

ARRÊT DU TRIBUNAL (dixième chambre élargie)

3 septembre 2025 (*)

« Transfert de données à caractère personnel vers les États-Unis – Décision d'exécution de la Commission constatant l'adéquation du niveau de protection des données à caractère personnel assuré par les États-Unis – Droit à un recours effectif – Droit à la vie privée et familiale – Décisions fondées exclusivement sur le traitement automatisé des données à caractère personnel – Sécurité du traitement des données à caractère personnel »

Dans l'affaire T-553/23,

Philippe Latombe, demeurant à Nantes (France), représenté par M^{es} N. Coutrelis, J.-B. Soufron et T. Lamballe, avocats,

partie requérante,

contre

Commission européenne, représentée par MM. D. Calleja Crespo, A. Bouchagiar, H. Kranenborg et C. Ladenburger, en qualité d'agents,

partie défenderesse,

soutenue par

Irlande, représentée par M^{mes} M. Browne, S. Finnegan et M. A. Joyce, en qualité d'agents, assistés de M. S. Brittain, barrister, et de M^{me} C. Donnelly, SC,

et par

États-Unis d'Amérique, représentés par MM. B. Walsh, S. Barton et A. Finlay, solicitors, M^{me} E. Barrington, SC, et M. D. Hardiman, barrister,

parties intervenantes,

LE TRIBUNAL (dixième chambre élargie),

composé de M^{me} O. Porchia, présidente, MM. M. Jaeger (rapporteur), L. Madise, P. Nihoul et S. Verschuur, juges,

greffier : M^{me} I. Kurme, administratrice,

vu l'ordonnance du 12 octobre 2023, Latombe/Commission (T-553/23 R, non publiée, EU:T:2023:621),

vu la phase écrite de la procédure,

à la suite de l'audience du 1^{er} avril 2025,

rend le présent

Arrêt

1 Par son recours fondé sur l'article 263 TFUE, le requérant, M. Philippe Latombe, demande, en substance, l'annulation de la décision d'exécution (UE) 2023/1795 de la Commission, du 10 juillet 2023, constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis (JO 2023, L 231, p. 118, ci-après la « décision attaquée »).

I. Antécédents du litige

2 Le requérant est un citoyen français qui allègue utiliser diverses plateformes informatiques collectant ses données à caractère personnel et les transférant aux États-Unis.

3 S'agissant du transfert de données à caractère personnel depuis l'Union européenne vers les États-Unis, dans un premier temps, par l'arrêt du 6 octobre 2015, Schrems (C-362/14, ci-après l'« arrêt Schrems I », EU:C:2015:650), la Cour a déclaré invalide la décision 2000/520/CE 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 (JO 2000, L 215, p. 7).

4 Dans un second temps, par l'arrêt du 16 juillet 2020, Facebook Ireland et Schrems (C-311/18, ci-après l'« arrêt Schrems II », EU:C:2020:559), la Cour a déclaré invalide la décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE – États-Unis (JO 2016, L 207, p. 1, ci-après la « décision d'adéquation concernant le bouclier de protection »).

5 Dans les arrêts Schrems I et Schrems II, la Cour, saisie par un renvoi préjudiciel en appréciation de validité, a estimé notamment que, contrairement à l'appréciation de la Commission européenne ressortant des décisions d'adéquation mentionnées aux points 3 et 4 ci-dessus, le système de la sphère de sécurité et le système du bouclier de protection des données (ci-après le « bouclier de protection ») régissant le transfert de données à caractère personnel ne garantissaient pas un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti par le droit de l'Union.

6 À la suite de l'arrêt Schrems II, la Commission a entamé des pourparlers avec le gouvernement des États-Unis en vue d'adopter une éventuelle nouvelle décision d'adéquation qui respecterait les exigences de l'article 45, paragraphe 2, du 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 (règlement général sur la protection des données) (JO 2016, L 119, p. 1, rectificatif JO 2018, L 127, p. 2, ci-après le « RGPD »), telles qu'elles ont été interprétées par la Cour.

7 Ainsi, le 7 octobre 2022, les États-Unis d'Amérique ont adopté l'Executive Order 14086 (décret présidentiel n° 14086, ci-après l'« E.O. 14086 »), qui renforce les mesures de protection de la vie privée régissant les activités de renseignement d'origine électromagnétique menées par les agences de renseignements établies aux États-Unis. Ce décret a été complété par l'Attorney General Order No. 5517–2022 (règlement du procureur général n° 5517–2022, ci-après le « règlement AG »), qui a ajouté la partie 201 au titre 28 du Code of Federal Regulations (CFR, Code des règlements fédéraux), encadrant la création et le fonctionnement de la Data Protection Review Court (Cour chargée du contrôle de la protection des données, ci-après la « DPRC »).

8 Le 10 juillet 2023, après examen de ces évolutions réglementaires aux États-Unis, la Commission a adopté, sur le fondement de l'article 45, paragraphe 3, du RGPD, la décision attaquée, qui met en place le nouveau cadre transatlantique de flux de données à caractère personnel entre l'Union et les États-Unis. L'article 1^{er} de ladite décision déclare que les États-Unis d'Amérique assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies dans ce pays et figurant sur la liste du « cadre de protection des données UE – États-Unis » (ci-après le « CPD ») tenue à jour et publiée par leur ministère du Commerce (ci-après les « organisations du CPD »).

II. Conclusions des parties

9 Le requérant conclut à ce qu'il plaise au Tribunal :

- annuler la décision attaquée, en substance, dans son entièreté ;
- condamner la Commission aux dépens.

10 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conclut à ce qu'il plaise au Tribunal :

- rejeter le recours comme étant irrecevable ;
- à titre subsidiaire, rejeter le recours comme étant non fondé ;
- condamner le requérant aux dépens.

III. En droit

A. Sur l'exception d'irrecevabilité

11 Par acte séparé déposé au greffe du Tribunal le 1^{er} décembre 2023, la Commission a soulevé une exception d'irrecevabilité, sur le fondement de l'article 130 du règlement de procédure du Tribunal.

12 La Commission fait valoir que le recours est irrecevable, au motif que le requérant n'a pas la qualité pour agir, qu'il n'a pas d'intérêt à agir et que la partie de la décision attaquée dont il demande l'annulation est indissociable du reste de cette décision.

13 Le requérant conteste les arguments de la Commission et soutient que son recours est recevable.

14 Il convient de rappeler que le juge de l'Union est en droit d'apprécier, suivant les circonstances de chaque espèce, si une bonne administration de la justice justifie de rejeter au fond un recours, sans statuer préalablement sur sa recevabilité (voir, en ce sens, arrêt du 26 février 2002, Conseil/Boehringer, C-23/00 P, EU:C:2002:118, points 51 et 52).

15 Ainsi, compte tenu des circonstances de la présente affaire, le Tribunal estime que le recours étant, en tout état de cause et pour les motifs exposés aux points 16 à 204 ci-après, dépourvu de fondement, il y a lieu, dans un souci de bonne administration de la justice, d'examiner son bien-fondé, sans statuer préalablement sur sa recevabilité (voir, en ce sens, arrêts du 10 octobre 2014, Marchiani/Parlement, T-479/13, non publié, EU:T:2014:866, point 23, et du 20 décembre 2023, Naturstrom/Commission, T-60/21, non publié, EU:T:2023:839, point 74).

B. Sur le fond

16 Au soutien du recours, le requérant invoque cinq moyens, tirés :

- le premier, de la violation des articles 3 et 4 du règlement n° 1/1958 du Conseil, du 15 avril 1958, portant fixation du régime linguistique de la Communauté économique européenne (JO 1958, 17, p. 385) ;
- le deuxième, de la violation des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne ;
- le troisième, de la violation de l'article 47, deuxième alinéa, de ladite charte et de l'article 45, paragraphe 2, du RGPD ;
- le quatrième, de la violation de l'article 22 du RGPD ;

– le cinquième, de la violation de l'article 32 du RGPD, lu en combinaison avec l'article 45, paragraphe 2, du même règlement.

17 Lors de l'audience, le requérant a renoncé à son premier moyen, portant sur la violation des articles 3 et 4 du règlement n° 1/1958. Il convient donc d'examiner uniquement ses deuxième à cinquième moyens.

1. Observations liminaires

18 En premier lieu, il convient de noter que l'article 45, paragraphe 1, du RGPD prévoit qu'un transfert de données à caractère personnel vers un pays tiers peut être autorisé par une décision de la Commission selon laquelle ce pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans celui-ci assurent un niveau de protection adéquat. Cette disposition est incluse dans le chapitre V dudit règlement qui, comme cela a été indiqué par la Cour, vise globalement à assurer la continuité du niveau élevé de protection des données à caractère personnel, qui est garanti par le droit de l'Union en vertu de ce règlement, lorsque celles-ci sont transférées vers un pays tiers (voir, en ce sens, arrêt Schrems II, point 93).

19 À cet égard, la Cour a précisé que, sans exiger que le pays tiers concerné garantisse un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union, l'expression « niveau de protection adéquat », figurant à l'article 45, paragraphe 1, du RGPD, devait être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu dudit règlement, lu à la lumière de la charte des droits fondamentaux (voir, en ce sens, arrêt Schrems II, points 94 et 162).

20 La Cour a également jugé que, même si les moyens auxquels le pays tiers avait recours pour assurer un niveau adéquat de protection des données à caractère personnel pouvaient être différents de ceux mis en œuvre au sein de l'Union afin de garantir le respect des exigences découlant de la directive 95/46, lue à la lumière de la charte des droits fondamentaux, ces moyens devaient néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union (arrêt Schrems I, point 74).

21 En outre, la Cour a considéré que, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, du nombre important de personnes dont les droits fondamentaux sont susceptibles d'être violés en cas de transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat, le pouvoir d'appréciation de la Commission quant au caractère adéquat du niveau de protection assuré par un pays tiers s'aurait réduit, de sorte qu'il y avait lieu, pour le juge de l'Union, de procéder à un contrôle strict de la légalité d'une décision d'adéquation (arrêt Schrems I, point 78).

22 En second lieu, il convient de rappeler que, selon une jurisprudence constante, la légalité d'un acte de l'Union doit être appréciée en fonction des éléments de fait et de droit existant à la date où cet acte a été adopté, de telle sorte que des actes postérieurs à l'adoption d'une décision ne peuvent affecter la validité de celle-ci (voir arrêts du 17 octobre 2019, *Alcogroup et Alcodis/Commission*, C-403/18 P, EU:C:2019:870, point 45 et jurisprudence citée, et du 28 janvier 2021, *Qualcomm et Qualcomm Europe/Commission*, C-466/19 P, EU:C:2021:76, point 82 et jurisprudence citée). Dès lors, en l'espèce, les appréciations effectuées par la Commission concernant la légalité de la décision attaquée doivent être examinées en fonction des seuls éléments dont elle disposait au moment où elle les a effectuées.

23 C'est dans ce contexte qu'il convient d'analyser les moyens soulevés par le requérant en examinant d'abord le troisième moyen, puis le deuxième moyen, ensuite le quatrième moyen et enfin le cinquième moyen.

2. Sur le troisième moyen, tiré de la violation de l'article 47, deuxième alinéa, de la charte des droits fondamentaux et de l'article 45, paragraphe 2, du RGPD

- 24 Par son troisième moyen, le requérant soutient que la Commission a violé l'article 47, deuxième alinéa, de la charte des droits fondamentaux et l'article 45, paragraphe 2, du RGPD, dès lors que, dans la décision attaquée, elle a considéré que la DPRC offrait un niveau de protection adéquat en ce qui concernait le droit des citoyens de l'Union à accéder à un tribunal indépendant et impartial établi préalablement par la loi.
- 25 À titre liminaire, il convient de relever que les termes de l'article 47, deuxième alinéa, de la charte des droits fondamentaux sont les suivants :
- « Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. »
- 26 Selon les explications relatives à la charte des droits fondamentaux (JO 2007, C 303, p. 17), l'article 47, deuxième alinéa, de ladite charte correspond à l'article 6, paragraphe 1, de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »). Les termes de cette dernière disposition sont les suivants :
- « Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. »
- 27 À cet égard, il y a lieu de rappeler que, selon la jurisprudence, dès lors que la CEDH ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union, l'examen de la validité d'un acte de droit dérivé doit être opéré au regard uniquement des droits fondamentaux garantis par la charte des droits fondamentaux (arrêt du 3 septembre 2015, *Inuit Tapiriit Kanatami e.a./Commission*, C-398/13 P, EU:C:2015:535, points 45 et 46).
- 28 Cependant, la jurisprudence reconnaît que, d'une part, en vertu de l'article 6, paragraphe 3, TUE, les droits fondamentaux reconnus par la CEDH font partie du droit de l'Union en tant que principes généraux et, d'autre part, il découle de l'article 52, paragraphe 3, de la charte des droits fondamentaux que les droits contenus dans celle-ci, correspondant à des droits garantis par la CEDH, ont le même sens et la même portée que ceux que leur confère la CEDH (voir arrêt du 31 mai 2018, *Korwin-Mikke/Parlement*, T-770/16, EU:T:2018:320, point 38 et jurisprudence citée).
- 29 Par conséquent, selon la jurisprudence, dans un souci de cohérence et sans que cela porte atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne, les droits contenus dans la charte des droits fondamentaux qui correspondent à ceux garantis par la CEDH doivent aussi être interprétés à la lumière de la jurisprudence de la Cour européenne des droits de l'homme (ci-après la « Cour EDH ») [voir, en ce sens, arrêts du 9 novembre 2023, *Staatssecretaris van Justitie en Veiligheid* (Notion d'atteintes graves), C-125/22, EU:C:2023:843, point 59, et du 31 mai 2018, *Korwin-Mikke/Parlement*, T-770/16, EU:T:2018:320, point 38].
- 30 Il s'ensuit, selon la jurisprudence, que la Cour doit veiller, au titre de l'article 52, paragraphe 3, de la charte des droits fondamentaux, à ce que l'interprétation qu'elle effectue de l'article 47, deuxième alinéa, de ladite charte assure un niveau de protection qui ne méconnaît pas celui garanti à l'article 6, paragraphe 1, de la CEDH, tel qu'il est interprété par la Cour EDH [voir arrêt du 6 octobre 2021, *W.Ż.* (Chambre de contrôle extraordinaire et des affaires publiques de la Cour suprême – Nomination), C-487/19, EU:C:2021:798, point 123 et jurisprudence citée].
- 31 Il y a également lieu de noter que l'article 45, paragraphe 2, du RGPD prévoit que, lorsqu'elle évalue le caractère adéquat du niveau de protection offert par un pays tiers, la Commission tient compte, en particulier, des éléments suivants :
- « a) [...] les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

- b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres ».

