Avis 5/2023 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE–États-Unis

Adopté le 28 février 2023

Résumé

Le 13 décembre 2022, la Commission européenne a publié un projet de décision d'adéquation (ci-après le «projet de décision»), qui comprend des annexes constituant un nouveau cadre pour les échanges transatlantiques de données à caractère personnel, le cadre de protection des données entre l'Union européenne et les États-Unis (ci-après le «CPD»), destiné à remplacer l'ancien bouclier de protection des données, invalidé par la Cour de justice de l'Union européenne (ci-après la «CJUE») le 16 juillet 2020, dans l'affaire Schrems II. La composante essentielle du CPD réside dans les principes du cadre de protection des données UE–États-Unis, notamment les principes complémentaires (ci-après dénommés collectivement les «principes du CPD»).

Conformément à l'article 70, paragraphe 1, point s), du règlement (UE) 2016/679[1] du Parlement européen et du Conseil (ci-après le «RGPD»), la Commission a demandé l'avis du comité européen de la protection des données (ci-après l'«EDPB») sur le projet de décision.

L'EDPB a évalué le caractère adéquat du niveau de protection offert aux États-Unis, sur la base de l'examen du projet de décision. L'EDPB a évalué à la fois les aspects commerciaux et l'accès aux données à caractère personnel transférées depuis l'UE par les autorités publiques aux États-Unis, ainsi que leur utilisation.

L'EDPB a tenu compte du cadre juridique de l'UE applicable en matière de protection des données, tel qu'énoncé dans le RGPD, ainsi que des droits fondamentaux à la vie privée et à la protection des données consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne et à l'article 8 de la convention européenne des droits de l'homme. Il a également examiné le droit à un recours effectif et à accéder à un tribunal impartial consacré à l'article 47 de la charte, ainsi que la jurisprudence relative aux différents droits fondamentaux.

En outre, l'EDPB a pris en compte les exigences des critères de référence pour l'adéquation qu'il a adoptés[2].

L'objectif principal de l'EDPB est de donner un avis à la Commission sur le caractère adéquat du niveau de protection accordé aux personnes dont les données à caractère personnel sont transférées vers les États-Unis. Il importe de noter que l'EDPB ne s'attend pas à ce que le cadre juridique américain reproduise la législation européenne en matière de protection des données.

Toutefois, l'EDPB rappelle que, pour être considéré comme assurant un niveau de protection adéquat, l'article 45 du RGPD et la jurisprudence de la CJUE exigent que la législation du pays tiers offre aux personnes concernées un niveau de protection substantiellement équivalent à celui garanti dans l'Union.

1.1. Aspects généraux de la protection des données

Le CPD prévoit que l'adhésion des organisations CPD aux principes de ce cadre peut être limitée dans certains cas (par exemple, dans la mesure nécessaire pour se conformer à une décision de justice ou

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

[2] GT art. 29, Critères de référence pour l'adéquation, WP 254 rev.01, 28 novembre 2017, tels que révisés et adoptés en dernier lieu le 6 février 2018, approuvés par l'EDPB le 25 mai 2018 (ci-après les «critères de référence pour l'adéquation»).

pour répondre à l'intérêt public). Afin de mieux cerner l'incidence de ces exemptions sur le niveau de protection des personnes concernées, l'EDPB recommande à la Commission d'inclure dans le projet de décision des précisions sur le champ d'application des exemptions, notamment sur les garanties applicables en vertu du droit américain.

L'EDPB note que la structure des annexes et leur numérotation rendent les informations assez difficiles à trouver et à y faire référence. Cela contribue à la complexité de la présentation globale du nouveau cadre, qui rassemble dans ses annexes des documents ayant une valeur juridique différente, et pourrait ne pas favoriser une bonne compréhension des principes du CPD par les personnes concernées, les organisations CPD et les autorités de l'UE chargées de la protection des données. L'EDPB souligne également que la terminologie devrait être utilisée de manière cohérente dans l'ensemble du CPD. De même, la définition de certains termes essentiels fait défaut[3].

L'EDPB se félicite des mises à jour apportées aux principes du CPD[4], qui constitueront le cadre juridique contraignant pour les organisations chargées du CPD, mais note qu'en dépit d'un certain nombre de modifications et d'explications supplémentaires apportées dans les considérants du projet de décision, les principes du CPD auxquels les organisations chargées du CPD doivent adhérer restent pour l'essentiel inchangés en ce qui concerne ceux applicables dans le cadre du bouclier de protection des données (sur lesquels se fondaient les examens conjoints annuels du groupe de travail article 29 (ci-après le «GT art. 29») et de l'EDPB). Les principes du CPD sont également, dans une large mesure, les mêmes que ceux du projet de bouclier de protection des données sur lequel le GT art. 29 a fondé son avis de 2016[5]. En ce qui concerne les principes du CPD qui sont substantiellement inchangés, l'EDPB estime qu'il n'est pas nécessaire de répéter toutes les observations formulées précédemment par le GT art. 29. L'EDPB a décidé de se concentrer sur des aspects spécifiques qu'il juge encore plus pertinents aujourd'hui, compte tenu de l'évolution de l'environnement juridique et technologique.

Par exemple, l'EDPB note que certains sujets de préoccupation précédemment soulevés par le GT art. 29 et l'EDPB en ce qui concerne les principes du bouclier de protection des données restent d'actualité. Il s'agit en particulier des droits des personnes concernées (par exemple, certaines exceptions au droit d'accès et au calendrier et aux modalités du droit d'opposition), de l'absence de définitions clés, du manque de clarté en ce qui concerne l'application des principes du CPD aux sous-traitants et de la large dérogation pour les informations accessibles au public[6].

L'EDPB tient également à rappeler que le niveau de protection des personnes dont les données sont transférées ne doit pas être compromis par des transferts ultérieurs du destinataire initial des données transférées[7]. L'EDPB invite une fois de plus la Commission à préciser que les garanties imposées par le destinataire initial à l'importateur dans le pays tiers doivent être effectives à l'égard de la législation du pays tiers, avant un transfert ultérieur dans le cadre du CPD.

Les évolutions rapides dans le domaine de l'automatisation de la prise de décision et du profilage — de plus en plus au moyen des technologies de l'IA — requièrent une attention particulière. L'EDPB se

[3] Tel est le cas des termes «agent» et «sous-traitant». En outre, la notion de «données relatives aux ressources humaines (RH)» doit encore être examinée avec les autorités américaines.

[4] Par exemple, la clarification selon laquelle les données codées sont des données à caractère personnel.

