États-Unis, le secrétaire adjoint aux services, qui sera le principal négociateur pour les transferts de données commerciales avec l'Union européenne; que la candidate du président au poste de secrétaire d'État américaine au commerce, Gina Raimondo, a réclamé la conclusion rapide des négociations sur un accord destiné à succéder au bouclier de protection des données en tant que «priorité absolue» lors d'une audition de confirmation devant le Sénat;

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/UE relative aux clauses contractuelles types (CCT), qui constituent le mécanisme le plus largement utilisé pour les transferts internationaux de données; prend acte, en outre, de l'annulation par la Cour de la décision (UE) 2016/1250 de la Commission relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis; relève que, à ce jour, aucun mécanisme durable garantissant le transfert légal de données à caractère personnel en vue d'un usage commercial entre l'Union et les États-Unis n'a résisté à un recours juridique devant la Cour de Justice de l'Union européenne;

2. prend acte du fait que la Cour a estimé que les CCT constituaient un mécanisme efficace pour garantir le respect du niveau de protection assuré dans l'Union, mais exige qu'un responsable du traitement/sous-traitant établi dans l'Union européenne et le destinataire de données à caractère personnel soient tenus de vérifier, avant tout transfert, que le niveau de protection requis par le droit de l'Union est bien respecté dans le pays tiers concerné; rappelle qu'il s'agit notamment d'évaluer le régime juridique régissant l'accès des autorités publiques aux données à caractère personnel,

afin de s'assurer que les personnes concernées et leurs données transférées ne risquent pas d'être soumises à des programmes de surveillance américains permettant la collecte massive de données à caractère personnel; fait observer que, lorsque le destinataire n'est pas en mesure de se conformer aux CCT, la Cour a jugé que les responsables du traitement ou les sous-traitants sont tenus de suspendre les transferts de données et/ou de résilier le contrat; relève toutefois que de nombreuses entreprises, en particulier des PME, ne disposent pas des connaissances ou des capacités nécessaires pour procéder à une telle vérification, ce qui pourrait perturber leurs activités;

3. est convaincu que l'arrêt de la Cour, qui met l'accent sur le niveau de protection des données garanti aux personnes concernées de l'Union dont les données ont été transférées aux États-Unis au titre du mécanisme du bouclier de protection des données, a également des implications pour les décisions relatives à l'adéquation de la protection des données dans d'autres pays tiers, Royaume-Uni inclus; réaffirme le besoin de clarté et de sécurité juridiques, étant donné que la capacité à transférer des données à caractère personnel par-delà les frontières en toute sécurité ne cesse de gagner en importance pour les particuliers en ce qui concerne la protection de leurs données à caractère personnel et leurs droits, ainsi que pour tous les types d'organisations qui fournissent des biens et des services à l'échelon international eu égard au régime juridique dans lequel elles exercent leurs activités; souligne, toutefois, que jusqu'à leur révocation, leur remplacement ou leur invalidation par la Cour, les décisions d'adéquation existantes restent en vigueur;

4. regrette que le commissaire irlandais à la protection des données ait assigné Maximilian Schrems et Facebook en justice devant la Haute Cour irlandaise, alors qu'il aurait pu prendre une décision dans le cadre des pouvoirs que lui confèrent l'article 4 de la décision 2010/87/UE et l'article 58 du RGPD; rappelle toutefois que le commissaire irlandais à la protection des données a utilisé la voie légale d'accès qui autorise les autorités de protection des données à porter leurs doutes quant à la validité d'une décision d'exécution de la Commission à l'attention d'un juge national en vue de saisir la Cour d'un renvoi préjudiciel; se dit fortement préoccupé par le fait que le commissaire irlandais à la protection des données n'ait pas encore tranché sur plusieurs réclamations concernant des infractions au RGPD déposées le 25 mai 2018, date de l'entrée en vigueur du RGPD, pas plus que sur d'autres plaintes émanant de groupes de consommateurs et autres alors qu'il est l'autorité compétente au premier chef pour ces affaires; craint que le commissaire à la protection des données n'interprète les termes «sans tarder», à l'article 60, paragraphe 3, du RGPD, contrairement à l'intention du législateur, comme correspondant à plus de quelques mois; s'inquiète que les autorités de contrôle n'aient pas pris de mesures proactives au titre des articles 61 et 66 du RGPD pour obliger l'autorité irlandaise de protection des données à respecter ses obligations en vertu du RGPD; est tout aussi préoccupé par le nombre insuffisant d'experts en technologies travaillant pour l'autorité de protection des données et par l'utilisation de systèmes obsolètes; déplore les implications de la tentative infructueuse de l'autorité de protection des données de faire supporter à une partie défenderesse 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;