32 C'est au regard de ces éléments qu'il convient d'examiner les deux griefs soulevés par le requérant au soutien du présent moyen.

a) *Sur le premier grief du troisième moyen, selon lequel la DPRC n'est pas un tribunal indépendant et impartial*

33 Par le premier grief de son troisième moyen, le requérant soutient que la DPRC n'est pas un tribunal indépendant et impartial au sens de l'article 47, deuxième alinéa, de la charte des droits fondamentaux, mais un organe parajudictionnel dépendant du pouvoir exécutif.

34 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

35 À titre liminaire, il convient de relever que, selon la jurisprudence, l'exigence d'indépendance des juridictions, qui est inhérente à la mission de juger, relève du contenu essentiel du droit à une protection juridictionnelle effective et du droit fondamental à un procès équitable, lequel revêt une importance cardinale en tant que garant de la protection de l'ensemble des droits que les justiciables tirent du droit de l'Union et de la préservation des valeurs communes aux États membres énoncées à l'article 2 TUE, notamment la valeur de l'État de droit [arrêt du 15 juillet 2021, Commission/Pologne (Régime disciplinaire des juges), C-791/19, EU:C:2021:596, point 58 et jurisprudence citée]. Conformément au principe de séparation des pouvoirs qui caractérise le fonctionnement d'un État de droit, l'indépendance des juridictions doit notamment être garantie à l'égard des pouvoirs législatif et exécutif (voir arrêt du 18 mai 2021, Asociația « Forumul Judecătorilor din România » e.a., C-83/19, C-127/19, C-195/19, C-291/19, C-355/19 et C-397/19, EU:C:2021:393, point 195 et jurisprudence citée).

36 La jurisprudence précise que l'exigence d'indépendance des juridictions comporte deux aspects. Le premier aspect, d'ordre externe, requiert que l'instance concernée exerce ses fonctions en toute autonomie, sans être soumise à aucun lien hiérarchique ou de subordination à l'égard de quiconque et sans recevoir d'ordres ou d'instructions de quelque origine que ce soit, étant ainsi protégée contre les interventions ou les pressions extérieures susceptibles de porter atteinte à l'indépendance de jugement de ses membres et d'influencer leurs décisions. Le second aspect, d'ordre interne, rejoint la notion d'« impartialité » et vise l'équale distance par rapport aux parties au litige et à leurs intérêts respectifs au regard de l'objet de celui-ci. Ce dernier aspect exige le respect de l'objectivité et l'absence de tout intérêt dans la solution du litige en dehors de la stricte application de la règle de droit (voir arrêt du 21 décembre 2021, Euro Box Promotion e.a., C-357/19, C-379/19, C-547/19, C-811/19 et C-840/19, EU:C:2021:1034, point 224 et jurisprudence citée).

37 Les garanties d'indépendance et d'impartialité requises en vertu du droit de l'Union postulent l'existence de règles, notamment en ce qui concerne la composition de l'instance, la nomination, la durée des fonctions ainsi que les causes d'abstention, de récusation et de révocation de ses membres, qui permettent d'écarter tout doute légitime, dans l'esprit des justiciables, quant à l'imperméabilité de cette instance à l'égard d'éléments extérieurs et à sa neutralité par rapport aux intérêts qui s'affrontent [voir arrêt du 15 juillet 2021, Commission/Pologne (Régime disciplinaire des juges), C-791/19, EU:C:2021:596, point 59 et jurisprudence citée].

38 C'est dans ce contexte qu'il convient d'examiner les trois arguments soulevés par le requérant au soutien du présent grief.

1) *Sur le premier argument, selon lequel la DPRC n'est pas un tribunal indépendant et impartial, dès lors que sa mission consiste à réexaminer les décisions du Civil Liberties Protection Officer of the Director of National Intelligence*

- 39 Par son premier argument, le requérant fait valoir, en substance, que la DPRC n'est pas un tribunal indépendant et impartial, dès lors que sa mission consiste à réexaminer les décisions du Civil Liberties Protection Officer of the Director of National Intelligence (Responsable de la protection des libertés civiles du directeur du renseignement national, ci-après le « CLPO », États-Unis), qui est rattaché au bureau du directeur du renseignement national des États-Unis (ci-après le « directeur du renseignement national »).
- 40 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.
- 41 Dans un souci de clarté, il convient de préciser que le premier argument du premier grief du troisième moyen doit être interprété en ce sens que, en substance, selon le requérant, d'une part, lors du traitement d'une réclamation concernant les données personnelles déposée par une personne concernée dans l'Union qui souhaite faire valoir une violation du droit des États-Unis régissant les activités de renseignement d'origine électromagnétique qui porte atteinte à ses intérêts en matière de protection de la vie privée et des libertés civiles (ci-après la « réclamation concernant les données personnelles »), le CLPO n'est pas entouré de suffisamment de garanties visant à assurer son indépendance, au motif qu'il est rattaché au bureau du directeur du renseignement national, et, d'autre part, que la DPRC n'est pas un tribunal indépendant et impartial en raison de l'insuffisance de garanties applicables au CLPO.
- 42 D'emblée, il convient de relever que l'examen des garanties relatives à l'indépendance du CLPO est sans pertinence pour apprécier si la DPRC constitue un tribunal indépendant et impartial. En effet, la DPRC a été instituée en tant qu'organe de contrôle indépendant du CLPO auquel, comme il ressort du considérant 184 de la décision attaquée, la personne ayant introduit la réclamation concernant les données personnelles ainsi que chaque composante de la communauté de renseignement peut demander le réexamen de la décision du CLPO et plusieurs garanties ont été prévues dans l'E.O. 14086 pour que les décisions du CLPO puissent être réexaminées et, le cas échéant, réformées de manière indépendante et impartiale par la DPRC.
- 43 Premièrement, il ressort des considérants 185 et 186 de la décision attaquée, sans que le requérant le conteste, que la DPRC est composée d'au moins six juges qui sont nommés par l'Attorney General (procureur général, États-Unis, ci-après le « procureur général »), après consultation du Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles, États-Unis, ci-après le « PCLOB »), du Secretary of Commerce (secrétaire d'État au commerce, États-Unis) et du directeur du renseignement national, pour des mandats renouvelables de quatre ans, en utilisant les mêmes critères que ceux qui s'appliquent aux juges de la magistrature fédérale et en tenant compte de leur expérience judiciaire antérieure. Ainsi, les juges doivent être des praticiens du droit, à savoir des membres actifs en règle du barreau qui sont dûment autorisés à pratiquer le droit, et ils doivent avoir une expérience appropriée en matière de droit de la protection de la vie privée et de la sécurité nationale. En outre, le procureur général doit veiller à ce qu'au moins la moitié des juges aient une expérience judiciaire antérieure et tous les juges doivent être titulaires d'une habilitation de sécurité afin de pouvoir accéder à des informations classifiées relatives à la sécurité nationale. Seules les personnes qui satisfont aux qualifications susmentionnées et qui ne sont pas employées du pouvoir exécutif au moment de leur nomination ou ne l'ont pas été au cours des deux années précédentes peuvent être nommées à la DPRC. De même, pendant la durée de leur mandat, les juges de la DPRC ne peuvent exercer aucune fonction officielle ni aucun emploi au sein du gouvernement des États-Unis.
- 44 Deuxièmement, il ressort des considérants 188 et 189 de la décision attaquée, sans que le requérant le conteste, que les décisions du CLPO sont réexaminées, de manière intégrale, par un panel de trois juges de la DPRC assistés par un avocat spécial. Or, lors dudit réexamen, la DPRC ne se base pas uniquement sur le dossier fourni par le CLPO, mais aussi sur les informations et sur les observations transmises par le plaignant, par l'avocat spécial qui assiste ses juges et par les agences de renseignement ainsi que, le cas échéant, sur les informations additionnelles qu'elle a demandées au cours de l'instruction de la réclamation concernant les données personnelles. De plus, lors de ce réexamen, elle doit appliquer la jurisprudence pertinente de la Supreme Court of the United States (Cour suprême des États-Unis).

- 45 Troisièmement, il ressort des considérants 190 et 191 de la décision attaquée, sans que le requérant le conteste, que la DPRC a un pouvoir de réformation, n'est pas liée par la décision du CLPO et, en cas de désaccord avec ce dernier, peut adopter sa propre décision relative à la réclamation concernant les données personnelles. De plus, quelle que soit la décision prise par la DPRC, cette décision est contraignante et définitive. Ainsi, tant les agences de renseignement que le gouvernement des États-Unis sont tenus de s'y conformer.
- 46 Il résulte de ce qui précède que les garanties prévues par l'E.O. 14086 en ce qui concerne le fonctionnement et les pouvoirs de la DPRC permettent un réexamen indépendant et impartial des décisions adoptées par le CLPO. Le requérant n'est donc pas fondé à soutenir qu'une insuffisance des garanties applicables au CLPO affecte l'indépendance et l'impartialité de la DPRC.
- 47 En tout état de cause, s'agissant de la prétendue insuffisance des garanties visant à assurer l'indépendance du CLPO, il y a lieu d'observer ce qui suit.
- 48 Il convient de relever, ainsi qu'il ressort des considérants 176 à 181 de la décision attaquée, sans que le requérant le conteste, que l'E.O. 14086, complété par le règlement AG, a mis en place un mécanisme spécifique de recours afin de traiter la réclamation concernant les données personnelles. Cette réclamation doit être déposée auprès de l'autorité de contrôle chargée, dans chaque État membre, de la surveillance du traitement des données à caractère personnel, qui la transmet ensuite au CLPO, à condition qu'elle contienne les éléments indiqués au point 178 de la décision attaquée, à savoir des informations concernant les données à caractère personnel dont il est raisonnable de penser qu'elles ont été transférées vers les États-Unis, les moyens par lesquels on peut estimer qu'elles ont été transférées, l'identité, si elle est connue, des entités du gouvernement des États-Unis soupçonnées d'être impliquées dans la violation présumée, le fondement de la violation présumée du droit des États-Unis et la nature de la réparation demandée. Dans ce contexte, le CLPO doit déterminer si les agences de renseignement ont violé le droit des États-Unis applicable et, si tel est le cas, il peut ordonner qu'elles mettent en œuvre des mesures correctives. La décision du CLPO relative à ladite réclamation est contraignante.
- 49 Certes, au considérant 179 de la décision attaquée, la Commission indique que le CLPO fait partie du bureau du directeur du renseignement national et que, outre sa compétence spécifique pour examiner la réclamation concernant les données personnelles, il est tenu, plus généralement, de s'assurer que la protection des libertés civiles et de la vie privée soit intégrée de manière appropriée dans les politiques et procédures dudit bureau et des agences de renseignement et que ceux-ci respectent les exigences applicables en matière de protection de la vie privée et de libertés civiles. Toutefois, d'une part, il y a lieu de noter que, comme cela est mentionné dans ce considérant, afin d'assurer l'indépendance du CLPO, l'E.O. 14086 prévoit que celui-ci ne peut être démis de ses fonctions que par ledit directeur et pour un motif valable, c'est-à-dire en cas d'action fautive, de faute de commission, d'atteinte à la sécurité, de négligence ou d'incapacité. D'autre part, ainsi qu'il ressort du considérant 180 de la décision attaquée, il est interdit aux agences de renseignement et au directeur du renseignement national d'entraver ou d'influencer indûment le travail du CLPO qui, lors de l'examen de la réclamation concernant les données personnelles, doit appliquer la loi de manière impartiale, en tenant compte à la fois des intérêts relevant de la sécurité nationale et de la protection de la vie privée.
- 50 Dans ces conditions, il y a lieu de rejeter le présent argument.
- 2) *Sur le deuxième argument, selon lequel la DPRC n'est pas un tribunal indépendant et impartial, dès lors qu'elle est composée de juges nommés par le procureur général après consultation du PCLOB*
- 51 Par son deuxième argument, le requérant soutient, en substance, que la DPRC n'est pas un tribunal indépendant et impartial, dès lors qu'elle est composée de juges nommés par le procureur général après consultation du PCLOB, qui est un organe dépendant du pouvoir exécutif.
- 52 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.
- 53 En premier lieu, il ressort du considérant 110 de la décision attaquée que le PCLOB est une agence indépendante, instituée au sein du pouvoir exécutif. L'indépendance de cette agence ressort en particulier de sa composition. En effet, elle est composée d'un conseil bipartisan constitué de cinq

membres nommés par le président des États-Unis, avec l'approbation du Sénat, pour un mandat fixe de six ans. Lesdits membres doivent être sélectionnés sur la base de leurs qualifications professionnelles, de leurs réalisations, de leur stature publique, de leur expertise en matière de protection de la vie privée et des libertés civiles et de leur expérience, sans tenir compte de leur affiliation politique. Le PCLOB ne peut compter plus de trois membres appartenant au même parti politique. Une personne nommée membre du PCLOB ne peut pas, pendant son mandat, être un représentant élu, un fonctionnaire ou un employé du gouvernement fédéral, autrement qu'en sa qualité de membre du PCLOB.