[5] Groupe de travail «article 29», avis 01/2016 sur le projet de décision d'adéquation du bouclier de protection des données UE–États-Unis, adopté le 13 avril 2016 (ci-après l'«avis 01/2016 du GT 29»).

[6] Bouclier de protection des données UE–États-Unis — Troisième examen annuel conjoint, rapport de l'EDPB adopté le 12 novembre 2019, paragraphe 11.

[7] Critères de référence pour l'adéquation du RGPD, 3.A.9.

félicite des références faites par la Commission aux garanties spécifiques prévues par la législation américaine pertinente dans différents domaines[8]. Toutefois, le niveau de protection des particuliers semble varier en fonction des règles sectorielles spécifiques éventuelles qui s'appliquent à la situation en cause. L'EDPB maintient que des règles spécifiques concernant la prise de décision automatisée sont nécessaires afin de fournir des garanties suffisantes, y compris le droit pour la personne de connaître la logique sous-jacente, de contester la décision et d'obtenir une intervention humaine lorsque la décision lui porte préjudice de manière significative.

L'EDPB rappelle l'importance d'une surveillance et d'une application effectives du CPD et estime que les contrôles de conformité en ce qui concerne les exigences davantage liées à des questions de fond sont essentiels. Ces aspects feront l'objet d'un suivi attentif de la part de l'EDPB, notamment dans le cadre des examens périodiques. L'EDPB prend note des engagements renouvelés figurant dans les lettres de la Commission fédérale du commerce (*Federal Trade Commission*, ci-après la «FTC»)[9] et du ministère des transports (*Department of Transportation*, ci-après le «DOT»)[10] en ce qui concerne la mise en œuvre, par exemple en vue de donner la priorité à l'enquête sur les violations présumées du CPD.

L'EDPB note que sept voies de recours sont offertes aux personnes concernées de l'UE si leurs données à caractère personnel sont traitées en violation du CPD. Ces mécanismes de recours sont les mêmes que ceux inclus dans l'ancien bouclier de protection des données, qui avait fait l'objet de commentaires de la part du GT art. 29[11]. L'efficacité de ces mécanismes de recours fera l'objet d'un suivi attentif de la part de l'EDPB, notamment dans le cadre des examens périodiques.

1.2. Accès et utilisation par les autorités publiques aux États-Unis des données à caractère personnel transférées à partir de l'Union européenne

Dans le projet de décision, la Commission européenne conclut que «toute atteinte aux droits fondamentaux des particuliers dont les données à caractère personnel sont transférées de l'Union européenne vers les États-Unis par des autorités publiques américaines pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale, en vertu du cadre de protection des données UE–États-Unis, sera limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé, et qu'il existe une protection juridique effective contre les atteintes de cette nature»[12].

La Commission européenne parvient à sa conclusion après une évaluation approfondie du décret présidentiel n° 14086 renforçant les garanties pour les activités américaines de renseignement d'origine électromagnétique (*executive order* 14086, ci-après «EO 14086»). L'EO 14086 a été publié par le président des États-Unis le 7 octobre 2022, à la suite de négociations menées par la Commission européenne avec le gouvernement américain à la suite de l'invalidation de la précédente décision d'adéquation, appelée bouclier de protection des données, par la Cour de justice de l'Union européenne (CJUE).

L'EDPB se féliciterait que non seulement l'entrée en vigueur, mais aussi l'adoption de la décision soient subordonnées, entre autres, à l'adoption de politiques et de procédures actualisées par toutes les agences de renseignement américaines pour mettre en œuvre l'EO 14086. L'EDPB recommande à la

[8] Voir le considérant 35 du projet de décision.
[9] Projet de décision, annexe IV.
[10] Projet de décision, annexe V.
[11] Voir en particulier l'avis 01/2016 du GT art. 29, section 2.2.6, point a).
[12] Voir le considérant 195 du projet de décision.

Commission d'évaluer ces politiques et procédures actualisées et de communiquer cette évaluation au comité.

En ce qui concerne l'accès des pouvoirs publics aux données à caractère personnel transférées aux États-Unis, l'EDPB a concentré son analyse sur l'évaluation du nouvel EO 14086, étant donné qu'il est effectivement destiné à remédier aux déficits constatés par la CJUE dans son arrêt Schrems II lorsqu'il a conclu à l'invalidité de la décision d'adéquation précédente.

L'EDPB reconnaît que le cadre juridique américain pour les activités de renseignement d'origine électromagnétique a été modifié par l'adoption de l'EO 14086 et considère que les garanties supplémentaires figurant dans ce décret ordre constituent une amélioration significative. L'EO 14086 introduit les notions de nécessité et de proportionnalité dans le cadre juridique américain en matière de renseignement d'origine électromagnétique et prévoit, si l'UE devait être désignée comme organisation d'intégration économique régionale éligible, un nouveau mécanisme de recours pour les citoyens de l'UE. L'EDPB estime que le nouveau mécanisme de recours est considérablement amélioré par rapport au précédent mécanisme de médiation prévu dans le cadre du bouclier de protection des données. Contrairement au cadre juridique précédent, qui ne créait pas de droits pour les citoyens de l'Union, comme l'a explicitement relevé la CJUE, le nouvel EO 14086 crée de tels droits et offre davantage de garanties pour l'indépendance de la Cour de contrôle de la protection des données, ainsi que des pouvoirs plus efficaces pour remédier aux violations.

En comparant les garanties supplémentaires de l'EO 14086 aux garanties essentielles européennes (GEE) élaborées par l'EDPB, comme la norme élaborée sur la base de la jurisprudence de la CJUE et de la Cour européenne des droits de l'homme (CEDH), l'EDPB a malgré tout recensé, dans son évaluation, un certain nombre de points nécessitant des éclaircissements supplémentaires, demandant une attention particulière ou suscitant des préoccupations. Ces points reflètent le fait que, si l'EDPB a fondé son avis sur l'arrêt Schrems II, la portée de l'évaluation de l'EDPB inclut nécessairement des considérations allant au-delà des conclusions spécifiques de l'arrêt Schrems II.

L'EDPB estime qu'il est nécessaire de clarifier davantage les questions relatives, en particulier, à la «collecte massive temporaire», ainsi qu'à la poursuite de la conservation et de la diffusion des données collectées (en masse) dans le cadre juridique américain.

Étant donné que le test de l'équivalence essentielle n'est pas un test d'identité et que les garanties incluses dans le nouveau cadre juridique sur le renseignement d'origine électromagnétique ont été renforcées, le principal point d'attention et de préoccupation de l'EDPB se concentre sur une évaluation des garanties dans leur intégralité, selon une approche globale couvrant les garanties pour l'ensemble du cycle de traitement, depuis la collecte de données jusqu'à la diffusion des données, y compris les éléments de surveillance et de recours.