5. s'inquiète du niveau insuffisant d'application du RGPD, notamment dans le domaine des transferts internationaux; exprime sa préoccupation face à l'absence de hiérarchisation et de supervision globale par les autorités de contrôle nationales en ce qui concerne les transferts de données à caractère personnel vers des pays tiers, malgré

l'évolution considérable de la jurisprudence de la Cour ces cinq dernières années; déplore l'absence de décisions et de mesures correctives pertinentes à cet égard et prie instamment le comité européen de la protection des données et les autorités de contrôle nationales d'inclure les transferts de données à caractère personnel dans leurs stratégies d'audit, de conformité et d'application; souligne que des procédures administratives contraignantes harmonisées en matière de représentation des personnes dont les données sont traitées et d'admissibilité sont nécessaires pour garantir la sécurité juridique et traiter les plaintes transfrontières;

6. prend acte du projet de décision d'exécution de la Commission sur les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers; prie instamment le comité européen de la protection des données de publier d'autres orientations sur les transferts internationaux de données pour les entreprises, en particulier pour les PME, qui incluent une liste de contrôle pour l'évaluation des transferts, des outils permettant de déterminer si les gouvernements sont autorisés à accéder à des données, ou s'ils disposent de la capacité de le faire, et des informations sur les mesures supplémentaires requises pour les transferts au moyen de CCT; invite le comité européen de la protection des données à solliciter également les contributions d'universitaires indépendants sur les législations nationales des principaux partenaires commerciaux, qui pourraient être contradictoires;

7. rappelle que, conformément aux lignes directrices 2/2018[1] du comité européen de la protection des données relatives aux dérogations à l'article 49 du règlement (UE) 2016/679, lorsque les transferts ont lieu en dehors du cadre de décisions constatant le caractère adéquat du niveau de protection ou d'autres instruments offrant des garanties appropriées, mais qu'ils se fondent sur des dérogations pour des situations spécifiques en vertu de l'article 49 du RGPD, ils doivent être interprétés strictement de sorte que l'exception ne devienne pas la règle; observe toutefois que, depuis l'invalidation du bouclier de protection des données UE-États-Unis, les flux transatlantiques de données ont été maintenus à des fins de publicité numérique malgré des doutes quant à la base juridique des transferts à des fins publicitaires; invite le comité européen de la protection des données et les autorités de protection des données à garantir une interprétation cohérente dans le cadre de l'application et du contrôle de ces dérogations, conformément aux lignes directrices du comité européen de la protection des données;

8. se réjouit des discussions au niveau international sur des flux transfrontières de données à caractère personnel conformes au RGPD et à la directive en matière de protection des données dans le domaine répressif[2]; souligne que le RGPD, la directive «grands risques», les règles concernant la vie privée et les autres mesures en vigueur et à venir protégeant les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ne doivent pas être menacés par des accords commerciaux internationaux ou y être intégrés; demande instamment à la Commission

---

1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf

2 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 (JO L 119 du 4.5.2016, p. 89).

de respecter la position horizontale de 2018[1] de l'Union et de ne pas s'en écarter, ainsi que de prendre en considération les engagements correspondants des pays tiers au titre du droit commercial au moment d'évaluer leur adéquation, notamment pour les transferts à venir de données;

Clauses contractuelles types

9. 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 en ce moment les parties prenantes dans le cadre d'une consultation publique sur ce projet; note que le comité européen de la protection des données et le contrôleur européen de la protection des données, dans un avis conjoint publié le 15 janvier 2021[2], ont émis des commentaires positifs au sujet des propositions de clauses contractuelles types, mais ont proposé plusieurs améliorations; attend de la Commission qu'elle prenne en considération les avis reçus avant de lancer la procédure de comité;