54 Il s'ensuit que, bien que le PCLOB ait été institué au sein du pouvoir exécutif, il a été conçu, par son statut fondateur, comme une agence indépendante dont la mission consiste à superviser, de manière impartiale, le travail mené par le pouvoir exécutif en vue de protéger, notamment, la vie privée et les libertés civiles. Ainsi, comme il est indiqué au considérant 194 de la décision attaquée, sans que le requérant le conteste, il doit contrôler chaque année si le CLPO et la DPRC ont traité les affaires reçues dans les délais impartis, s'ils ont eu accès à toutes les informations nécessaires, s'ils ont pris en compte toutes les garanties prévues par l'E.O. 14086 et si les agences du renseignement se sont conformées à leurs décisions. À la suite de cette vérification, il doit certifier publiquement que le CLPO et la DPRC ont respecté ces garanties. De plus, il doit présenter un rapport au président des États-Unis, au procureur général, au directeur du renseignement national, aux chefs des agences de renseignement, au CLPO et aux commissions du renseignement de l'United States Congress (Congrès des États-Unis). Ce rapport est rendu public dans une version non classifiée. Le procureur général, le directeur du renseignement national, le CLPO et les chefs des agences de renseignement sont tenus de mettre en œuvre toutes les recommandations figurant dans ledit rapport.

55 Dans ces conditions, le fait que le PCLOB ait été institué au sein du pouvoir exécutif ne permet pas en soi de conclure que, en raison de sa consultation avant la nomination des juges de la DPRC, cette dernière n'est pas un tribunal indépendant et impartial.

56 En deuxième lieu, il convient de noter que, pour s'assurer que les juges de la DPRC soient indépendants du pouvoir exécutif, l'E.O. 14086 prévoit que, lors de leur nomination, le procureur général doit respecter les critères et les conditions indiqués au point 43 ci-dessus. De plus, ainsi qu'il ressort du considérant 187 de la décision attaquée, les juges de la DPRC ne peuvent être révoqués que par le procureur général et uniquement pour un motif valable, à savoir une action fautive, une faute de commission, une atteinte à la sécurité, une négligence ou une incapacité, après avoir dûment pris en compte les normes applicables aux juges fédéraux énoncées dans les règles relatives à la déontologie judiciaire et à la procédure d'incapacité judiciaire.

57 Il s'ensuit que les règles portant sur la nomination et la révocation des juges de la DPRC ne sauraient remettre en cause son indépendance et son impartialité.

58 En troisième lieu, il convient de relever que, aux termes de l'article 3, paragraphe 1, de la décision attaquée, la Commission est tenue de suivre de manière permanente l'application du cadre juridique sur lequel se fonde ladite décision, notamment les conditions dans lesquelles les transferts ultérieurs de données à caractère personnel sont effectués, les droits individuels sont exercés et les autorités publiques des États-Unis ont accès aux données transférées sur la base de cette décision, dans le but de déterminer si les États-Unis d'Amérique continuent d'assurer un niveau de protection adéquat. Ainsi, conformément au paragraphe 5 dudit article, lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités des États-Unis et, si nécessaire, elle décide de suspendre, de modifier, d'abroger la décision attaquée ou d'en restreindre le champ d'application. Il s'ensuit que, si le cadre juridique en vigueur aux États-Unis au moment de l'adoption de la décision attaquée qui a conduit la Commission à considérer, dans celle-ci, que la DPRC offrait une protection juridique substantiellement équivalente à celle garantie par le droit de l'Union change, la Commission décide, si nécessaire, de suspendre, de modifier ou d'abroger la décision attaquée ou d'en restreindre le champ d'application.

59 Eu égard à l'ensemble de ces considérations, il y a lieu de rejeter le présent argument.

3) *Sur le troisième argument, selon lequel la DPRC n'est pas un tribunal indépendant et impartial, dès lors que le règlement AG n'exclut pas la possibilité que ses juges subissent des formes de supervision autres que quotidiennes de la part du pouvoir exécutif*

60 Par son troisième argument, le requérant fait valoir, en substance, que la DPRC n'est pas un tribunal indépendant et impartial, dès lors que le règlement AG n'exclut pas la possibilité que ses juges subissent des formes de supervision autres que quotidiennes de la part du pouvoir exécutif.

61 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.

62 Il y a lieu de noter que, s'il résulte du dossier que, aux termes de l'article 201.7, sous d), du règlement AG, les juges de la DPRC ne doivent pas être assujettis à la supervision quotidienne du procureur général, le considérant 187 de la décision attaquée indique également que, au titre de l'E.O. 14086, les agences de renseignement et le procureur général ne doivent pas entraver ni influencer indûment le travail de la DPRC. En outre, il ressort du dossier que l'E.O. 14086 et le règlement AG limitent la possibilité pour le pouvoir exécutif d'influencer le travail de la DPRC en établissant que ses juges ne peuvent être révoqués que par le procureur général et uniquement pour les motifs indiqués au point 56 ci-dessus.

63 Dans ce contexte, il y a lieu de rejeter le présent argument et, partant, le premier grief du troisième moyen dans son ensemble.

b) Sur le second grief du troisième moyen, selon lequel la DPRC n'est pas un tribunal établi préalablement par la loi

64 Par le second grief de son troisième moyen, le requérant fait valoir que la DPRC n'a pas été établie préalablement par la loi, au sens de l'article 47, deuxième alinéa, de la charte des droits fondamentaux, dans la mesure où elle n'a pas été créée par une loi adoptée par le Congrès des États-Unis, mais par un acte de l'exécutif, à savoir une décision du procureur général.

65 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

66 En premier lieu, il résulte de la jurisprudence de la Cour, développée à la lumière de celle de la Cour EDH concernant l'article 6, paragraphe 1, de la CEDH (Cour EDH, 1^{er} décembre 2020, Guðmundur Andri Ástráðsson c. Islande, CE:ECHR:2020:1201JUD002637418, § 231 et 233), que, si le droit à un tribunal établi préalablement par la loi constitue un droit autonome, ce dernier n'en a pas moins des liens très étroits avec les garanties d'indépendance et d'impartialité figurant dans cette même disposition. Plus particulièrement, bien que toutes les exigences dictées par ces notions poursuivent chacune un but précis qui fait d'elles des garanties spécifiques d'un procès équitable, ces garanties tendent au respect des mêmes principes fondamentaux que sont la prééminence du droit et la séparation des pouvoirs. À la base de chacune de ces exigences se trouve, ainsi, l'impératif de préserver la confiance que le pouvoir judiciaire se doit d'inspirer au justiciable et l'indépendance de ce pouvoir à l'égard des autres pouvoirs [voir arrêts du 22 février 2022, Openbaar Ministerie (Tribunal établi par la loi dans l'État membre d'émission), C-562/21 PPU et C-563/21 PPU, EU:C:2022:100, point 56 et jurisprudence citée, et du 29 mars 2022, Getin Noble Bank, C-132/20, EU:C:2022:235, point 117 et jurisprudence citée).

67 La Cour a également précisé, en faisant écho à la jurisprudence de la Cour EDH (Cour EDH, 8 juillet 2014, Biagioli c. San Marino, CE:ECHR:2014:0708DEC000816213, § 72 à 74 ; voir, également, Cour EDH, 2 mai 2019, Pasquini c. San Marino, CE:ECHR:2019:0502JUD005095616, § 100 et 101 et jurisprudence citée), que l'expression « établi préalablement par la loi » a pour objet d'éviter que l'organisation du système judiciaire ne soit laissée à la discrétion de l'exécutif et de faire en sorte que cette matière soit régie par une loi adoptée par le pouvoir législatif d'une manière conforme aux règles encadrant l'exercice de sa compétence. Cette expression reflète, ainsi, le principe de l'État de droit et concerne non seulement la base légale de l'existence même du tribunal, mais encore la composition du siège dans chaque affaire ainsi que toute autre disposition du droit interne dont le non-respect rend irrégulière la participation d'un ou de plusieurs juges à l'examen de l'affaire, ce qui inclut, en particulier, des dispositions concernant l'indépendance et l'impartialité des membres de la juridiction visée (voir arrêt du 29 mars 2022, Getin Noble Bank, C-132/20, EU:C:2022:235, point 121 et jurisprudence citée).

- 68 Dans ce contexte, la Cour a jugé qu'une constatation relative à l'existence d'une violation de l'exigence d'un tribunal établi préalablement par la loi et aux conséquences d'une telle violation était soumise à une appréciation globale d'un certain nombre d'éléments qui, considérés ensemble, contribuent à générer, dans l'esprit des justiciables, des doutes légitimes en ce qui concerne l'indépendance et l'impartialité des juges [voir arrêt du 22 février 2022, *Openbaar Ministerie* (Tribunal établi par la loi dans l'État membre d'émission), C-562/21 PPU et C-563/21 PPU, EU:C:2022:100, point 74 et jurisprudence citée].
- 69 Ainsi, la Cour a considéré que la circonstance selon laquelle un organe, tel qu'un conseil national de la magistrature, impliqué dans le processus de désignation des juges soit, de manière prépondérante, composé de membres choisis par le pouvoir législatif ne saurait, à elle seule, conduire à faire douter de l'indépendance des juges nommés au terme de ce processus, mais que, toutefois, il peut en aller différemment lorsque cette circonstance, combinée à d'autres éléments pertinents et aux conditions dans lesquelles ces choix ont été opérés, conduit à générer de tels doutes [voir arrêt du 22 février 2022, *Openbaar Ministerie* (Tribunal établi par la loi dans l'État membre d'émission), C-562/21 PPU et C-563/21 PPU, EU:C:2022:100, point 75 et jurisprudence citée].
- 70 Par ailleurs, dans son arrêt du 1^{er} décembre 2020, *Guðmundur Andri Ástráðsson c. Islande* (CE:ECHR:2020:1201JUD002637418, § 207 et 212), la Cour EDH a estimé que la nomination de juges par l'exécutif ou par le législateur est admissible, pourvu que les juges ainsi nommés soient libres de toute pression ou de toute influence lorsqu'ils exercent leur rôle juridictionnel.
- 71 Il résulte, en substance, de cette jurisprudence que, pour apprécier si les exigences qui découlent de l'article 47, deuxième alinéa, de la charte des droits fondamentaux sont remplies, il ne faut pas se limiter à apprécier la nature formelle du texte juridique établissant un tribunal et définissant ses règles de fonctionnement, mais il convient de vérifier si ce texte juridique prévoit des garanties suffisantes visant à assurer son indépendance et son impartialité vis-à-vis des autres pouvoirs, notamment du pouvoir exécutif.
- 72 En second lieu, il convient de rappeler que, comme cela a été jugé par la Cour dans l'arrêt *Schrems I* et dans l'arrêt *Schrems II*, dans le cadre d'une décision d'adéquation, la Commission n'est pas tenue de s'assurer que les dispositions pertinentes du pays tiers sont identiques à celles en vigueur dans l'Union, mais qu'elles sont substantiellement équivalentes à celles garanties par le droit de l'Union en vertu du RGPD, lu à la lumière de la charte des droits fondamentaux (voir points 19 et 20 ci-dessus). Il s'ensuit que, en l'espèce, le Tribunal est tenu de vérifier le bien-fondé du constat d'adéquation effectué par la Commission dans la décision attaquée, selon lequel les dispositions du droit des États-Unis concernant l'établissement et le fonctionnement de la DPRC offrent des garanties substantiellement équivalentes à celles prévues par le droit de l'Union à l'article 47, deuxième alinéa, de ladite charte. De telles garanties sont offertes, en particulier, lorsque le texte juridique établissant ce tribunal et définissant ses règles de fonctionnement vise à assurer son indépendance et son impartialité à l'égard des autres pouvoirs, notamment du pouvoir exécutif, et ce malgré le fait que ledit texte ne constitue pas, d'un point de vue formel, une loi.
- 73 En l'espèce, il ressort du considérant 185 de la décision attaquée, sans que le requérant le conteste, que la DPRC a été établie par le règlement AG. Il en découle que la DPRC n'a pas été constituée par une loi adoptée par le pouvoir législatif, à savoir le Congrès des États-Unis, mais par un acte émanant du pouvoir exécutif. Le procureur général est, en effet, le chef du département de la justice des États-Unis et le principal responsable de l'application de la loi au sein du gouvernement fédéral des États-Unis. Il est le principal conseiller du président des États-Unis pour toutes les questions juridiques et fait partie de son cabinet.
- 74 Dans ce contexte, il convient de vérifier si, de manière substantiellement équivalente au droit de l'Union, l'E.O. 14086 et le règlement AG prévoient des garanties visant à assurer l'indépendance et l'impartialité de la DPRC.
- 75 À cet égard, premièrement, il convient de noter qu'il ressort du dossier, sans être contesté, que :

- le procureur général a adopté le règlement AG sur la base de son pouvoir statutaire d'émettre des décisions contraignantes sur des questions de droit des États-Unis, y compris celles relatives au transfert des données depuis l'Union régies par l'E.O. 14086 ;
- en instituant la DPRC, le procureur général lui a délégué son pouvoir de statuer sur la légalité des activités de renseignement d'origine électromagnétique contestées par un citoyen de l'Union ; ainsi, le procureur général n'est plus habilité de jure à exercer le pouvoir qu'il a délégué à la DPRC tant que celle-ci existe ;
- comme cela est indiqué à la note en bas de page n° 366 figurant à la page 63 de la décision attaquée, la Cour suprême des États-Unis a reconnu la possibilité, pour le procureur général, d'établir des organes indépendants dotés d'un pouvoir de décision, tels que la DPRC ; de plus, elle a considéré que la délégation de pouvoir effectuée par le procureur général à son mandataire est contraignante pour le pouvoir exécutif ; ainsi, il ressort de la jurisprudence de ladite juridiction que, tant que le règlement AG reste en vigueur, le pouvoir exécutif est lié par celui-ci et que ni les agences de renseignement ni le gouvernement des États-Unis ne peuvent revoir ou révoquer ses décisions.