À cet égard, l'EDPB souligne les constatations suivantes:

Si l'EDPB reconnaît que l'EO 14086 introduit les notions de nécessité et de proportionnalité dans le cadre juridique du renseignement d'origine électromagnétique, il souligne la nécessité de suivre de près les effets de ces modifications dans la pratique, y compris le réexamen des politiques et procédures internes mettant en œuvre les garanties du décret présidentiel au niveau des agences.

L'EDPB se félicite également du fait que l'EO 14086 contient une liste de finalités spécifiques pour lesquelles la collecte peut ou ne peut pas avoir lieu, tout en notant que les objectifs peuvent être mis à jour en y ajoutant des objectifs supplémentaires, qui ne sont pas nécessairement publics, compte tenu des nouveaux impératifs de sécurité nationale.

À titre d'exemple de déficit dans le cadre actuel, l'EDPB a notamment constaté que le cadre juridique américain, lorsqu'il autorise la collecte de données en masse en vertu du décret présidentiel n° 12333, n'exige pas l'autorisation préalable d'une autorité indépendante, comme l'exige la jurisprudence la plus récente de la Cour européenne des droits de l'homme, ni ne prévoit un contrôle indépendant systématique ex post par une juridiction ou un organe indépendant équivalent. En ce qui concerne l'autorisation préalable indépendante de surveillance au titre de l'article 702 de la loi sur la surveillance et le renseignement étranger (ci-après la «FISA»), l'EDPB regrette que la Cour FISA (ci-après la «FISC») n'examine pas une demande de programme aux fins de la conformité avec l'EO 14086 lors de la certification du programme autorisant le ciblage de personnes non américaines, même si les autorités de renseignement qui mettent en œuvre le programme sont liées par celui-ci. De l'avis de l'EDPB, les garanties supplémentaires contenues dans ce décret devraient néanmoins être prises en compte, y compris par la FISC. L'EDPB rappelle que les rapports du Conseil de surveillance de la vie privée et des libertés civiles (ci-après le «PCLOB») seraient particulièrement utiles pour évaluer comment les garanties de l'EO 14086 seront mises en œuvre et comment ces garanties sont appliquées lorsque les données sont collectées au titre de l'article 702 de la FISA et de l'EO 12333.

En ce qui concerne le mécanisme de recours, l'EDPB reconnaît des améliorations significatives en ce qui concerne les pouvoirs de la Cour de contrôle de la protection des données (ci-après la «DPRC») et son indépendance accrue par rapport au médiateur. L'EDPB reconnaît également les garanties supplémentaires prévues dans le nouveau mécanisme de recours, telles que le rôle des avocats spéciaux, qui comprend la défense de l'intérêt du plaignant ainsi que le réexamen du mécanisme de recours par le PCLOB. Tout en tenant compte de la nature de la sécurité nationale et des garanties prévues dans l'EO 14086, l'EDPB est néanmoins préoccupé par l'application générale de la réponse standard de la DPRC notifiant au plaignant soit qu'aucune violation couverte n'a été constatée, soit qu'une décision nécessitant une réparation appropriée a été émise, et qu'elle n'est pas susceptible de recours, prise dans son ensemble. Compte tenu de l'importance du mécanisme de recours, l'EDPB invite la Commission à suivre de près le fonctionnement pratique de ce mécanisme.

L'EDPB attend de la Commission qu'elle donne suite à son engagement de suspendre, d'abroger ou de modifier la décision d'adéquation pour des raisons d'urgence, en particulier si l'exécutif américain décidait de restreindre les garanties incluses dans le décret présidentiel[13].

Dans l'ensemble, l'EDPB note avec satisfaction les améliorations substantielles apportées par le décret présidentiel par rapport au cadre juridique antérieur, notamment en ce qui concerne l'introduction des principes de nécessité et de proportionnalité et le mécanisme de recours individuel pour les personnes concernées de l'UE. Compte tenu des préoccupations exprimées et des clarifications requises, l'EDPB suggère que ces préoccupations soient prises en compte et que la Commission fournisse les éclaircissements demandés afin de consolider les motifs du projet de décision et d'assurer un suivi étroit de la mise en œuvre concrète de ce nouveau cadre juridique, en particulier des garanties qu'il prévoit, lors des futurs examens conjoints.

[13] Voir le considérant 212 du projet de décision.

Table des matières

Le comité européen de la protection des données

Le comité européen de la protection des données a adopté la déclaration suivante:

vu l'article 70, paragraphe 1, point s), 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/CE (ci-après le «RGPD»)[1],

vu l'accord sur l'Espace économique européen, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[2],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ L'AVIS SUIVANT:

1 INTRODUCTION

1.1 Le cadre des États-Unis relatif à la protection des données

1. Les États-Unis d'Amérique (ci-après les «États-Unis») et l'Union européenne (ci-après l'«UE») ont des approches différentes en matière de respect de la vie privée et de protection des données. Alors que le respect de la vie privée et la protection des données dans l'UE sont des droits fondamentaux garantis par les articles 7 et 8 de la charte européenne des droits fondamentaux, la protection des données aux États-Unis est généralement envisagée du point de vue de la protection des consommateurs. En conséquence, les approches réglementaires aux États-Unis et dans l'UE diffèrent[3].

2. Contrairement à l'approche globale de l'UE adoptée par le RGPD, aux États-Unis, il n'existe pas de loi générale globale sur la protection des données au niveau fédéral. La protection de la vie privée aux États-Unis est plutôt assurée par une approche sectorielle et étatique. Par exemple, certains secteurs spécifiques sont couverts par des actes spécifiques, par exemple:

   - La *Health Insurance Portability and Accountability Act* (HIPAA)[4]

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE), JO L 119 du 4.5.2016, p. 1.

[2] Dans le présent avis, on entend par «États membres» les États membres de l'EEE.

[3] Voir également le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil constatant le niveau de protection adéquat des données à caractère personnel en vertu du cadre de protection des données UE–États-Unis, publié le 13 décembre 2022 (ci-après le «projet de décision»), annexe I, section I.