10. rappelle qu'un grand nombre de PME ont recours à des clauses contractuelles types; souligne que toutes les entreprises ont un besoin urgent de lignes directrices claires et d'une aide, de sorte à garantir la sécurité juridique lors de l'application et de l'interprétation de l'arrêt de la Cour;

11. prend acte des recommandations 01/2020[3] 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; se réjouit que le comité européen de la protection des données ait organisé une consultation publique au sujet de ses recommandations; se dit préoccupé par les potentielles dissonances entre ces recommandations et la proposition de la Commission relative aux clauses contractuelles types; invite la Commission et le comité européen de la protection des données à coopérer en vue de finaliser leurs documents respectifs, afin de garantir la sécurité juridique conformément à l'arrêt de la Cour; estime que la Commission doit suivre les orientations du comité européen de la protection des données;

12. se félicite en particulier des recommandations du comité européen de la protection des données concernant la nécessité, pour les responsables du traitement, de s'appuyer sur des facteurs objectifs pour déterminer si des éléments de la législation ou de la pratique du pays tiers peuvent affecter l'efficacité des garanties appropriées des outils de transfert en ce qui concerne les transferts en question plutôt que sur des facteurs

---

1 Proposition de dispositions de l'Union relatives aux flux de données transfrontières et à la protection des données à caractère personnel et de la vie privée, http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf

2 Avis conjoint 2/2021 du comité européen de la protection des données et du contrôleur européen de la protection des données sur les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers du 14 janvier 2021: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

3 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 du 11 novembre 2020, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_fr

subjectifs, tels que la probabilité que les autorités publiques aient accès aux données d'une manière non conforme aux normes de l'Union, qui ont été rejetées à plusieurs reprises par la Cour; demande à cet égard à la Commission de veiller à ce que sa proposition relative aux clauses contractuelles types soit pleinement conforme à la jurisprudence applicable de la Cour;

13. estime crucial que les entreprises actives dans l'Union qui transfèrent des données nominatives hors 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 du comité européen de la protection des données; se dit favorable à la création d'une boîte à outils de mesures supplémentaires, comme une certification de sécurité et de protection des données ou des garanties en matière de chiffrement et de pseudonymisation, acceptées par les autorités de réglementation, et à des ressources accessibles au public sur la législation pertinente des principaux partenaires commerciaux de l'Union;

14. 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; espère que, si aucun accord n'est trouvé rapidement avec les États-Unis pour garantir un niveau de protection adéquat essentiellement équivalent à celui offert par le RGPD et la charte, ces transferts seront suspendus jusqu'à ce que la situation soit résolue; souligne la conclusion de la Cour selon laquelle ni l'article 702 de la FISA ni le décret présidentiel nº 12333 (JO 12333), lu en combinaison avec la directive présidentielle nº 28 (PPD-28), ne correspondent aux garanties minimales découlant, en droit de l'Union, du principe de proportionnalité, de sorte que les programmes de surveillance fondés sur ces dispositions ne peuvent être considérés comme limités à ce qui est strictement nécessaire; souligne qu'il est nécessaire de résoudre les problèmes soulevés par l'arrêt de la Cour de manière durable pour assurer une protection des données à caractère personnel des personnes concernées; rappelle qu'aucun contrat entre entreprises n'est à même d'offrir une protection contre l'accès indiscriminé, par les services de renseignement, au contenu des communications électroniques, pas plus qu'un contrat entre entreprises n'offre suffisamment de voies de recours judiciaires contre la surveillance de masse; soulève que cela suppose obligatoirement une réforme des lois et pratiques américaines en matière de surveillance, afin de garantir que l'accès des autorités américaines responsables de la sécurité aux données transférées depuis l'Union est limité à ce qui est nécessaire et proportionné et que les citoyens européens dont les données sont traitées puissent introduire des recours juridictionnels effectifs devant les tribunaux des États-Unis;

15. souligne que les PME européennes, ainsi que les organisations et associations à but non lucratif, disposent d'un pouvoir de négociation et de capacités juridiques et financières limités, alors qu'on attend d'elles qu'elles évaluent en autonomie l'adéquation de la protection des données dans des pays tiers, ce qui implique d'appréhender les cadres juridiques complexes de divers pays tiers; invite instamment la Commission et le comité européen de la protection des données à fournir des orientations en ce qui concerne l'utilisation pratique de mesures supplémentaires fiables, en particulier pour les PME;