76 Deuxièmement, d'une part, il convient de rappeler qu'il ressort de la décision attaquée, en substance, que :

- les juges de la DPRC sont nommés par le procureur général sur la base des critères et dans le respect des conditions mentionnées au point 43 ci-dessus ;
- les juges de la DPRC ne peuvent être révoqués que par le procureur général pour les seuls motifs visés au point 56 ci-dessus et dans le respect des normes applicables aux juges fédéraux énoncées dans les règles relatives à la déontologie judiciaire et à la procédure d'incapacité judiciaire ;
- la décision adoptée par la DPRC est contraignante et définitive. Ainsi, tant le pouvoir exécutif que les agences de renseignement sont tenus d'y se conformer ;
- le travail effectué par la DPRC fait l'objet d'une supervision de la part du PCLOB, dans les limites indiquées au point 54 ci-dessus.

77 D'autre part, ainsi qu'il ressort des considérants 187 à 189 de la décision attaquée, les juges de la DPRC doivent respecter, lors de l'accomplissement de leur mission au sein de cette dernière, les garanties procédurales suivantes :

- ils doivent examiner la réclamation concernant les données personnelles au sein d'un panel composé de trois juges, dont un juge président ; pour chaque affaire, la composition du panel de trois juges est choisie, au tour de rôle, par le bureau des libertés civiles et de la vie privée du ministère de la Justice, qui est chargé de fournir un soutien administratif à la DPRC, en veillant à ce que chaque panel comprenne au moins un juge ayant une expérience judiciaire antérieure ;
- lors de l'examen de la réclamation concernant les données personnelles, ils sont assistés par un avocat spécial qui est nommé par le procureur général, après consultation du secrétaire d'État au commerce, du directeur du renseignement national et du PCLOB, pour un mandat de deux ans renouvelable ; l'avocat spécial doit avoir une expérience appropriée dans le domaine du droit de la vie privée et de la sécurité nationale, il doit être un avocat expérimenté et un membre actif et en règle du barreau ; de plus, lors de sa nomination, il ne doit pas avoir été employé du pouvoir exécutif au cours de deux années précédentes ; l'avocat spécial a accès à toutes les informations, y compris aux informations classifiées, et, bien qu'il ne défende pas les intérêts du plaignant et qu'il n'ait pas de relation avocat-client avec celui-ci, il doit veiller à ce que, dans chaque affaire, les intérêts du plaignant soient représentés et les juges de la DPRC soient bien informés de toutes les questions de droit et de fait pertinentes ;
- afin de rendre leur décision, ils doivent prendre en compte le dossier de l'enquête, les informations et les observations fournies par le plaignant, par l'avocat spécial, par les agences de

renseignement et par le CLPO ainsi que, le cas échéant, les informations additionnelles transmises par le CLPO sur demande de la DPRC ;

- ils doivent adopter une décision sur la réclamation concernant les données personnelles par écrit et à la majorité des voix.

78 Troisièmement, il y a lieu de relever qu'il a été remédié aux carences qui avaient été relevées par la Cour dans l'arrêt Schrems II en ce qui concernait l'absence de garanties relatives à la révocation, par le pouvoir exécutif, du médiateur du bouclier de protection et au défaut de caractère contraignant de ses décisions. En effet, il résulte du dossier que l'E.O. 14086 limite les hypothèses dans lesquelles le procureur général peut révoquer les juges de la DPRC et prévoit que ses décisions sont contraignantes.

79 Dans ce contexte, il y a lieu de rejeter le second grief du troisième moyen.

80 Cette conclusion ne saurait être remise en cause par le fait qu'il ressort du dossier que, au même titre que d'autres tribunaux du système juridique des États-Unis, tout en étant habilitée à statuer sur des questions juridiques, la DPRC ne constitue pas une autorité judiciaire établie en vertu de l'article III de la Constitution des États-Unis.

81 En effet, dans l'arrêt Schrems II, la Cour a estimé qu'une protection juridictionnelle effective pouvait être assurée non seulement par une juridiction appartenant à l'ordre judiciaire, mais aussi par tout autre « organe » qui offrait aux personnes dont les données sont transférées vers les États-Unis des garanties substantiellement équivalentes à celles requises par l'article 47 de la charte des droits fondamentaux (arrêt Schrems II, point 197).

82 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de rejeter le troisième moyen dans son intégralité.

3. Sur le deuxième moyen, tiré de la violation des articles 7 et 8 de la charte des droits fondamentaux

83 Par son deuxième moyen, le requérant fait valoir que la Commission a violé les articles 7 et 8 de la charte des droits fondamentaux, dans la mesure où, dans la décision attaquée, elle a considéré que les États-Unis d'Amérique assuraient un niveau de protection adéquat en ce qui concernait la collecte en vrac, par les agences de renseignement de ce pays, de données à caractère personnel.

a) Sur l'objet du deuxième moyen

84 Il convient de noter que, aux pages 2 et 23 de la requête ainsi qu'à la page 4 de la réplique, lorsqu'il énonce le libellé du deuxième moyen, le requérant se réfère à la violation, par la Commission, des articles 7 et 8 de la charte des droits fondamentaux en ce qui concerne non seulement la collecte en vrac, mais aussi la collecte massive de données à caractère personnel. Toutefois, dans les développements qui suivent l'énonciation du libellé dudit moyen, le requérant concentre son argumentation uniquement sur la collecte en vrac de ces données.

85 Il ressort de la note en bas de page n° 250 figurant à la page 46 de la décision attaquée, du considérant 141 de ladite décision, sans être contesté, ainsi que des réponses fournies par les parties aux questions posées par le biais d'une mesure d'organisation de la procédure et lors de l'audience que :

- aux États-Unis, la collecte de renseignements d'origine électromagnétique à des fins de sécurité nationale, y compris en ce qui concerne les données transférées depuis l'Union, peut uniquement prendre la forme d'une « collecte ciblée » ; cette expression n'est pas définie dans le droit des États-Unis, mais est généralement utilisée pour décrire la collecte de renseignements visant une personne spécifique, un compte de communication ou une autre cible identifiée qui est effectuée par les agences de renseignement au titre du Foreign Intelligence Surveillance Act (loi sur la surveillance du renseignement étranger, ci-après le « FISA ») et de l'E.O. 14086.
- en dehors des États-Unis, y compris lorsque des données personnelles sont en transit depuis l'Union vers des organisations du CPD, la collecte de renseignements d'origine

électromagnétique à des fins de sécurité nationale se fait, prioritairement, par le biais d'une collecte ciblée ; or, lorsqu'il est nécessaire de faire progresser une priorité validée en matière de renseignement, au sens de la section 2, sous b), iii), de l'E.O. 14086, qui ne peut pas être raisonnablement obtenue par une collecte ciblée, les agences de renseignement peuvent effectuer une « collecte en vrac » de données à caractère personnel ; la collecte en vrac est définie dans le droit des États-Unis par la section 4, sous b), de l'E.O. 14086 comme étant la collecte autorisée de grandes quantités de renseignements d'origine électromagnétique qui, pour des raisons techniques ou opérationnelles, est effectuée sans utiliser de discriminants, par exemple des identifiants ou des critères de sélection spécifiques ; la collecte en vrac est régie par l'E.O. 14086 et par l'Executive Order 12333, United States Intelligence Activities (décret présidentiel n° 12333 sur les activités de renseignement des États-Unis), tel que modifié par les Executive Orders 13284 (2003), 13355 (2004) et 13470 (2008) (décrets présidentiels n°s 13284/2003, 13355/2004 et 13470/2008) qui l'assujettissent à plusieurs garanties et limitations ;

- la « collecte massive » de données à caractère personnel à laquelle la Commission se réfère à la note en bas de page n° 250 de la décision attaquée comme étant une collecte effectuée de manière généralisée et indifférenciée sans restrictions ni garanties n'est pas autorisée aux États-Unis et ne peut être effectuée ni sur son territoire ni en dehors de celui-ci.

86 Il résulte de ce qui précède que, dès lors que la collecte massive n'est pas autorisée aux États-Unis et que la collecte en vrac peut être uniquement effectuée en dehors des États-Unis, l'objet du présent moyen se limite, en l'espèce, à l'appréciation de l'existence d'une violation, par la Commission, des articles 7 et 8 de la charte des droits fondamentaux en ce qui concerne la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union vers les organisations du CPD, à l'exclusion de toute collecte de données à caractère personnel effectuée, le cas échéant, sur le territoire de l'Union par les agences de renseignement des États-Unis ou des États membres.

b) Sur le premier grief du deuxième moyen, selon lequel les activités de renseignement effectuées en vertu de l'article 702 du FISA ne sont pas assujetties aux garanties prévues par l'E.O. 14086

87 Par le premier grief de son deuxième moyen, le requérant fait valoir que la Commission a violé les articles 7 et 8 de la charte des droits fondamentaux dès lors que, dans la décision attaquée, elle a considéré, en substance, que les États-Unis d'Amérique offraient un niveau de protection substantiellement équivalent à celui qui est garanti par le droit de l'Union en vertu du RGPD, lu à la lumière de ladite charte, malgré le fait que l'article 702 du FISA octroie aux agences de renseignement des États-Unis la possibilité de collecter en vrac les données à caractère personnel de ressortissants d'autres pays.

88 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

89 Il convient de relever que l'article 702 du FISA n'autorise pas la collecte en vrac, mais uniquement la collecte ciblée de données à caractère personnel.

90 Il s'ensuit que, dans la mesure où l'article 702 du FISA ne concerne pas la collecte en vrac de données à caractère personnel, il est dénué de pertinence en l'espèce.

91 Ainsi, il y a lieu de rejeter le premier grief du deuxième moyen.

c) Sur le deuxième grief du deuxième moyen, selon lequel l'E.O. 14086 n'assujettit pas la collecte en vrac de données à caractère personnel à l'autorisation préalable d'une autorité judiciaire ou administrative

92 Par le deuxième grief de son deuxième moyen, le requérant fait valoir que la Commission a violé les articles 7 et 8 de la charte des droits fondamentaux dès lors que, dans la décision attaquée, elle a considéré que les États-Unis d'Amérique offraient un niveau de protection substantiellement équivalent à celui qui est garanti par le droit de l'Union en vertu du RGPD, lu à la lumière de ladite charte, malgré

le fait que l'E.O. 14086 n'établit pas l'obligation, pour les agences de renseignement des États-Unis, d'obtenir, en amont de la collecte en vrac de données à caractère personnel, l'autorisation préalable d'une autorité judiciaire ou administrative.

- 93 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.
- 94 En l'espèce, il ressort du dossier, sans que cela soit contesté par les parties, que le droit des États-Unis n'établit pas l'obligation, pour les agences de renseignement, d'obtenir l'autorisation préalable d'une autorité judiciaire ou administrative avant d'effectuer la collecte en vrac de données à caractère personnel en transit depuis l'Union vers les organisations du CPD.
- 95 Il convient d'établir si cette absence d'autorisation préalable est susceptible d'affecter la légalité de la décision attaquée, dans la mesure où elle pourrait remettre en question la conclusion figurant à l'article 1^{er} de ladite décision, selon laquelle les États-Unis d'Amérique offrent un niveau adéquat de protection des données à caractère personnel.
- 96 À titre liminaire, il y a lieu de rappeler, que, comme cela a été jugé par la Cour dans l'arrêt Schrems II, pour évaluer la légalité d'une décision d'adéquation, il est nécessaire d'apprécier si le droit du pays tiers assure un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui qui est garanti au sein de l'Union en vertu du RGPD, lu à la lumière de la charte des droits fondamentaux (voir point 19 ci-dessus).
- 97 C'est dans ce contexte qu'il convient d'examiner les quatre arguments soulevés par le requérant au soutien du présent grief.

1) Sur le premier argument, fondé sur l'arrêt Schrems II

- 98 Par son premier argument, le requérant fait valoir, en substance, que, comme cela était le cas pour la décision d'adéquation concernant le bouclier de protection annulée par la Cour dans l'arrêt Schrems II en raison notamment du défaut de mise en place d'un contrôle judiciaire, la collecte en vrac de données à caractère personnel qui est effectuée, en l'espèce, par les agences de renseignement des États-Unis ne fait pas l'objet d'une surveillance judiciaire et n'est pas encadrée par des règles suffisamment claires et précises.
- 99 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.
- 100 Il convient de noter que, dans l'arrêt Schrems II, la Cour a jugé que les articles 7 et 8 de la charte des droits fondamentaux participaient du niveau de protection, requis au sein de l'Union, dont le respect devait être constaté par la Commission avant que celle-ci n'adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du RGPD. En effet, selon la Cour, tout traitement des données à caractère personnel d'une personne physique, y compris leur transfert vers un pays tiers dans le cadre d'une décision d'adéquation, affecte tant le droit fondamental de cette personne au respect de la vie privée, garanti à l'article 7 de ladite charte, que son droit à la protection de ses données à caractère personnel, figurant à l'article 8 de cette charte (arrêt Schrems II, points 169 à 171).
- 101 Toutefois, la Cour a précisé que les droits consacrés aux articles 7 et 8 de la charte des droits fondamentaux n'étaient pas des prérogatives absolues, mais devaient être pris en considération par rapport à leur fonction dans la société (arrêt Schrems II, point 172).
- 102 Ainsi, conformément à l'article 52, paragraphe 1, de la charte des droits fondamentaux, toute limitation de l'exercice des droits et des libertés reconnus par les articles 7 et 8 de ladite charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. De plus, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui (arrêt Schrems II, point 174).