[4] La loi sur la portabilité et la responsabilité de l'assurance maladie de 1996 (HIPAA) est une loi fédérale américaine. Elle établit des normes nationales pour protéger les informations sensibles sur la santé des patients. L'objectif de l'HIPAA est de protéger de manière adéquate les informations relatives à la santé des personnes,

- La *Children's Online Privacy Protection Act* (COPPA)[5]
- La *Gramm-Leach-Billey Act* (GLBA)[6]

3. Dans le domaine de l'accès des pouvoirs publics aux données à caractère personnel transférées de l'UE vers les États-Unis, un certain nombre de bases juridiques, de limitations et de garanties différentes s'appliquent. Les procédures juridiques d'accès à l'information à des fins répressives découlent soit directement de la Constitution américaine (le quatrième amendement), soit du droit écrit et procédural, ou des lignes directrices et des politiques du ministère de la justice au niveau fédéral ou au niveau des États. L'accès à l'information à des fins de sécurité nationale est régi par plusieurs instruments juridiques, et notamment par la loi sur la surveillance et le renseignement étranger (la «FISA»), le décret présidentiel n° 12333, le décret présidentiel n° 14086 récemment adopté ainsi que le règlement relatif au procureur général (ci-après le «règlement AG»)[7] instituant une Cour de contrôle de la protection des données (la «DPRC»).

4. Le 13 décembre 2022, la Commission a publié son projet de décision d'exécution de la Commission conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil constatant le niveau de protection adéquat des données à caractère personnel en vertu du cadre de protection des données entre l'Union européenne et les États-Unis (ci-après le «projet de décision»), qui contient en annexe le cadre de protection des données UE–États-Unis (ci-après le «CPD»). Pour les raisons exposées ci-dessus, le projet de décision n'est pas fondé sur un cadre juridique fédéral spécifique et complet, mais sur le CPD.

5. Le CPD fonctionne comme suit: *«Le ministère américain du commerce (ci-après le "ministère") publie les principes du cadre de protection des données UE–États-Unis, y compris les principes supplémentaires (ci-après dénommés collectivement les «principes») et l'annexe I des principes (ci-*

---

tout en permettant la circulation d'informations sur la santé en vue de la fourniture et de la promotion de soins de santé de haute qualité. L'HIPAA régit l'utilisation et la divulgation d'informations relatives à la santé par les entités soumises au *Privacy Rule* (règlement sur le respect de la vie privée). Elle comprend également des normes relatives au droit des personnes de comprendre et de contrôler la manière dont leurs informations relatives à la santé sont utilisées.
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] L'objectif premier de la loi sur la protection de la vie privée en ligne des enfants (COPPA) est de permettre aux parents de contrôler quelles sont les informations à caractère personnel collectées sur leurs enfants de moins de 13 ans auprès des opérateurs de sites web et services en ligne destinés aux enfants (y compris les applications mobiles et les dispositifs de l'internet des objets, tels que les jouets intelligents) ou de sites grand public. La COPPA exige que ces opérateurs envoient une notification parentale et doivent obtenir un consentement parental vérifiable. Cela vaut également pour les données provenant d'enfants étrangers si les sites web ou les services sont exploités aux États-Unis et soumis à la COPPA. Dans le même temps, les règlements s'appliquent également aux sites web et aux services basés à l'étranger s'ils s'adressent à des enfants aux États-Unis. Voir: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions et projet de décision, annexe IV, p. 3.

[6] L'un des objectifs de la loi Gramm-Leach-Bliley est de protéger la vie privée des consommateurs dans le secteur financier. La GLBA impose aux établissements financiers d'expliquer à leurs clients leurs pratiques en matière de partage d'informations et de créer des garanties pour protéger l'information des clients (par exemple, pour les entreprises réglementées par la FTC en vertu de la règle de sauvegarde de la FTC). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] Décret du procureur général n° 5517-2022, qui modifie les règlements du ministère américain de la justice tels qu'ils ont été autorisés et ordonnés par l'EO 14086.

après l'"annexe I"), sous son autorité légale pour encourager, promouvoir et développer le commerce international (titre 15 du code des États-Unis, article 1512)»[8].

6. L'élaboration des «principes» (ci-après les «principes du CPD») a été menée en concertation avec la Commission européenne (ci-après la «Commission»), l'industrie et d'autres parties prenantes afin d'atteindre l'objectif de facilitation du commerce et des échanges[9] entre l'UE et les États-Unis, tout en veillant à ce que les personnes concernées bénéficient d'un niveau de protection substantiellement équivalent à celui garanti dans l'Union.

7. Les principes du CPD sont décrits comme un «élément clé» du CPD. D'une part, ils fournissent un «mécanisme prêt à l'emploi» pour les transferts de données de l'UE vers les États-Unis. D'autre part, les données à caractère personnel transférées de l'UE vers les États-Unis sont préservées et protégées, comme l'exige le droit de l'Union.

8. Le CPD ne s'applique qu'aux organisations américaines qui se sont autocertifiées conformément aux exigences du cadre (ci-après les «organisations CPD»). Pour l'instant, cela n'est possible que si elles relèvent de la compétence de la Commission fédérale du commerce (*Federal Trade Commission*, ci-après la «FTC») ou du ministère des transports (*Department of Transportation*, ci-après le «DoT»). À l'avenir, d'autres organes statutaires — compétents pour superviser la mise en œuvre des principes du CPD — pourraient être ajoutés dans une future annexe.

9. Il est expliqué dans les principes du CPD que les conditions du cadre sont exécutoires i) par la FTC en vertu de l'article 5 de la *Federal Trade Commission Act* (ci-après la «FTCA») interdisant les actes déloyaux ou trompeurs dans le commerce ou nuisant au commerce[10], ii) par le DoT en vertu du titre 49 du code des États-Unis, article 41712, interdisant à un transporteur ou à un agent de billeterie de pratiquer des pratiques déloyales ou trompeuses dans le domaine du transport aérien en vue de la vente ou du transport aérien ou iii) en vertu d'autres dispositions législatives ou réglementaires interdisant de tels actes.

10. Il est souligné dans les principes du CPD que ni le RGPD n'est affecté dans son application, ni les obligations existantes en matière de protection de la vie privée, appliquées par ailleurs en vertu du droit américain, ne sont limitées par les principes du CPD.

1.2 Portée de l'évaluation de l'EDPB

11. Le projet de décision reflète l'évaluation du CPD par la Commission, qui est le résultat des discussions avec le gouvernement américain. Conformément à l'article 70, paragraphe 1, point s), du RGPD, l'EDPB doit rendre un avis sur les conclusions de la Commission en ce qui concerne le caractère adéquat du niveau de protection dans un pays tiers et, si nécessaire, s'efforcer de formuler des propositions pour résoudre tout problème.