16. prie instamment les autorités chargées de la protection des données de respecter leurs obligations, soulignées dans l'arrêt de la Cour, de veiller à une application correcte et rapide du RGPD en surveillant étroitement le recours aux CCT; invite les autorités chargées de la protection des données à aider les entreprises à se conformer à la jurisprudence de la Cour; somme également les autorités de contrôle nationales d'exercer tous les pouvoirs d'enquête et de correction que leur confère l'article 58 du RGPD dans les cas où les exportateurs de données transfèrent des données à caractère personnel en dépit de l'existence de lois dans le pays tiers de destination empêchant l'importateur de données de se conformer aux clauses contractuelles types, et l'absence de mesures supplémentaires efficaces; rappelle que la Cour a indiqué que chaque autorité de contrôle est «tenue de s'acquitter [...] de sa mission consistant à veiller au plein respect du RGPD»;

Bouclier de protection des données

17. relève que 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 de l'accès massif des pouvoirs publics des États-Unis aux données à caractère personnel transférées dans le cadre du bouclier de protection des données, qui ne respecte pas les principes de nécessité et de proportionnalité, 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 ou toute autre autorité indépendante remplissant la fonction d'un tribunal; s'attend à ce que l'administration américaine actuelle s'applique davantage à respecter ses obligations dans le cadre d'éventuels futurs mécanismes de transfert que les administrations précédentes, qui ont fait preuve d'un manque d'engagement politique à respecter et à faire respecter les règles de la sphère de sécurité, ainsi qu'à faire respecter les règles du bouclier de protection des données;

18. fait observer que, en réaction à l'arrêt Schrems II, certaines entreprises ont revu à la hâte leurs déclarations de protection des données et leurs contrats avec des tiers eu égard à leurs engagements au titre du bouclier de protection des données sans évaluer les mesures les plus pertinentes pour transférer les données en toute légalité;

19. regrette que, malgré les nombreux appels adressés à la Commission par le Parlement dans ses résolutions de 2016, de 2017 et de 2018 afin qu'elle prenne toutes les mesures nécessaires pour s'assurer que le bouclier de protection des données respecte pleinement le RGPD et la charte, la Commission n'ait pas agi conformément à l'article 45, paragraphe 5, du RGPD; déplore que la Commission ait ignoré la demande du Parlement l'invitant à suspendre le bouclier de protection des données jusqu'à ce que les autorités américaines respectent les dispositions de ce cadre, dans laquelle il insistait sur le risque de voir le bouclier de protection des données invalidé par la Cour; rappelle que les problèmes liés au fonctionnement du bouclier de protection des données ont été soulevés à plusieurs reprises par le groupe de travail «article 29» et le comité européen de la protection des données;

20. regrette que la Commission fasse passer les relations avec les États-Unis avant les intérêts des citoyens de l'Union et qu'elle laisse dès lors le soin à des citoyens individuels de défendre le droit de l'Union;

Surveillance de masse et cadre juridique

21. encourage la Commission à suivre de manière proactive l'utilisation de technologies de surveillance de masse aux États-Unis et dans d'autres pays tiers qui font ou feraient l'objet d'un constat d'adéquation, comme le Royaume-Uni; prie instamment la Commission de n'adopter aucune décision constatant l'adéquation de la protection des données pour les pays où les lois et les programmes relatifs à la surveillance de masse ne satisfont pas aux critères de la Cour, dans l'esprit ou dans la lettre;

22. prend acte de la récente entrée en vigueur, aux États-Unis, de la loi californienne sur la protection de la vie privée des consommateurs; prend note des discussions et des propositions législatives connexes au niveau fédéral; souligne que, même si elles constituent des avancées dans la bonne direction, ni la loi californienne sur la protection de la vie privée des consommateurs ni aucun des projets de loi au niveau fédéral présentés aux États-Unis ne répondent pour l'heure aux critères du RGPD en matière de constat d'adéquation; encourage vivement le législateur américain à adopter un acte législatif qui réponde à ces exigences et contribue ainsi à garantir que le droit américain offre un niveau de protection essentiellement équivalent à celui qui est actuellement garanti dans l'Union;