- 103 Dans ce contexte, la Cour a jugé que la possibilité qui était donnée par le décret présidentiel n° 12333, tel que modifié, aux agences de renseignement des États-Unis d'accéder aux données à caractère personnel en transit depuis l'Union, sans que cet accès ait fait l'objet d'une quelconque surveillance judiciaire, ne permettait pas d'encadrer de manière suffisamment claire et précise la portée de la collecte en vrac de données à caractère personnel qui était effectuée par les agences de renseignement. Ainsi, elle a considéré que ledit décret présidentiel ne correspondait pas aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité et que les programmes de surveillance menés sur la base de ce décret n'étaient pas limités au strict nécessaire (arrêt Schrems II, points 183 et 184).
- 104 Il y a lieu de préciser l'interprétation qu'il convient de donner à l'expression « quelconque surveillance judiciaire » figurant au point 183 de l'arrêt Schrems II.
- 105 À cet égard, il convient de relever qu'aucun élément dans l'arrêt Schrems II, en particulier au point 183 dudit arrêt et dans l'expression « quelconque surveillance judiciaire », ne suggère que la collecte en vrac de données à caractère personnel doit obligatoirement faire l'objet d'une autorisation préalable délivrée par une autorité indépendante. Au contraire, il ressort d'une lecture conjointe de ladite expression et des points 186 à 197 de cet arrêt que la décision autorisant une telle collecte doit, au minimum, faire l'objet d'un contrôle judiciaire a posteriori.
- 106 En l'espèce, comme cela est indiqué aux points 24 à 82 ci-dessus, l'E.O. 14086 et le règlement AG assujettissent les activités de renseignement d'origine électromagnétique menées par les agences de renseignement des États-Unis, y compris lorsque ces dernières effectuent une collecte en vrac de données à caractère personnel, à la surveillance judiciaire a posteriori de la DPRC, dont les décisions sont définitives et contraignantes et s'imposent tant vis-à-vis du gouvernement des États-Unis que desdites agences. Par conséquent, contrairement à ce que fait valoir le requérant, il ne saurait être considéré que la collecte en vrac de données à caractère personnel effectuée par les agences de renseignement sur la base de la décision attaquée ne satisfait pas aux exigences découlant de l'arrêt Schrems II à cet égard.
- 107 De plus, en premier lieu, il convient de rappeler que, comme cela ressort du considérant 141 de la décision attaquée, sans que le requérant le conteste, l'E.O. 14086 établit que les agences de renseignement doivent donner la priorité à la collecte ciblée de données à caractère personnel. Ainsi, la collecte en vrac n'est autorisée que pour faire progresser une priorité validée en matière de renseignement qui ne peut pas être raisonnablement obtenue par une collecte ciblée. À cet égard, il y a lieu de noter qu'il ressort du considérant 135 de ladite décision que les priorités validées en matière de renseignement sont établies dans le cadre d'une procédure spéciale visant à garantir le respect des exigences légales applicables, notamment celles relatives à la vie privée et aux libertés civiles. Plus précisément, les priorités en matière de renseignement sont définies par le directeur du renseignement national et sont soumises à l'approbation du président des États-Unis. Or, avant de proposer au président des États-Unis des priorités en matière de renseignement, ledit directeur doit obtenir, pour chaque priorité, une évaluation de la part du CLPO. Dans le cadre de cette évaluation, le CLPO doit déterminer si la priorité en cause fait progresser un ou plusieurs des objectifs légitimes énumérés dans l'E.O. 14086, si elle n'a pas été conçue pour la collecte de renseignements d'origine électromagnétique à des fins interdites et si elle a été établie après avoir dûment pris en compte les aspects relatifs à la vie privée et aux libertés civiles de toutes les personnes concernées, quels que soient leur nationalité et leur lieu de résidence.
- 108 En deuxième lieu, il convient de relever que, comme cela est mis en exergue par les considérants 127 à 131, 134 et 135 de la décision attaquée, sans que le requérant le conteste, l'E.O. 14086 fixe des exigences fondamentales s'appliquant à toutes les activités de renseignement d'origine électromagnétique, y compris lorsque celles-ci sont effectuées par le biais d'une collecte en vrac de données à caractère personnel.
- 109 Premièrement, les activités de renseignement d'origine électromagnétique doivent être fondées sur une loi ou sur une autorisation présidentielle et doivent être effectuées conformément au droit des États-Unis, notamment à leur Constitution.

- 110 Deuxièmement, les activités de renseignement d'origine électromagnétique ne peuvent être menées qu'après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, qu'elles sont nécessaires pour poursuivre une priorité validée en matière de renseignement.
- 111 Troisièmement, les activités de renseignement d'origine électromagnétique doivent être menées de manière proportionnée par rapport à la priorité validée en matière de renseignement pour laquelle elles ont été autorisées, afin de trouver un juste équilibre entre l'importance de la priorité poursuivie en matière de renseignement et l'incidence sur la vie privée et les libertés civiles de la personne concernée, quels que soient sa nationalité et son lieu de résidence.
- 112 Quatrièmement, l'E.O. 14086 énumère les objectifs généraux qui ne peuvent pas être poursuivis par des activités de renseignement d'origine électromagnétique. Il s'agit notamment des objectifs consistant à entraver les critiques, les désaccords ou la libre expression d'idées ou d'opinions politiques par des personnes ou par la presse, à défavoriser des personnes au motif de leur appartenance ethnique, de leur race, de leur genre, de leur identité sexuelle, de leur orientation sexuelle ou de leur religion ou à conférer un avantage concurrentiel aux entreprises établies aux États-Unis.
- 113 En troisième lieu, il ressort du considérant 141 de la décision attaquée, sans que le requérant le conteste, que l'E.O. 14086 établit des garanties spécifiques s'appliquant à la collecte en vrac de données à caractère personnel.
- 114 Tout d'abord, l'E.O. 14086 prévoit que des méthodes et des mesures techniques doivent être appliquées afin de limiter les données collectées à ce qui est nécessaire pour poursuivre une priorité validée en matière de renseignement, tout en réduisant autant que possible la collecte d'informations non pertinentes.
- 115 Ensuite, l'E.O. 14086 indique que la collecte en vrac de données à caractère personnel ne peut être effectuée que pour répondre à six objectifs spécifiques (ci-après les « objectifs spécifiques de la collecte en vrac »), à savoir la protection contre le terrorisme, l'espionnage, les armes de destruction massive, les cybermenaces, les menaces dirigées à l'encontre du personnel des États-Unis ou de ses alliés et la criminalité transnationale. Il prévoit la possibilité, pour le président des États-Unis, de mettre à jour lesdits objectifs spécifiques si de nouveaux impératifs de sécurité nationale apparaissent, tels que de nouvelles menaces ou des menaces accrues pour la sécurité nationale pour lesquelles celui-ci estime que la collecte en vrac de données à caractère personnel pourrait être utilisée. Ces mises à jour doivent, en principe, être rendues publiques par le directeur du renseignement national, sauf si le président des États-Unis considère que cela constituerait en soi un risque pour la sécurité nationale de ce pays.
- 116 Enfin, l'E.O. 14086 prévoit que toute interrogation des données de renseignement d'origine électromagnétique obtenues en vrac ne peut avoir lieu que si elle est nécessaire pour poursuivre une priorité validée en matière de renseignement, dans le cadre de la poursuite des objectifs spécifiques de la collecte en vrac et conformément à des politiques et des procédures qui tiennent dûment compte de l'incidence des interrogations de ces données sur la vie privée et les libertés civiles de toutes les personnes concernées, quels que soient leur nationalité ou leur lieu de résidence.
- 117 Dans ces conditions, il ne saurait être valablement soutenu que la mise en œuvre de la collecte en vrac n'est pas encadrée de manière suffisamment claire et précise.
- 118 Eu égard à l'ensemble de ces considérations, il y a lieu de rejeter le présent argument.
- 2) *Sur le deuxième argument, fondé sur l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18)*
- 119 Par son deuxième argument, le requérant, se référant expressément au point 189 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), soutient que la Cour a établi l'obligation, pour les agences de renseignement, d'obtenir l'autorisation préalable d'une autorité judiciaire ou administrative en amont de la collecte de données de connexion auprès des opérateurs qui les détenaient. Selon lui, la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union ne ferait pas, en l'espèce, l'objet d'une telle autorisation préalable.

- 120 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.
- 121 Il y a lieu de relever que, dans l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), la Cour a notamment considéré que l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11), lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, devait être interprété en ce sens qu'il ne s'opposait pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir au recueil en temps réel des données relatives au trafic et des données de localisation, lorsque celui-ci était limité aux personnes à l'égard desquelles il existait une raison valable de soupçonner qu'elles étaient impliquées dans des activités de terrorisme et soumis au contrôle préalable d'une juridiction ou d'une entité administrative indépendante (point 192 dudit arrêt).
- 122 Il s'ensuit que l'hypothèse en cause dans l'affaire ayant donné lieu à l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) diffère de celle qui est en cause en l'espèce. En l'occurrence, il ne s'agit pas d'apprécier le besoin d'assujettir le recueil, par les fournisseurs de services de communications électroniques, des données relatives au trafic et des données de localisation des utilisateurs soupçonnés d'être impliqués d'une manière ou d'une autre dans des activités de terrorisme au contrôle préalable d'une autorité judiciaire ou administrative, mais d'apprécier si le fait que le droit des États-Unis ne prévoit pas d'obligation, pour les agences de renseignement, d'obtenir, en amont de la collecte en vrac de données à caractère personnel en transit vers ce pays, l'autorisation préalable d'une autorité judiciaire ou administrative remet en cause le bien-fondé du constat d'adéquation effectué par la Commission dans la décision attaquée.
- 123 Dans ces conditions, il a lieu de conclure que la référence à l'arrêt du 6 octobre 2020, *La Quadrature du Net e.a.* (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) n'est pas pertinente en l'espèce.
- 124 Cette conclusion ne saurait être remise en cause par la prise en compte de l'arrêt du 30 avril 2024, *La Quadrature du Net e.a.* (Données personnelles et lutte contre la contrefaçon) (C-470/21, EU:C:2024:370), sur lequel les parties à la présente affaire ont été invitées à se prononcer par le biais d'une mesure d'organisation de la procédure.
- 125 Ce qui était en cause dans l'affaire ayant donné lieu à l'arrêt du 30 avril 2024, *La Quadrature du Net e.a.* (Données personnelles et lutte contre la contrefaçon) (C-470/21, EU:C:2024:370) était la légalité de l'accès, par une autorité publique nationale chargée de la protection des droits d'auteur et des droits voisins contre les atteintes à ces droits commises sur Internet, aux données conservées par les fournisseurs de services de communications électroniques relatives à l'identité civile correspondant à des adresses IP à des fins de lutte contre la contrefaçon. Plus particulièrement, cet accès se justifiait en vue de l'objectif d'identifier le titulaire d'une adresse IP s'étant livré à une activité portant atteinte aux droits d'auteur ou aux droits voisins, dès lors qu'il avait illégalement mis à disposition sur Internet des œuvres protégées aux fins du téléchargement de celles-ci par d'autres personnes. Dans ces conditions, la Cour a jugé qu'un contrôle préalable par une juridiction ou par une entité administrative indépendante :
- ne devait pas être mis en place lorsque l'autorité nationale compétente avait accès aux données relatives à l'identité civile d'une personne correspondant à une adresse IP, à la seule fin d'identifier l'utilisateur concerné et sans que ces données puissent être associées à des informations relatives aux communications effectuées, dès lors que l'ingérence qui comportait un tel accès ne pouvait pas être qualifiée de grave (points 133 et 134 dudit arrêt) ;
 - devait être mis en place avant que l'autorité nationale compétente mette en relation les données d'identité civile d'une personne correspondant à une adresse IP et le fichier relatif à l'œuvre mise illégalement à disposition sur Internet en vue du téléchargement de celle-ci par d'autres personnes et qu'elle envoie à la personne concernée une lettre constatant que celle-ci s'était livrée à des faits illicites (voir, en ce sens, point 141 de cet arrêt).