12. L'EDPB se félicite des mises à jour apportées aux principes du CPD[11], qui constitueront le cadre juridique contraignant pour les organisations CPD. Toutefois, l'EDPB note que les principes du CPD

[8] Projet de décision, annexe I, section I.
[9] Ibidem.
[10] Titre 15 du code des États-Unis, article 45, point a).
[11] Par exemple, la clarification selon laquelle les données codées sont des données à caractère personnel.

restent essentiellement les mêmes que ceux du bouclier de protection des données[12] [sur lesquels se fondaient les examens annuels conjoints du groupe de travail article 29 (ci-après le «GT art. 29») et de l'EDPB]. Les principes du CPD sont également, dans une large mesure, les mêmes que ceux du projet de bouclier de protection des données sur lequel le GT art. 29 a fondé son avis de 2016[13] (ci-après l'«avis 01/2016 du GT art. 29»). En ce qui concerne les principes du CPD qui sont substantiellement inchangés, l'EDPB estime qu'il n'est pas nécessaire de répéter toutes les observations formulées précédemment par le GT art. 29. L'EDPB a décidé de se concentrer sur des aspects spécifiques qu'il juge encore plus pertinents aujourd'hui, compte tenu de l'évolution de l'environnement juridique et technologique.

13. En outre, conformément à la jurisprudence de la CJUE[14], une partie très importante de l'analyse porte sur le régime juridique de l'accès des pouvoirs publics aux données à caractère personnel transférées vers les États-Unis.

14. Dans son évaluation, l'EDPB a tenu compte du cadre européen applicable en matière de protection des données, y compris les articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), qui protègent respectivement le droit à la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à accéder à un tribunal impartial, et l'article 8 de la convention européenne des droits de l'homme (ci-après la «CEDH»), qui protège le droit à la vie privée et familiale. Outre ce qui précède, l'EDPB a examiné les exigences du RGPD, la jurisprudence pertinente et les critères de référence pour l'adéquation adoptés par l'EDPB (ci-après les «critères de référence pour l'adéquation du RGPD»)[15].

15. Cet exercice a pour objectif de donner un avis à la Commission sur l'évaluation du caractère adéquat du niveau de protection fournir par le CPD. Ce concept de «niveau de protection adéquat», qui existait déjà au titre de la directive 95/46/CE, a été développé par la CJUE. Il importe dès lors de rappeler la norme définie par la CJUE dans ses arrêts Schrems I[16] (invalidant la «sphère de sécurité») et Schrems II[17] (invalidant le bouclier de protection des données).

16. Dans l'arrêt Schrems I, la CJUE a jugé que si le «niveau de protection» dans le pays tiers doit être «substantiellement équivalent» à celui garanti dans l'Union, *«les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union»*[18]. Par conséquent, l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles et fondamentales de la législation objet de

[12] Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis (JO L 207 du 1.8.2016, p. 1).

[13] Groupe de travail «article 29», avis 01/2016 sur le projet de décision d'adéquation du bouclier de protection des données UE–États-Unis, adopté le 13 avril 2016 (ci-après l'«avis 01/2016 du GT art. 29»).

[14] En particulier: Arrêt de la Cour de justice du 6 octobre 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, et arrêt de la Cour de justice du 16 juillet 2020, Data Protection Commissioner/Facebook Ireland Limited et Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] GT art. 29, Critères de référence pour l'adéquation, WP 254 rev.01, 28 novembre 2017, tels que révisés et adoptés en dernier lieu le 6 février 2018, approuvés par l'EDPB le 25 mai 2018 (ci-après les «critères de référence pour l'adéquation du RGPD»).

[16] Arrêt Schrems I de la Cour de justice du 6 octobre 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 (ci-après l'«arrêt Schrems I de la CJUE»).

[17] Arrêt de la Cour de justice du 16 juillet 2020, Data Protection Commissioner/Facebook Ireland Limited et Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (ci-après l'«arrêt Schrems II de la CJUE»).

[18] Arrêt Schrems I de la CJUE, points 73 et 74.

l'examen. L'adéquation peut être obtenue en combinant les droits des personnes concernées et les obligations de ceux qui traitent les données à caractère personnel ou qui exercent un contrôle sur ce traitement et la supervision par des organes indépendants. Toutefois, les règles sur la protection des données ne sont efficaces que si elles sont applicables et suivies en pratique. Il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou vers une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données[19].

17. Dans son arrêt Schrems II, la CJUE a estimé que les lois sur la base desquelles les autorités de renseignement américaines peuvent accéder aux données à caractère personnel transférées aux États-Unis (article 702 FISA/EO 12333) restreignent de manière disproportionnée les droits consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») et ne sont donc pas encadrées d'une manière qui satisfasse à des exigences substantiellement équivalentes à celles requises, en vertu du droit de l'Union, par l'article 52, paragraphe 1, deuxième phrase, de la charte[20].

18. En outre, la CJUE a statué que le cadre juridique antérieur ne fournissait pas de garanties substantiellement équivalentes à celles exigées par l'article 47 de la charte, étant donné que le mécanisme du médiateur ne pouvait compenser le fait que ni la directive présidentielle PPD-28 ni l'EO 12333 n'accordent à des personnes non américaines un recours effectif[21]. Le médiateur n'était pas indépendant du pouvoir exécutif et n'avait pas le pouvoir d'adopter des décisions contraignantes à l'égard des services de renseignement américains[22].

19. L'EO 14086, qui remplace généralement la PPD-28, a introduit deux nouvelles exigences en droit américain qui font écho à l'arrêt Schrems II de la CJUE: d'une part, que les activités de renseignement d'origine électromagnétique ne sont menées que dans la mesure nécessaire pour faire progresser une collecte de renseignements prioritaire validée et uniquement dans la mesure et d'une manière qui soient proportionnées à la priorité validée en matière de renseignement; et, d'autre part, un mécanisme de recours.

20. Dans cet avis, l'EDPB évalue en particulier dans quelle mesure le CPD ainsi que l'EO 14086 récemment adopté répondent effectivement aux conclusions formulées par la CJUE dans son arrêt.

1.3 Commentaires généraux et inquiétudes

1.3.1 Évaluation du droit interne

21. L'EDPB croit comprendre que l'évaluation contenue dans le projet de décision porte sur les principes du CPD. Néanmoins, l'EDPB apprécierait de recevoir des informations sur le contexte juridique américain dans lequel les organisations DPF opèrent. Cela permettrait de mieux comprendre l'interaction entre le CPD et le droit américain. Par exemple, l'annexe I, point 1[23], indique que les principes du CPD ne *«(...) limitent pas les obligations en matière de protection de la vie privée qui s'appliquent par ailleurs en vertu du droit américain»*, sans décrire ces obligations.