23. 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 modifier la section 702 de la loi FISA, et le président américain à modifier le décret présidentiel nº 12333 et la directive présidentielle nº 28, en particulier en ce qui concerne la surveillance de masse et l'octroi du même niveau de protection aux citoyens de l'Union et des États-Unis; encourage les États-Unis à mettre en place des mécanismes pour garantir que les citoyens reçoivent des notifications (différées) et puissent contester toute surveillance inappropriée au titre de la section 702 et du décret présidentiel nº 12333, de même qu'un mécanisme conscacré par la loi pour garantir que les non-ressortissants américains jouissent de droits opposables en dehors du «Judicial Redress Act» (loi sur le recours juridictionnel);

24. rappelle que les États membres continuent d'échanger des données à caractère personnel avec les États-Unis au titre du programme de surveillance du financement du terrorisme, de l'accord entre l'Union européenne et les États-Unis sur les dossiers passagers (données PNR) ou encore des accords intergouvernementaux mettant en œuvre la loi relative au respect des obligations fiscales concernant les comptes étrangers (FATCA), qui a des effets néfastes sur les «Américains accidentels», comme cela est évoqué dans la résolution du Parlement du 5 juillet 2018 sur les effets néfastes de la loi des États-Unis relative au respect des obligations fiscales concernant les comptes étrangers sur les citoyens de l'Union européenne, et en particulier les «Américains accidentels»[1]; rappelle que les États-Unis ont encore accès aux bases de données des services répressifs des États membres, qui contiennent les empreintes digitales et les données ADN des citoyens de l'Union; demande à la Commission d'étudier les incidences des arrêts Schrems I et II sur ces échanges de données et de présenter son analyse et la manière dont elle entend rendre ces échanges conformes aux arrêts, lors d'une audition publique et par écrit, à la commission des libertés civiles, de la justice et des affaires intérieures d'ici le 30 septembre 2021;

---

1 JO C 118 du 8.4.2020, p. 141.

25. invite également la Commission à analyser la situation des fournisseurs d'informatique dans le cloud relevant de la section 702 du FISA et qui opèrent des transferts de données au moyen de CCT; demande en outre à la Commission d'examiner les effets sur les droits accordés au titre de l'accord-cadre entre l'Union et les États-Unis, notamment le droit au recours juridictionnel, compte tenu du fait que les États-Unis n'accordent ce droit de manière explicite qu'aux citoyens de pays désignés qui autorisent les transferts de données vers les États-Unis à des fins commerciales; estime inacceptable que la Commission n'ait toujours pas publié ses conclusions sur le premier examen conjoint de l'accord-cadre, un an après l'échéance, et l'invite, si nécessaire, à rendre sans tarder l'accord conforme aux normes établies par les arrêts de la Cour;

26. juge nécessaire, au regard des lacunes caractérisées en matière de protection des données de citoyens européens transférées aux États-Unis, de soutenir l'investissement dans des outils européens de conservation des données (ex. service cloud) pour réduire la dépendance de l'Union en capacités de stockage vis-à-vis des pays tiers et pour renforcer l'autonomie stratégique de l'Union en matière de gestion et de protection des données;

Décisions d'adéquation

27. demande à la Commission de prendre toutes les mesures qui s'imposent pour faire en sorte que toute nouvelle décision relative à l'adéquation de la protection des données aux États-Unis soit pleinement conforme au règlement (UE) 2016/679, à la charte et à tous les aspects des arrêts de la Cour; rappelle que les cadres d'adéquation favorisent considérablement l'activité économique, en particulier pour les PME et les jeunes entreprises, qui, contrairement aux grandes entreprises, ne disposent souvent pas des capacités financières, juridiques et techniques nécessaires pour utiliser d'autres outils de transfert; invite les États membres à conclure des accords de non-espionnage avec les États-Unis; appelle la Commission à profiter de ses contacts avec ses homologues américains pour faire passer le message selon lequel, en l'absence de modification des lois et pratiques de surveillance des États-Unis, la seule option envisageable pour faciliter une décision d'adéquation à l'avenir consisterait à conclure des accords de «non-espionnage» avec les États membres;