- 126 Il s'ensuit que l'affaire ayant donné lieu à l'arrêt du 30 avril 2024, *La Quadrature du Net e.a.* (Données personnelles et lutte contre la contrefaçon) (C-470/21, EU:C:2024:370) porte sur l'accès, par les autorités nationales, à une adresse IP à des fins de lutte contre la contrefaçon et qu'un tel objet se distingue de la collecte en vrac, par les agences de renseignement, de données à caractère personnel en transit depuis l'Union. Dès lors, il ne saurait être considéré, au regard dudit arrêt, que la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union doit faire l'objet d'une autorisation préalable.
- 127 Il convient, ainsi, de rejeter le présent argument.
- 3) *Sur le troisième argument, fondé sur l'arrêt de la Cour EDH du 25 mai 2021, Big Brother Watch et autres c. Royaume-Uni (CE:ECHR:2021:0525JUD005817013)*
- 128 Par son troisième argument, le requérant fait valoir, en substance, que, dans l'arrêt de la Cour EDH du 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni* (CE:ECHR:2021:0525JUD005817013, ci-après l'« arrêt *Big Brother Watch* »), la Cour EDH a considéré que les activités d'interception en masse de données à caractère personnel devaient être soumises à l'autorisation préalable d'une autorité indépendante à partir du moment où étaient définis les objectifs et l'étendue de l'opération de surveillance. Selon lui la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union ne fait pas l'objet, en l'espèce, d'une telle autorisation préalable.
- 129 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.
- 130 Il y a lieu de relever que l'affaire ayant donné lieu à l'arrêt *Big Brother Watch* portait notamment sur la compatibilité, au regard de l'article 8 de la CEDH, du régime britannique de surveillance secrète qui donnait aux agences de renseignement la faculté d'intercepter en masse les communications électroniques et les données de communication associées, c'est-à-dire les données de trafic qui se rapportaient aux communications interceptées, qui étaient effectuées en principe hors des îles Britanniques.
- 131 En outre, comme cela ressort de la jurisprudence citée au point 29 ci-dessus, dans la mesure où l'article 8 de la CEDH consacre, au même titre que l'article 7 de la charte des droits fondamentaux, le droit au respect de la vie privée et familiale, la jurisprudence de la Cour EDH relative à l'article 8 de la CEDH doit être prise en compte pour interpréter la portée de l'article 7 de ladite charte. Il s'ensuit que, si le Tribunal devait juger que l'arrêt *Big Brother Watch* est pertinent en l'espèce, les considérations avancées par la Cour EDH dans cet arrêt, en ce qui concerne la portée de l'article 8 de la CEDH, devraient être prises en compte pour interpréter la portée de l'article 7 de cette charte.
- 132 À cet égard, il convient de rappeler que, dans l'arrêt *Big Brother Watch*, la Cour EDH s'est prononcée sur la légalité de l'interception en masse par les services de renseignement britanniques des communications électroniques et des données de communication associées qui étaient effectuées en principe hors des îles Britanniques.
- 133 Or, comme les parties à la présente affaire l'ont relevé dans leur réponse à la mesure d'organisation de la procédure et lors de l'audience, les développements avancés par la Cour EDH dans l'arrêt *Big Brother Watch* sont pertinents en l'espèce, dans la mesure où l'interception en masse de données à caractère personnel qui était en cause dans l'affaire ayant donné lieu audit arrêt peut être regardée comme incluant la collecte en vrac qui fait l'objet de la décision attaquée.
- 134 Premièrement, il y a lieu de relever que, alors que la version française de l'arrêt *Big Brother Watch* emploie l'expression « interception en masse » de données, la version anglaise utilise l'expression « bulk interception », qui correspond plus précisément à la notion française d'« interception en vrac ».
- 135 Deuxièmement, par opposition à l'interception ciblée, l'interception de renseignements en cause dans l'arrêt *Big Brother Watch* a été définie par la Cour EDH comme étant celle qui ne visait pas des personnes déterminées et, par conséquent, était susceptible d'affecter un grand nombre de personnes et de données de communication associées et ainsi d'avoir une portée très large, dès lors qu'elle

permettait notamment de recueillir des informations dans le cadre du renseignement extérieur et de détecter de nouvelles menaces provenant d'acteurs connus ou inconnus. De plus, selon ladite Cour, du fait de sa finalité liée à la protection de la sécurité nationale, l'interception en masse était généralement effectuée par les autorités compétentes dans le secret, ce qui impliquait que celles-ci ne rendaient publiques que peu d'informations sur le fonctionnement du système, voire aucune (voir, en ce sens, arrêt Big Brother Watch, point 322).

136 Troisièmement, dans l'arrêt Big Brother Watch, la Cour EDH a considéré que, bien que les régimes d'interception en masse n'étaient pas tous conçus sur le même modèle et que leurs modalités de mise en œuvre pouvaient changer sans toujours respecter un ordre chronologique strict, l'interception en masse était un processus graduel qui se déroulait, en substance, selon les quatre étapes suivantes (ci-après les « étapes de l'interception ») :

- a) l'interception en masse et la rétention initiale des communications électroniques appartenant à un grand nombre de personnes et des données de communication associées ;
- b) l'application de sélecteurs spécifiques aux communications retenues et aux données de communication associées afin d'identifier les communications susceptibles d'avoir un intérêt pour les services de renseignement ;
- c) l'examen, par des analystes, des communications sélectionnées et des données de communication associées ;
- d) la rétention subséquente des données et leur utilisation aux fins de leur inclusion dans un rapport de renseignement, de leur communication à d'autres services de renseignement du pays ou de leur transmission à des services de renseignement étrangers (voir, en ce sens, arrêt Big Brother Watch, points 325 à 329).

137 Il s'ensuit qu'une opération de collecte en vrac de données à caractère personnel, telle que celle faisant l'objet de la décision attaquée, entre dans le périmètre de la première des étapes de l'interception identifiées par la Cour EDH dans l'arrêt Big Brother Watch, dans la mesure où elle consiste à recueillir, à des fins de protection de la sécurité nationale, les données à caractère personnel en transit depuis l'Union d'un grand nombre de personnes.

138 Dans ce contexte, il convient de tirer les conséquences de l'arrêt Big Brother Watch dans le cadre de l'appréciation de la légalité d'une décision d'adéquation adoptée sur le fondement de l'article 45, paragraphe 3, du RGPD, telle que la décision attaquée.

139 À cet égard, en premier lieu, il convient de noter que, dans l'arrêt Big Brother Watch, la Cour EDH a précisé que l'article 8 de la CEDH n'interdisait pas de recourir à l'interception en masse afin de protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves et que les États jouissaient d'une ample marge d'appréciation pour déterminer le type de régime d'interception dont ils avaient besoin (arrêt Big Brother Watch, point 347).

140 En deuxième lieu, la Cour EDH a indiqué que l'interception en masse des données à caractère personnel devait être encadrée par plusieurs garanties de bout en bout qui, prises ensemble, constituaient la pierre angulaire de tout système d'interception en masse, à savoir :

- l'obtention de l'autorisation d'une autorité indépendante dès la définition de l'objet et de l'étendue de l'opération de surveillance en cause (arrêt Big Brother Watch, point 350) ;
- la mise en place d'un système de supervision et d'un contrôle juridictionnel indépendant a posteriori (voir, en ce sens, arrêt Big Brother Watch, points 336 et 347) ;
- la prévision de règles juridiques qui permettaient d'assurer, pour chacune des étapes de l'interception, la nécessité et la proportionnalité des mesures prises (voir, en ce sens, arrêt Big Brother Watch, point 350) ; à cet égard, ladite Cour a rappelé qu'une ingérence dans les droits garantis par l'article 8 de la CEDH ne pouvait se justifier au regard du paragraphe 2 de cet article que si elle était prévue par la loi, visait un ou plusieurs des buts légitimes énumérés dans ce

paragraphe et était nécessaire, dans une société démocratique, pour atteindre ces buts ; or, en matière de surveillance secrète, la prévisibilité des mesures adoptées impliquait que le droit interne était suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique était habilitée à recourir à de pareilles mesures (arrêt *Big Brother Watch*, points 332 et 333).

- 141 En troisième lieu, la Cour EDH a fait valoir que, si l'article 8 de la CEDH s'appliquait à chacune des étapes de l'interception, le besoin de prévoir des garanties augmentait au fur et à mesure que le processus franchissait ces différentes étapes et, par conséquent, que l'intensité de l'atteinte au droit au respect de la vie privée devenait plus important. Ainsi, selon elle, c'est à la fin du processus, lorsque des informations relatives à une personne en particulier sont analysées ou que le contenu de communications est examiné par un analyste, que la présence de garanties est plus que jamais nécessaire (voir, en ce sens, arrêt *Big Brother Watch*, points 330 et 331).
- 142 En quatrième lieu, la Cour EDH a considéré que, dans la mesure où inclure tous les sélecteurs employés par les agences de renseignement pour filtrer les communications collectées dans le périmètre de l'autorisation préalable n'était pas faisable en pratique, la portée de cette autorisation devait être limitée afin d'y inclure à tout le moins les types ou les catégories de sélecteurs à utiliser (arrêt *Big Brother Watch*, point 354).
- 143 En l'espèce, d'une part, il convient de rappeler que, comme cela a été jugé par la Cour dans les arrêts *Schrems I* et *Schrems II*, la Commission n'est pas tenue, dans le cadre d'une décision d'adéquation, de s'assurer que les dispositions pertinentes du pays tiers sont identiques à celles en vigueur dans l'Union, mais qu'elles sont substantiellement équivalentes (voir points 19 et 20 ci-dessus).
- 144 D'autre part, il y a lieu de considérer que, dès lors que la collecte en vrac de données à caractère personnel effectuée par les agences de renseignement des États-Unis, qui est contestée dans le cadre du présent litige, peut être assimilée à l'interception de données qui est effectuée dans le cadre de la première des étapes de l'interception précisées par la Cour EDH dans l'arrêt *Big Brother Watch*, le besoin de prévoir, pour cette phase spécifique de la collecte en vrac, des garanties limitant le pouvoir discrétionnaire des agences de renseignement est plus limité, compte tenu du contexte dans lequel l'interception est effectuée. En effet, ce qui est en cause en l'espèce est uniquement l'interception initiale en vrac de données à caractère personnel par des agences de renseignement, à l'exclusion des activités postérieures, qui ne font pas l'objet de ce recours et qui pourraient consister, le cas échéant, dans l'application de sélecteurs spécifiques, dans l'examen des données collectées et dans leur usage ou leur communication ultérieure.
- 145 Il s'ensuit que le fait de prévoir une autorisation préalable n'est pas la seule garantie devant entourer l'interception en masse de données à caractère personnel, mais constitue l'un des éléments qui, pris ensemble, constituent la pierre angulaire de tout régime d'interception en masse. À cet égard, il convient de rappeler que le droit des États-Unis en vigueur prévoit des règles juridiques encadrant de manière suffisamment claire et précise la mise en œuvre, par les agences de renseignement des États-Unis, de la collecte en vrac de données à caractère personnel (voir points 107 à 116 ci-dessus) et octroie aux personnes concernées par le transfert de leurs données le droit à un recours juridictionnel effectif devant la DPRC (voir points 33 à 63 ci-dessus). En outre, les considérants 162 à 169 de la décision attaquée indiquent, sans que le requérant le conteste, que les activités de renseignement menées par les agences de renseignement sont contrôlées par le PCLOB qui, comme cela ressort du point 54 ci-dessus, a été conçu par son statut fondateur comme une agence indépendante. De même, lesdites activités font l'objet d'une supervision, en premier lieu, de la part des responsables juridiques et des délégués qui, au sein de chaque agence de renseignement, sont chargés de la surveillance et du respect dudit droit, en deuxième lieu, de l'inspecteur général indépendant chargé, pour chaque agence de renseignement, de contrôler les activités de renseignement extérieur effectuées par l'agence en cause et, en troisième lieu, de l'Intelligence Oversight Board (Conseil de surveillance du renseignement, États-Unis), créé au sein du President's Intelligence Advisory Board (Conseil consultatif en matière de renseignement relevant du président, États-Unis) et tenu de superviser le respect de la loi par les autorités des États-Unis ainsi que, en quatrième lieu, des commissions spéciales instituées au sein du Congrès des États-Unis qui exercent des fonctions de surveillance à l'égard de toutes les activités de renseignement extérieur de ce pays.

146 Eu égard à ces considérations, il ne saurait être conclu que le fait de ne pas prévoir d'autorisation préalable s'appliquant à la collecte initiale en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union suffit pour considérer que le droit des États-Unis ne fournit pas, à la lumière des enseignements tirés de l'arrêt Big Brother Watch, des garanties substantiellement équivalentes à celles prévues par le droit de l'Union.

147 Il y a lieu, ainsi, de rejeter le présent argument.

4) Sur le quatrième argument, fondé sur l'avis 5/2023 du Contrôleur européen de la protection des données

148 Par son quatrième argument, le requérant fait valoir que, dans son avis 5/2023, du 28 février 2023, relatif au projet de décision d'exécution de la Commission constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE – États-Unis (ci-après l'« avis 5/2023 »), le Comité européen de la protection des données (ci-après le « CEPD ») a souligné l'importance d'assujettir la collecte en vrac de données à caractère personnel à une autorisation préalable. Selon lui, la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union ne fait pas l'objet, en l'espèce, d'une autorisation préalable.

149 La Commission, soutenue par l'Irlande et les États-Unis d'Amérique, conteste l'argument du requérant.

150 Il convient de noter que l'avis 5/2023 a été rendu par le CEPD sur le fondement de l'article 70, paragraphe 1, sous s), du RGPD. Cette disposition prévoit que, de sa propre initiative ou à la demande de la Commission, le CEPD peut rendre, au profit de cette dernière, un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers.

151 Or, lorsqu'il agit sur le fondement de l'article 70, paragraphe 1, du RGPD, le CEPD se limite à exercer une fonction de conseil par le biais de la rédaction d'avis, de lignes directrices, de recommandations et de recommandations de bonnes pratiques qui ne produisent pas d'effets juridiques obligatoires (voir, en ce sens, ordonnance du président de la Cour du 29 novembre 2023, CEPD/CRU, C-413/23 P, non publiée, EU:C:2023:1036, point 11). Ainsi, cet avis ne lie pas la Commission, qui reste libre d'apprécier si le droit de ce pays offre globalement un niveau de protection substantiellement équivalent à celui qui est garanti par le droit de l'Union en ce qui concerne la collecte en vrac de données à caractère personnel. En tout état de cause, il convient de constater que, dans ledit avis, le CEPD n'a pas indiqué que le défaut de mise en place d'un contrôle préalable relatif à la collecte en vrac de données à caractère personnel portait nécessairement atteinte à l'évaluation positive, de la part la Commission, du caractère adéquat du niveau de protection des données à caractère personnel offert par le CPD. Au contraire, il a relevé, au point 165 du même avis, que cette évaluation dépendait de toutes les circonstances de l'espèce et, notamment, de la mise en place par les États-Unis d'Amérique d'un contrôle judiciaire a posteriori et d'un mécanisme de recours.