[19] Critères de référence pour l'adéquation du RGPD, p. 2.
[20] Arrêt Schrems II de la CJUE, points 184 et 185.
[21] Arrêt Schrems II de la CJUE, point 192.
[22] Arrêt Schrems II de la CJUE, point 195.
[23] Projet de décision, annexe I, section I, dernière phrase.

1.3.2 Engagements internationaux pris par les États-Unis

22. En vertu de l'article 45, paragraphe 2, point c), du RGPD et des critères de référence pour l'adéquation dans le cadre du RGPD, lorsqu'elle évalue le caractère adéquat du niveau de protection d'un pays tiers, la Commission tient compte, entre autres, des engagements internationaux pris par le pays tiers ou d'autres obligations découlant de la participation du pays tiers à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel, ainsi que de l'application de ces obligations.

23. Les États-Unis sont partie à plusieurs accords internationaux qui garantissent le droit à la vie privée, tels que le pacte international relatif aux droits civils et politiques (article 17), la convention relative aux droits des personnes handicapées (article 22) et la convention relative aux droits de l'enfant (article 16). En outre, les États-Unis, en tant que membre de l'OCDE, adhèrent au cadre de protection de la vie privée de l'OCDE, en particulier aux lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel. Le 14 décembre 2022, la déclaration de l'OCDE sur l'accès des pouvoirs publics aux données à caractère personnel détenues par des entités du secteur privé a été adoptée par des ministres et des représentants de haut niveau des membres de l'OCDE et de l'Union européenne. Les États-Unis sont également partie à la convention de Budapest sur la cybercriminalité.

24. En outre, les États-Unis sont membre du système transfrontalier de protection de la vie privée (CBPR) de la coopération économique Asie-Pacifique (ci-après la «CEAP»), qui est une certification de confidentialité des données soutenue par les pouvoirs publics, à laquelle les entreprises peuvent adhérer pour démontrer qu'elles respectent les règles internationalement reconnues en matière de protection de la vie privée. Ces règles de protection de la vie privée ont été approuvées par les dirigeants de la CEAP.

25. L'EDPB prend également note de la participation des États-Unis, en tant qu'État observateur, aux travaux du comité consultatif de la convention n° 108 du Conseil de l'Europe.

26. En outre, l'EDPB prend note et se félicite de la participation continue des organismes américains au format nouvellement établi en 2021 de la «table ronde des autorités du G7 chargées de la protection des données et de la protection de la vie privée» (ci-après la «table ronde des APD du G7»), qui réunit des autorités indépendantes de protection des données et de contrôle de la vie privée des pays du G7. Dans ce contexte, ils ont soutenu, par exemple, le dernier communiqué[24] de la table ronde des APD du G7 adopté le 8 septembre 2022 à Bonn, en Allemagne, qui était axé sur le concept de «libre circulation des données en toute confiance».

1.3.3 Progrès dans le domaine de la législation américaine en matière de protection des données

27. L'EDPB prend particulièrement note de l'évolution de la législation relative à la protection des données au niveau des États aux États-Unis. L'EDPB se félicite de l'adoption de lois sur la protection des données

[24] Table ronde des autorités du G7 chargées de la protection des données et de la vie privée, «Promouvoir la libre circulation des données avec confiance et partage des connaissances sur les perspectives des espaces internationaux de données», 8 septembre 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

qui sont entrées en vigueur ou entreront en vigueur d'ici à 2023 dans cinq États (Californie, Colorado, Connecticut, Virginia et Utah)[25]..

28. L'EDPB note également que des initiatives correspondantes ont déjà été lancées dans de nombreux autres États américains en vue de l'adoption de nouvelles lois nationales.

29. En outre, l'EDPB salue explicitement les efforts déployés en ce qui concerne l'initiative bipartisane en faveur d'une loi fédérale sur la protection des données, à savoir la loi sur la vie privée et la protection des données américaines (American Data Privacy and Protection Act — ADPPA).

1.3.4 Portée du projet de décision

30. Conformément à l'article 1er du projet de décision, la Commission conclut que les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées de l'UE vers des organisations établies aux États-Unis qui figurent dans la «liste du cadre de protection des données», qui est tenue à jour et mise à la disposition du public par le ministère américain du commerce, conformément à l'annexe I, section I.3[26].

31. Le CPD est accessible aux sociétés relevant de la compétence de la FTC ou du DoT. Il est souligné que d'autres organes statutaires américains dotés de pouvoirs similaires pourraient être ajoutés à l'avenir[27].

1.3.5 Limitations de l'obligation d'adhérer aux principes du CPD

32. L'annexe I, point I.5, prévoit que l'adhésion des organisations CPD aux principes du CPD peut être limitée, entre autres, i) dans la mesure nécessaire pour se conformer à une décision de justice ou pour satisfaire à des exigences d'intérêt public, d'application de la loi[28] ou de sécurité nationale[29] (y compris lorsque la loi ou la réglementation gouvernementale créent des obligations contradictoires) et ii) par une loi, une ordonnance judiciaire ou une réglementation gouvernementale créant des autorisations explicites, à condition que, dans l'exercice de cette autorisation, une organisation CPD puisse démontrer que son non-respect des principes du CPD est limité à la mesure nécessaire pour répondre aux intérêts légitimes supérieurs poursuivis par cette autorisation.

33. En l'absence de connaissance complète du droit américain tant au niveau fédéral qu'au niveau des États, il est difficile pour l'EDPB d'évaluer en détail le champ d'application des exemptions énumérées dans ce paragraphe. Par conséquent, l'EDPB recommande à la Commission d'inclure dans le projet de décision des précisions sur le champ d'application des exemptions, y compris sur les garanties applicables en vertu du droit américain, afin de mieux cerner l'incidence de ces exemptions sur le niveau de protection des personnes concernées. L'EDPB souligne également que la Commission devrait

[25] *California Consumer Privacy Act* (2018; en vigueur le 1er janvier 2020); *California Privacy Rights Act* (2020; pleinement opérationnelle le 1er janvier 2023); *Colorado Privacy Act* (2021; en vigueur le 1er juillet 2023); *Connecticut Data Privacy Act* (2022; en vigueur le 1er juillet 2023); *Virginia Consumer Data Protection Act* (2021; en vigueur le 1er janvier 2023); *Utah Consumer Privacy Act* (2022; en vigueur le 31 décembre 2023).

[26] Projet de décision, considérations finales, article 1er, p. 57. L'EDPB croit comprendre que le projet de décision ne couvrira pas les transferts provenant d'entités situées en dehors de l'UE mais soumises au RGPD en vertu de l'article 3, paragraphe 2, du RGPD vers des entités certifiées aux États-Unis.

[27] Projet de décision, annexe I, section I.2.