28. estime qu'aucune décision d'adéquation future de la Commission ne devrait s'appuyer sur un système d'autocertification, comme c'était le cas pour la sphère de sécurité et le bouclier de protection des données; invite la Commission à associer pleinement le comité européen de la protection des données à la surveillance de la conformité de toute nouvelle décision relative à l'adéquation de la protection des données en lien avec les États-Unis, ainsi que de son application; demande à la Commission de convenir avec l'administration américaine des mesures nécessaires pour permettre au comité européen de la protection des données de mener cette tâche à bien; attend de la Commission qu'elle accorde davantage de poids à l'avis du Parlement au sujet de toute nouvelle décision relative à l'adéquation de la protection des données en lien avec les États-Unis avant d'adopter une telle décision;

29. rappelle que la Commission réexamine actuellement toutes les décisions relatives à l'adéquation adoptées au titre de la directive 95/46/CE; souligne que la Commission devrait appliquer les normes les plus strictes établies par le RGPD et par la CJUE dans ses arrêts «Schrems I et II» afin d'évaluer si un niveau de protection substantiellement équivalent à celui garanti par le RGPD, notamment en ce qui concerne l'accès à un

recours effectif et la protection contre l'accès indu des autorités du pays tiers aux données à caractère personnel, est accordé; prie instamment la Commission de clôturer de toute urgence ces réexamens et de révoquer ou de suspendre toute décision antérieure au RGPD dès lors qu'elle établit que le pays tiers en question n'offre pas un niveau de protection essentiellement équivalent et qu'aucune solution ne peut être trouvée à cette situation;

30. estime que l'administration Biden, par la désignation d'un expert rompu aux questions de vie privée en tant que négociateur en chef pour le système destiné à succéder au bouclier de protection des données, a montré sa volonté de parvenir en priorité à une solution pour les transferts de données commerciales entre l'Union européenne et les États-Unis; s'attend à ce que le dialogue entre la Commission et les autorités américaines compétentes, qui a débuté directement après l'arrêt de la Cour, s'intensifie au cours des prochains mois;

31. 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 sont adoptées, en particulier dans le domaine de l'accès à des fins de sécurité nationale et de renseignement, ce qui peut advenir au moyen de réformes claires, juridiquement viables, applicables et non discriminatoires du droit et des pratiques des États-Unis en la matière; rappelle, à cet égard, l'importance de garanties solides dans le domaine de l'accès aux données à caractère personnel par les autorités publiques; invite la Commission à concrétiser ses «ambitions géopolitiques» pour imposer aux États-Unis et dans d'autres pays tiers une protection des données essentiellement équivalente à celle de l'Union;

32. recommande aux autorités nationales de protection des données de suspendre le transfert de données à caractère personnel susceptibles d'être accessibles aux autorités publiques américaines si la Commission devait adopter une nouvelle décision relative à l'adéquation de la protection des données en lien avec les États-Unis en l'absence de telles réformes substantielles;

33. se félicite que la Commission respecte les critères établis dans le cadre du groupe de travail «Article 29» sur les critères de référence en matière d'adéquation au titre du RGPD[1] (tels qu'approuvés par le comité européen de la protection des données) et dans les recommandations 01/2021 du comité européen de la protection des données sur les critères de référence en matière d'adéquation au titre de la directive en matière répressive[2]; estime que la Commission ne devrait pas se soustraire à ces critères lorsqu'elle évalue si un pays tiers remplit les conditions pour bénéficier d'une décision d'adéquation; prend note du fait que le comité européen de la protection des données a récemment mis à jour ses recommandations relatives aux garanties essentielles concernant les mesures de surveillance, à la lumière de la jurisprudence de la Cour[3];

---

1 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

2 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_fr

3 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr

°

° °

34. charge son Président de transmettre la présente résolution à la Commission, au Conseil européen, au Conseil de l'Union européenne, au comité européen de la protection des données, aux parlements nationaux des États membres, au Congrès et au gouvernement des États-Unis d'Amérique ainsi qu'au Parlement et au gouvernement du Royaume-Uni.