152 Dans ce contexte, l'avis 5/2023 ne permet pas de considérer que la collecte en vrac, par les agences de renseignement des États-Unis, de données à caractère personnel en transit depuis l'Union doit faire l'objet d'une autorisation préalable et que la protection offerte par ce pays n'est pas substantiellement équivalente à celle qui est garantie par le droit de l'Union.

153 Il y a lieu, ainsi, de rejeter le présent argument et, partant, le deuxième grief du deuxième moyen dans son ensemble.

d) Sur le troisième grief du deuxième moyen, selon lequel l'E.O. 14086 donne au président des États-Unis le pouvoir d'autoriser une mise à jour secrète des objectifs spécifiques de la collecte en vrac

154 Par le troisième grief de son deuxième moyen, le requérant fait valoir que la Commission a violé les articles 7 et 8 de la charte des droits fondamentaux lorsqu'elle a considéré, dans la décision attaquée, que les États-Unis d'Amérique offraient un niveau de protection substantiellement équivalent à celui qui est garanti par le droit de l'Union en vertu du RGPD, lu à la lumière de ladite charte, malgré le fait

que l'E.O. 14086 donne au président des États-Unis, pour des raisons de sécurité nationale, la faculté d'autoriser une mise à jour secrète des objectifs spécifiques de la collecte en vrac. Plus particulièrement, il estime que, contrairement à ce qui a été jugé dans l'arrêt de la Cour EDH du 4 décembre 2015, *Roman Zakharov c. Russie* (CE:ECHR:2015:1204JUD004714306, ci-après l'« arrêt Zakharov »), l'attribution audit président du pouvoir de mettre à jour ces objectifs spécifiques ne permet pas aux personnes concernées par un transfert de données à caractère personnel d'identifier, de manière précise, le cadre juridique dans lequel celles-ci sont traitées aux États-Unis.

- 155 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.
- 156 Il convient de noter que, dans l'arrêt *Zakharov*, la Cour EDH a considéré qu'une ingérence dans le droit fondamental au respect de la vie privée et familiale ne pouvait se justifier au regard de l'article 8, paragraphe 2, de la CEDH que si elle était prévue par la loi (arrêt *Zakharov*, point 227). Or, selon ladite Cour, l'expression « prévue par la loi » signifiait que la mesure litigieuse devait être accessible à la personne concernée et qu'elle devait être prévisible quant à ses effets (arrêt *Zakharov*, point 228). En matière d'interception de communications, la « prévisibilité » ne signifiait pas qu'un individu devait se trouver à même de prévoir quand les autorités étaient susceptibles d'intercepter ses communications, mais que, en substance, les limitations à son droit au respect de la vie privée et familiale devaient résulter de règles claires (arrêt *Zakharov*, point 229).
- 157 Il convient également de rappeler que, conformément à la jurisprudence citée au point 29 ci-dessus, dans la mesure où l'article 8 de la CEDH consacre, au même titre que l'article 7 de la charte des droits fondamentaux, le droit au respect de la vie privée et familiale, la jurisprudence de la Cour EDH relative à l'article 8 de la CEDH, incluant donc l'arrêt *Zakharov*, doit être prise en compte pour interpréter, comme en l'espèce, l'article 7 de ladite charte.
- 158 À cet égard, il ressort de la section 2, sous c), ii), C) de l'E.O. 14086 que la faculté donnée au président des États-Unis de mettre à jour la liste des objectifs spécifiques de la collecte en vrac n'est pas illimitée, mais est circonscrite aux seules hypothèses où cette mise à jour est rendue nécessaire par l'émergence de nouveaux impératifs de sécurité nationale, tels que de nouvelles menaces ou des menaces accrues pour la sécurité nationale pour lesquelles la collecte en vrac de données à caractère personnel pourrait être utilisée. De plus, il ressort de cette disposition et il a été confirmé par les États-Unis d'Amérique lors de la l'audience que la mise à jour, par ledit président, desdits objectifs spécifiques n'est pas secrète, mais fait l'objet d'une publicité de la part du directeur du renseignement national, sauf si ce président considère que cette publicité constitue en soi un risque pour la sécurité nationale de son pays. En outre, même dans cette hypothèse, la collecte en vrac est assujettie à toutes les garanties et à toutes les limitations prévues par l'E.O. 14086 et, si une personne concernée introduit la réclamation concernant les données personnelles, celle-ci fait l'objet d'une surveillance de la part du CLPO et, le cas échéant, d'un réexamen par la DPRC.
- 159 Dans ce contexte, il ne saurait être considéré que la faculté donnée au président des États-Unis de mettre à jour la liste des objectifs spécifiques de la collecte en vrac est contraire aux exigences identifiées par la Cour EDH dans l'arrêt *Zakharov*.
- 160 Ainsi, il y a lieu de rejeter le troisième grief du deuxième moyen et, partant, ledit moyen dans son ensemble.

4. Sur le quatrième moyen, tiré de la violation de l'article 22 du RGPD

- 161 Par son quatrième moyen, le requérant soutient que la Commission a violé l'article 22 du RGPD dans la mesure où, dans la décision attaquée, elle a omis de prévoir une disposition établissant le droit des personnes concernées à ne pas faire l'objet de décisions fondées exclusivement sur le traitement automatisé de données à caractère personnel, incluant le profilage, produisant des effets juridiques à leur égard ou les affectant de manière significative (ci-après les « décisions entièrement automatisées »).
- 162 À titre liminaire, il convient de relever que les termes de l'article 22 du RGPD sont les suivants :

« 1. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

2. Le paragraphe 1 ne s'applique pas lorsque la décision :

- a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
- b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou
- c) est fondée sur le consentement explicite de la personne concernée. »

163 Il y a lieu également de noter que le terme « profilage », figurant à l'article 22, paragraphe 1, du RGPD, est défini à l'article 4, paragraphe 4, du même règlement comme étant « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

164 Il s'ensuit que, aux termes de l'article 22 du RGPD, toute personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé des données à caractère personnel, y compris lorsque cette mesure consiste à analyser et prédire certains aspects de son comportement.

165 Or, il ressort de la décision attaquée qu'elle ne traite pas spécifiquement de la question relative aux décisions entièrement automatisées.

166 Ainsi, il y a lieu de décider si une telle omission est susceptible d'affecter la légalité de la décision attaquée, dans la mesure où elle pourrait remettre en question la conclusion figurant à l'article 1^{er} de ladite décision, selon laquelle les États-Unis d'Amérique offrent un niveau adéquat de protection des données à caractère personnel.

167 C'est dans ce contexte qu'il convient d'analyser les trois griefs soulevés par le requérant au soutien de son quatrième moyen, en commençant par les premier et troisième griefs qu'il convient d'examiner ensemble.

a) Sur les premier et troisième griefs du quatrième moyen, selon lesquels, d'une part, le fait que les décisions entièrement automatisées soient généralement adoptées par des responsables du traitement qui, étant établis dans l'Union, sont assujettis au RGPD ne donne pas de garantie en ce qui concerne les autres cas et, d'autre part, l'établissement, par le droit des États-Unis, de protections sectorielles dans les cas où l'adoption des décisions entièrement automatisées ne rentre pas dans le champ d'application dudit règlement est sans pertinence en l'espèce

168 Par les premier et troisième griefs de son quatrième moyen, le requérant soutient, d'une part, que le fait que les décisions entièrement automatisées soient généralement adoptées par des responsables du traitement qui, étant établis dans l'Union, sont assujettis au RGPD ne donne pas de garantie en ce qui concerne les autres cas. D'autre part, il relève que la circonstance selon laquelle le droit des États-Unis offre des protections sectorielles dans l'hypothèse où l'adoption de telles décisions ne rentre pas dans le champ d'application dudit règlement est sans pertinence en l'espèce, dans la mesure où cette circonstance ne permet pas de conclure que, sur le plan général, la protection que ce pays offre concernant toutes les décisions entièrement automatisées est équivalente à celle qui est garantie par l'article 22 de ce règlement.

169 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

- 170 Il convient de relever qu'il ressort du considérant 33 de la décision attaquée que, en cas de transfert de données à caractère personnel depuis l'Union vers les États-Unis, trois cas de figure doivent être distingués en ce qui concerne l'adoption des décisions entièrement automatisées.
- 171 Premièrement, il se peut que les décisions entièrement automatisées soient adoptées par un responsable du traitement établi dans l'Union qui a collecté, dans l'Union, les données personnelles des personnes concernées. À cet égard, il convient de noter que l'article 4, paragraphe 7, du RGPD définit le responsable du traitement comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel. Dans cette hypothèse, dans la mesure où, conformément à l'article 3, paragraphe 1, dudit règlement, le responsable du traitement est assujéti au même règlement, il doit respecter les exigences prévues par l'article 22 de ce règlement en ce qui concerne de telles décisions.
- 172 Deuxièmement, il se peut que les décisions entièrement automatisées soient adoptées soit par un sous-traitant établi dans un pays tiers, agissant au nom du responsable du traitement établi dans l'Union qui lui a transféré les données à caractère personnel qu'il a collectées dans l'Union, soit par un sous-traitant ultérieur, agissant au nom du sous-traitant établi dans l'Union qui lui a transféré les données qu'il a collectées dans l'Union. À cet égard, il convient de préciser que l'article 4, paragraphe 8, du RGPD définit le sous-traitant comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Dans ces hypothèses, dans la mesure où les sous-traitants étrangers agissent au nom du responsable du traitement ou du sous-traitant de l'Union, ils sont assujéttis audit règlement en vertu de l'article 3, paragraphe 1, de ce règlement. Ainsi, s'agissant de telles décisions, le responsable du traitement et le sous-traitant doivent se conformer aux exigences prévues par l'article 22 du même règlement.
- 173 Troisièmement, il se peut que les décisions entièrement automatisées soient adoptées par un responsable du traitement ou un sous-traitant qui ne sont pas établis dans l'Union, mais qui s'adresse à des personnes concernées qui se trouvent dans l'Union en leur offrant des biens ou des services ou en suivant leur comportement. Or, dans cette hypothèse, l'article 3, paragraphe 2, du RGPD prévoit que le responsable du traitement et le sous-traitant étranger sont assujéttis audit règlement. Ainsi, s'agissant des décisions entièrement automatisées, ils doivent se conformer aux exigences prévues par l'article 22 dudit règlement.
- 174 Il s'ensuit qu'il ressort de la décision attaquée que les hypothèses dans lesquelles les décisions entièrement automatisées ne rentrent pas dans le champ d'application de l'article 22 du RGPD sont résiduelles et se limitent au cas où les organisations du CPD collectent directement, dans l'Union, les données à caractère personnel, sans toutefois offrir aux citoyens de l'Union des biens ou des services et sans suivre leur comportement, au sens de l'article 3, paragraphe 2, dudit règlement.
- 175 Or, il ressort des considérants 35 et 36 de la décision attaquée, sans que le requérant le conteste, que, dans ces hypothèses, le droit des États-Unis offre des protections sectorielles semblables à celles prévues par le RGPD dans les domaines tels que l'octroi de crédits, les offres de prêts immobiliers, les décisions de recrutement, l'emploi, le logement et l'assurance, dans lesquels il est plus probable que les organisations du CPD adoptent des décisions entièrement automatisées.
- 176 Ainsi, en matière de crédit à la consommation, le Fair Credit Reporting Act (Loi sur l'information loyale en matière de crédit) et l'Equal Credit Opportunity Act (Loi sur l'égalité des chances en matière de crédit) contiennent des garanties qui offrent aux consommateurs une forme de droit à l'explication et un droit de contestation des décisions entièrement automatisées. Ces lois s'appliquent à un grand nombre de domaines tels que le crédit, l'emploi, le logement et l'assurance. En outre, le titre VII du Civil Rights Act (Loi sur les droits civils) et le Fair Housing Act (Loi sur le logement équitable) protègent les personnes physiques contre les modèles utilisés dans les décisions entièrement automatisées qui pourraient donner lieu à une discrimination sur la base de certaines caractéristiques et leur accordent le droit de contester de telles décisions. De plus, en ce qui concerne les informations relatives à la santé, les règles adoptées par les autorités des États-Unis en application du Health Insurance Portability and Accountability Act (Loi sur la portabilité et la responsabilité en matière

d'assurance maladie) exigent que les prestataires médicaux reçoivent des informations leur permettant d'informer les personnes des systèmes de prise de décisions entièrement automatisés utilisés dans le secteur médical.

177 Dans ce contexte, contrairement à ce que fait valoir le requérant, il ne saurait être considéré que les protections sectorielles prévues par le droit des États-Unis sont sans pertinence en l'espèce, dès lors qu'elles n'ont pas la même portée générale que l'article 22 du RGPD.

178 À cet égard, il convient de rappeler que, dans les arrêts Schrems I et Schrems II, la Cour a jugé que, sans exiger que le pays tiers concerné garantisse un niveau de protection identique à celui qui était garanti dans l'ordre juridique de l'Union, l'expression « niveau de protection adéquat », figurant à l'article 45, paragraphe 1, du RGPD, devait être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui qui est garanti au sein de l'Union en vertu dudit règlement, lu à la lumière de la charte des droits fondamentaux (voir points 19 et 20 ci-dessus).