[28] Voir la section 3.1 du présent avis pour de plus amples commentaires sur l'utilisation des données à caractère personnel couvertes par le CPD UE–États-Unis à des fins répressives.

[29] Voir la section 3.2 du présent avis pour de plus amples commentaires sur l'utilisation des données à caractère personnel couvertes par le CPD UE–États-Unis à des fins de sécurité nationale.

être informée de l'application et de l'adoption de toute loi ou de tout règlement gouvernemental susceptible d'avoir une incidence sur l'adhésion aux principes du CPD et qu'elle devrait en contrôler l'application et l'adoption.

1.3.6 Modifications concernant le «bouclier de protection des données»

34. L'EDPB salue les efforts déployés pour répondre aux exigences de l'arrêt Schrems II. Néanmoins, l'EDPB aurait accueilli favorablement le fait que, si d'autres questions avaient été recensées i) dans l'avis 01/2016 du GT art. 29 et ii) lors des examens conjoints précédents[30], celles-ci aient été également abordées à l'occasion des négociations du CPD.

35. L'EDPB note également qu'en dépit d'un certain nombre de modifications et d'explications supplémentaires apportées dans les considérants du projet de décision, les principes du CPD auxquels les organisations CPD doivent adhérer restent pour l'essentiel inchangés en ce qui concerne ceux applicables dans le cadre du bouclier de protection des données.

1.3.7 Manque de clarté des documents du CPD

36. L'EDPB note que la structure des annexes et leur numérotation rendent les informations assez difficiles à trouver et à y faire référence. Cela contribue à la complexité de la présentation globale du nouveau cadre, qui rassemble dans ses annexes des documents ayant une valeur juridique différente, et pourrait ne pas favoriser une bonne compréhension des principes du CPD par les personnes concernées, les organisations CPD et les autorités de l'UE chargées de la protection des données (ci-après les «APD de l'UE»).

37. L'EDPB souligne également que la terminologie devrait être utilisée de manière cohérente dans l'ensemble du CPD. Tel n'est pas le cas actuellement, par exemple, de la notion de «traitement». En effet, certaines parties du CPD énumèrent certains types d'opérations de traitement de données au lieu d'utiliser le terme «traitement». Il peut en résulter une insécurité juridique et d'éventuelles lacunes en matière de protection[31].

38. L'EDPB se félicite que les définitions de certains des termes utilisés figurent dans le CPD[32]. Toutefois, ce n'est pas le cas pour d'autres termes essentiels, tels qu'au moins «agent» ou «sous-traitant», qui, de l'avis de l'EDPB, justifient une définition claire et spécifique à l'annexe I, point I 8, du CPD, et sur lesquels les États-Unis et l'UE sont d'accord, afin d'éviter toute confusion à un stade ultérieur pour les organisations CPD qui s'appuient sur le CPD, les autorités de contrôle et le grand public.

---

[30] Examens annuels: Bouclier de protection des données UE–États-Unis — Premier examen conjoint annuel, WP 255, rapport du GT art. 29 adopté le 28 novembre 2017 (ci-après le «premier rapport d'examen conjoint»); Bouclier de protection des données UE–États-Unis — Deuxième examen conjoint annuel, rapport de l'EDPB adopté le 22 janvier 2019 (ci-après le «deuxième rapport d'examen conjoint»); Bouclier de protection des données UE–États-Unis — Troisième examen conjoint annuel, rapport de l'EDPB adopté le 12 novembre 2019 (ci-après le «troisième rapport d'examen conjoint»).

[31] Par exemple i) selon le libellé du projet de décision, annexe I, section III.6. f), les principes du CPD ne seraient applicables que lorsque l'organisation «stocke, utilise ou divulgue» les données reçues (c'est-à-dire pas pour d'autres opérations couvertes par le terme «traitement», telles que la collecte, l'enregistrement, la modification, l'extraction, la consultation ou l'effacement) et ii) conformément à l'annexe I, section II.4. a) du projet de décision, la sécurité des données ne serait imposée que pour «créer, conserver, utiliser ou diffuser» des informations à caractère personnel.

[32] Projet de décision, annexe I, section I 8.

39. En ce qui concerne la question des divergences d'interprétation entre l'UE et les États-Unis sur la notion de données relatives aux ressources humaines (RH), l'EDPB souscrit au troisième rapport d'examen de la Commission en ce qui concerne l'objectif de poursuivre les discussions avec les autorités américaines[33].

2 ASPECTS GÉNÉRAUX DE LA PROTECTION DES DONNÉES

2.1 Principes généraux

2.1.1 Concepts

40. Sur la base des critères de référence pour l'adéquation au RGPD, des concepts et/ou des principes fondamentaux en matière de protection des données devraient exister dans le cadre juridique du pays tiers. Ceux-ci ne doivent pas refléter la terminologie du RGPD, mais ils devraient refléter les concepts consacrés par la législation européenne en matière de protection des données et être cohérents avec ces concepts. Par exemple, le RGPD inclut les notions importantes suivantes: «données à caractère personnel», «traitement des données à caractère personnel», «responsable du traitement», «sous-traitant», «destinataire» et «données sensibles». L'EDPB se félicite que les définitions des termes «données à caractère personnel», «traitement» et «responsable du traitement» soient incluses dans le CPD, comme c'était le cas dans le bouclier de protection des données.

41. L'EDPB note qu'il est malaisé de déterminer dans quelle mesure les principes du CPD sont applicables aux organisations CPD qui reçoivent des données à caractère personnel de l'UE à des fins de «simple traitement» (dénommées «agents» ou «sous-traitants»). Le CPD ne fait pas de distinction entre les principes du CPD applicables aux agents et les principes du CPD applicables aux responsables du traitement, tandis que plusieurs des obligations figurant dans ces principes ne conviennent pas aux agents/sous-traitants. Par exemple, un agent/sous-traitant ne devrait pas être en mesure de fournir aux personnes tous les éléments de la notification complète, comme l'exige le principe de la notification (par exemple, les finalités pour lesquelles il recueille et utilise des informations à caractère personnel les concernant)[34], étant donné qu'un agent/sous-traitant ne peut déterminer seul les moyens et les finalités du traitement[35].