179 De plus, dans l'arrêt Schrems I, la Cour a considéré que, même si les moyens auxquels le pays tiers avait recours pour assurer un niveau adéquat de protection des données à caractère personnel pouvaient être différents de ceux mis en œuvre au sein de l'Union, ces moyens devaient néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle qui est garantie au sein de l'Union (voir point 20 ci-dessus).

180 Eu égard à l'ensemble de ces considérations, il y a lieu de rejeter les premier et troisième griefs du quatrième moyen.

b) Sur le deuxième grief du quatrième moyen, selon lequel l'étude commanditée par la Commission en 2018, qui démontrait la nature résiduelle des cas dans lesquels les organisations établies aux États-Unis ayant adhéré au bouclier de protection adoptaient des décisions entièrement automatisées, est sans pertinence en l'espèce

181 Par le deuxième grief de son quatrième moyen, le requérant soutient que le fait que l'étude concernant les décisions entièrement automatisées, citée au considérant 34 de la décision attaquée, que la Commission avait commanditée en 2018 et dont les résultats figurent au point 4.1.5 du rapport COM(2018) 860 final de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le second examen annuel du fonctionnement du bouclier de protection (ci-après l'« étude de 2018 »), a conclu qu'il n'existait pas de preuve de l'existence de décisions entièrement automatisées adoptées par des organisations établies aux États-Unis ayant adhéré au bouclier de protection est sans pertinence en l'espèce. Plus particulièrement, il fait valoir que ladite étude se réfère à la décision d'adéquation concernant le bouclier de protection qui a été annulée par la Cour dans l'arrêt Schrems II et qu'elle ne prend pas en compte la situation actuelle, qui se caractérise par un développement extrêmement rapide des services entièrement automatisés basés sur l'intelligence artificielle.

182 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

183 Il ressort notamment de l'étude de 2018 que, d'une part, aucune donnée ne permettait, à l'époque, de considérer que les entreprises établies aux États-Unis qui avaient adhéré au bouclier de protection avaient adopté des décisions entièrement automatisées et, d'autre part, les États-Unis d'Amérique avaient mis en œuvre des législations sectorielles dans les domaines tels que le crédit à la consommation, l'emploi, le logement, l'assurance et la santé, dans lesquels il était plus probable que des décisions entièrement automatisées soient adoptées.

184 À cet égard, en premier lieu, il convient de noter que l'étude de 2018 n'est pas citée dans la décision d'adéquation concernant le bouclier de protection et a été commanditée par la Commission après l'entrée en vigueur de ladite décision. Le fait que cette décision ait été annulée par la Cour dans l'arrêt Schrems II est donc sans pertinence en l'espèce. En outre, dans l'arrêt Schrems II, la Cour n'a pas annulé ladite décision sur la base des éléments indiqués dans ladite étude.

185 En deuxième lieu, certes, l'étude de 2018 n'a pas pris en compte la situation factuelle et juridique présente aux États-Unis en 2023, à la date d'adoption de la décision attaquée, mais celle présente en 2018, lorsqu'elle a été réalisée. Toutefois, la nature résiduelle des cas dans lesquels des organisations établies aux États-Unis ayant adhéré au bouclier de protection avaient adopté des décisions entièrement automatisées a été confirmée par le rapport COM(2019) 495 final de la Commission au Parlement européen et au Conseil, du 23 octobre 2019, sur le troisième examen annuel du fonctionnement du bouclier de protection. En effet, dans ce rapport, il était notamment indiqué que le nombre d'organisations établies aux États-Unis participant au bouclier de protection qui avaient adopté des décisions entièrement automatisées était limité et que les décisions prises par ces organisations n'avaient généralement pas d'effets juridiques et ne produisaient pas d'autres effets vis-à-vis des personnes concernées.

186 En troisième lieu, il convient de noter que, dans ses écritures, le requérant n'a fourni aucun élément de preuve permettant de considérer que, après la réalisation de l'étude de 2018, des organisations établies aux États-Unis ont adopté des décisions entièrement automatisées et n'a pas expliqué à suffisance de droit la raison pour laquelle l'évolution de l'intelligence artificielle priverait de pertinence ladite étude.

187 Dans ce contexte, il y a lieu de rejeter le deuxième grief du quatrième moyen et, partant, ledit moyen dans son ensemble.

5. Sur le cinquième moyen, tiré de la violation de l'article 32 du RGPD, lu en combinaison avec l'article 45, paragraphe 2, du même règlement

188 Par son cinquième moyen, le requérant fait valoir que la Commission a violé l'article 32 du RGPD, lu en combinaison avec l'article 45, paragraphe 2, du même règlement, dans la mesure où, dans la décision attaquée, elle a considéré que les États-Unis d'Amérique offraient un niveau de protection substantiellement équivalent à celui qui est garanti dans l'Union concernant la mise en place, par les responsables du traitement et les sous-traitants établis aux États-Unis, des mesures techniques et organisationnelles adéquates visant à garantir la sécurité du traitement des données à caractère personnel transférées depuis l'Union vers ce pays.

189 À cet égard, en premier lieu, le requérant fait valoir que le point II.4 sous a), de l'annexe 1 de la décision attaquée se limite à prévoir que les organisations du CPD doivent prendre des mesures de sécurité raisonnables et appropriées exclusivement lorsqu'elles créent, maintiennent, utilisent ou disséminent des données à caractère personnel. Ainsi, aucune mesure de sécurité ne serait exigée lorsque ces organisations consultent des données à caractère personnel provenant de l'Union. Le requérant soutient que la consultation fait pourtant partie des opérations incluses dans la notion de « traitement » des données à caractère personnel figurant à l'article 4, paragraphe 2, du RGPD.

190 En second lieu, le requérant soutient que le point III.6, sous f), de l'annexe 1 de la décision attaquée prévoit l'obligation, pour les organisations établies aux États-Unis qui sortent du CPD, de continuer à respecter les principes figurant dans cette décision, y compris ceux relatifs à la sécurité du traitement, aussi longtemps qu'elles stockent, utilisent ou divulguent des données à caractère personnel transférées depuis l'Union vers les États-Unis, mais ne prévoit pas une telle obligation lorsque ces mêmes organisations consultent des données à caractère personnel.

191 La Commission, soutenue par l'Irlande et par les États-Unis d'Amérique, conteste l'argumentation du requérant.

192 À titre liminaire, tout d'abord, il y a lieu de rappeler que les termes de l'article 32 du RGPD sont les suivants :

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

- b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. »

193 Ensuite, le terme « traitement », figurant à l'article 32 du RGPD, est défini à l'article 4, paragraphe 2, du même règlement comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

194 Selon la jurisprudence, il ressort notamment de l'expression « toute opération », figurant à l'article 4, paragraphe 2, du RGPD, que le législateur de l'Union a entendu donner à la notion de « traitement » une portée large, ce qui est corroboré par le caractère non exhaustif, exprimé par la locution « telles que », des opérations énumérées à ladite disposition (voir arrêt du 7 mars 2024, Endemol Shine Finland, C-740/22, EU:C:2024:216, point 29 et jurisprudence citée).

195 Enfin, il y a lieu de relever que, parmi les éléments que la Commission doit prendre en compte lorsqu'elle évalue, au titre de l'article 45, paragraphe 2, sous a), du RGPD, le niveau de protection offert par un pays tiers, figurent les mesures de sécurité concernant les données à caractère personnel mises en œuvre par ce pays.

196 C'est dans ce contexte qu'il convient d'examiner, ensemble, les deux arguments soulevés par le requérant au soutien du présent moyen.

197 À cet égard, il convient de rappeler que les termes du point II.4, sous a), de l'annexe 1 de la décision attaquée sont les suivants :

« Les organisations qui créent, gèrent, utilisent ou diffusent des données à caractère personnel doivent prendre des mesures raisonnables et adéquates pour éviter la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction de ces données, en prenant dûment en considération les risques liés au traitement et la nature des données à caractère personnel. »

198 De plus, les termes du point III.6, sous f), de l'annexe 1 de la décision attaquée sont les suivants :

« Une organisation doit appliquer les principes à toutes les données à caractère personnel reçues depuis l'Union sur la foi du [CPD]. L'engagement d'adhérer aux principes n'est pas limité dans le temps en ce qui concerne les données à caractère personnel reçues au cours de la période durant laquelle l'organisation bénéficie des avantages du [CPD] ; son engagement signifie qu'elle continuera à appliquer les principes à ces données aussi longtemps qu'elle stockera, utilisera ou divulguera celles-ci, même si elle quitte ultérieurement le [CPD] pour quelque raison que ce soit. »

199 Il s'ensuit que les points II.4, sous a) et III.6, sous f) de l'annexe 1 de la décision attaquée ne concernent pas toute forme de traitement des données à caractère personnel, au sens de l'article 4, paragraphe 2, du RGPD. Au contraire, d'une part, le premier desdits points limite l'obligation des organisations du CPD d'adopter des mesures de sécurité aux seules hypothèses dans lesquelles elles créent, gèrent, utilisent ou diffusent des données à caractère personnel. D'autre part, le second desdits points prévoit que les organisations qui quittent le CPD doivent continuer à appliquer les principes

figurant dans la décision attaquée aussi longtemps qu'elles stockent, utilisent ou divulguent des données à caractère personnel transférées depuis l'Union vers les États-Unis.

200 Or, premièrement, il y a lieu de rappeler que, dans les arrêts Schrems I et Schrems II, la Cour a considéré qu'il n'était pas nécessaire que le pays tiers assure une protection juridique identique à celle qui est garantie dans l'ordre juridique de l'Union (voir points 19 et 20 ci-dessus). Il s'ensuit que, si, dans la décision attaquée, la Commission estime que le droit des États-Unis en vigueur au moment de l'adoption de cette décision garantit un niveau de protection substantiellement équivalent à celui prévu en droit de l'Union, il n'est pas nécessaire que ladite décision contienne exactement les mêmes termes que ceux figurant dans le RGPD.

201 Deuxièmement, les principes figurant dans le point II.4, sous a), de l'annexe 1 de la décision attaquée doivent être interprétés à la lumière des éléments figurant au considérant 23 de ladite décision, qui, de manière similaire à l'article 32 du RGPD, prévoit ce qui suit :

« Les données à caractère personnel devraient en outre être traitées d'une manière garantissant leur sécurité, y compris leur protection contre tout traitement non autorisé ou illicite et contre toute perte, toute destruction ou tout dégât d'origine accidentelle. À cette fin, les responsables du traitement et les sous-traitants devraient prendre les mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre d'éventuelles menaces. Ces mesures devraient être évaluées en tenant compte de l'état de la technique, des coûts y afférents ainsi que de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits des personnes. »

202 Troisièmement, il y a lieu de relever que les termes « créer », « gérer », « utiliser » et « diffuser » figurant au point II.4, sous a), de l'annexe 1 de la décision attaquée ainsi que les termes « stocker », « utiliser » et « divulguer » figurant au point III.6, sous f), de la même annexe constituent des manifestations spécifiques de l'opération consistant dans le « traitement » des données à caractère personnel, au sens de l'article 32 du RGPD, et que, au même titre que celui-ci, ils visent à couvrir un large éventail d'opérations concernant les données à caractère personnel.

203 Quatrièmement, le terme « utiliser », qui figure tant dans le point II.4, sous a), de l'annexe 1 de la décision attaquée que dans le point III.6, sous f), de la même annexe se définit comme le fait de recourir à quelque chose pour un but ou un usage précis. Dans cette optique, l'utilisation des données à caractère personnel inclut leur consultation, dans la mesure où, par définition, pour pouvoir recourir à des données, il est nécessaire au préalable d'y avoir accès et donc de les consulter. Il en découle que l'argument du requérant selon lequel aucune mesure de sécurité n'est exigée dans la décision attaquée lorsque des organisations du CPD consultent des données à caractère personnel provenant de l'Union n'est pas fondé.

204 Eu égard à l'ensemble de ces éléments, il y a lieu de rejeter le cinquième moyen et, partant, le recours dans son intégralité.

IV. Sur les dépens

205 Aux termes de l'article 134, paragraphe 1, du règlement de procédure, toute partie qui succombe est condamnée aux dépens, s'il est conclu en ce sens.

206 La Commission ayant conclu à la condamnation du requérant et celui-ci ayant succombé, il y a lieu de le condamner à supporter, outre ses propres dépens, ceux exposés par la Commission, y compris dans le cadre de la procédure en référé.

207 Par ailleurs, en vertu de l'article 138, paragraphe 1, du règlement de procédure, les États membres et les institutions qui interviennent au litige supportent leurs propres dépens. Par conséquent, l'Irlande supportera ses propres dépens.

208 En outre, aux termes de l'article 138, paragraphe 3, du règlement de procédure, le Tribunal peut décider qu'une partie intervenante autre que celles mentionnées aux paragraphes 1 et 2 de cet article

supportera ses propres dépens. En l'espèce, il y a lieu de décider que les États-Unis d'Amérique supporteront leurs propres dépens.

Par ces motifs,

LE TRIBUNAL (dixième chambre élargie)

déclare et arrête :

- 1) **Le recours est rejeté.**
- 2) **M. Philippe Latombe supportera ses propres dépens ainsi que ceux exposés par la Commission européenne, y compris dans le cadre de la procédure en référé.**
- 3) **L'Irlande supportera ses propres dépens.**
- 4) **Les États-Unis d'Amérique supporteront leurs propres dépens.**

Porchia

Jaeger

Madise

Nihoul

Verschuur

Ainsi prononcé en audience publique à Luxembourg, le 3 septembre 2025.

Le greffier

La présidente

V. Di Bucci

O. Porchia

* Langue de procédure : le français.