2.1.2 Le principe de limitation de la finalité

42. Les critères de référence pour l'adéquation au RGPD, conformément au RGPD, prévoient que les données à caractère personnel devraient être traitées pour une finalité spécifique et ensuite utilisées uniquement dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

43. Le principe d'intégrité des données et de limitaton des finalités dispose qu'une organisation ne peut traiter des informations à caractère personnel d'une manière incompatible avec les finalités pour lesquelles elles ont été collectées ou autorisées ultérieurement par la personne concernée[36]. L'EDPB

[33] Troisième rapport d'examen conjoint, pages 5, 15-16 et 30. Voir également le document de travail des services de la Commission accompagnant le rapport de la Commission au Parlement européen et au Conseil sur le troisième examen annuel du fonctionnement du bouclier de protection des données UE–États-Unis, pp. 17-18.
[34] Projet de décision, annexe I, section II.1 a).
[35] Voir également l'avis 01/2016 du GT art. 29, p. 16.
[36] Projet de décision, annexe I, section II.5.

fait observer qu'une terminologie différente est utilisée dans le cadre des principes «Notification», «Choix» et «Intégrité des données et limitation des finalités». Comme l'indique le GT art. 29 et malgré des précisions utiles dans les considérants du projet de décision, des termes tels que «finalités différentes», finalités «substantiellement différente» ou «utilisation qui n'est pas cohérente avec» sont utilisés dans le CPD sans définition claire de ces notions dans ce document, ce qui pourrait entraîner une insécurité juridique.

2.1.3 Droits d'accès, de rectification, d'effacement et d'opposition

44. Dans le CPD, les droits d'accès, de rectification et d'effacement des personnes concernées sont couverts par le principe d'accès[37].

45. Le principe d'accès reste inchangé par rapport au bouclier de protection des données. Par conséquent, certains sujets de préoccupation exprimés dans l'avis 01/2016 du GT art. 29 sont toujours valables, comme indiqué ci-dessous.

46. En ce qui concerne le droit d'accès des personnes, l'EDPB estime nécessaire de rappeler qu'il serait préférable d'intégrer les détails relatifs à l'obligation de répondre aux demandes des particuliers dans le texte principal du principe (ils sont encore uniquement décrits dans une note de bas de page[38]). En outre, il devrait être clair que l'accès devrait être accordé dans la mesure où une organisation CPD traite des informations à caractère personnel, et pas seulement lorsqu'elle les «stocke»[39]. De l'avis de l'EDPB, la formulation actuelle pourrait conduire à une interprétation restrictive du droit d'accès.

47. En ce qui concerne la liste des exceptions au droit d'accès[40], certaines ont encore tendance à faire pencher la balance vers les intérêts des organisations CPD. L'EDPB demeure préoccupé par le fait que, dans ces cas, il ne semble pas nécessaire de tenir compte des droits et des intérêts de la personne[41].

48. Un autre point qui a antérieurement suscité la préoccupation du GT art. 29[42] est l'exception - qui semble trop large pour l'EDPB - au droit d'accès aux informations accessibles au public et aux informations provenant de registres publics[43]. L'EDPB a déclaré à plusieurs reprises que, en vertu du droit de l'Union, les personnes concernées ont toujours le droit d'accéder à leurs données, que les données à caractère personnel aient été publiées ou non. Si les demandes d'accès devaient être rejetées au motif que les données ont été obtenues à partir de sources ou de registres publics accessibles au public, les personnes concernées perdraient la possibilité de contrôler l'exactitude des données et de vérifier si les données ont été licitement rendues publiques.

49. L'EDPB rappelle que le droit d'accès est consacré à l'article 8, paragraphe 2, de la charte. Bien qu'il ne s'agisse pas d'un droit absolu, il est fondamental pour le droit à la protection des données à caractère personnel, car il facilite l'exercice des autres droits de la personne concernée, tels que la rectification et l'effacement, et le droit d'opposition[44].

50. Outre les droits d'accès, d'effacement et de suppression, les personnes concernées devraient avoir le droit de s'opposer, pour des raisons impérieuses et légitimes tenant à leur situation particulière, à tout

[37] Projet de décision, annexes I, sections II.6 et III.8 a i).
[38] Projet de décision, annexe I, section III.8.a i) 1. Note de bas de page 14.
[39] Projet de décision, annexe I, section III.8.d ii).
[40] Projet de décision, annexe I, III.8.e.
[41] Avis 01/2016 du GT art. 29, point 2.2.5.
[42] Avis 01/2016 du GT art. 29, point 2.2.9.
[43] Projet de décision, annexe I, section III.15.d et e.
[44] Avis 01/2016 du GT art. 29, point 2.2.5.

moment, au traitement de leurs données dans des conditions spécifiques établies dans le cadre juridique du pays tiers[45].

51. Avec le principe relatif au choix, le CPD prévoit le droit de s'opposer («opt-out») à la divulgation d'informations à caractère personnel à un tiers ou à l'utilisation d'informations à caractère personnel à des fins substantiellement différentes[46]. En outre, les personnes bénéficient à tout moment d'un droit d'opposition à l'utilisation de leurs informations à caractère personnel à des fins de prospection directe[47]. Sauf dans le contexte de la prospection directe, les modalités, en particulier le calendrier, pour l'exercice du droit d'opposition ne sont pas détaillées. Par conséquent, l'EDPB invite la Commission à préciser comment les personnes peuvent exercer leur droit d'opposition.

52. Comme indiqué dans l'avis 01/2016 du GT art. 29, l'EDPB considère que la simple référence à l'existence de ce droit dans la politique de confidentialité ne saurait suffire. Une possibilité individualisée d'exercer ce droit ne devrait pas uniquement être offerte en cas de divulgation ou de réutilisation d'informations à caractère personnel. L'EDPB souligne qu'un droit général d'opposition pour des motifs impérieux et légitimes liés à la situation particulière de la personne concernée devrait être offert dans le cadre du CPD. L'EDPB recommande que ce droit d'opposition soit garanti à tout moment et que ce droit ne se limite pas à l'utilisation des données à des fins de prospection directe[48].

53. En ce qui concerne les données relatives aux ressources humaines, l'EDPB apprécie les clarifications apportées par la Commission en ce qui concerne l'application des principes de notification et de choix dans le cas où une organisation américaine certifiée a l'intention d'utiliser des données RH à des fins différentes, non liées à l'emploi, telles que des communications publicitaires[49]. Toutefois, l'EDPB maintient que le traitement ultérieur des données RH à des fins non liées à l'emploi sera, dans la plupart des cas, considéré comme incompatible avec la finalité initiale, et que le consentement sera rarement entièrement libre lorsqu'il est donné dans un contexte professionnel.

54. L'EDPB réitère également les préoccupations du GT art. 29 en ce qui concerne la dérogation aux principes de notification et de choix pour les données relatives aux ressources humaines *«dans la mesure et pendant la période nécessaires pour éviter de porter atteinte à la capacité de l'organisation à accorder des promotions, faire des nominations ou d'autres décisions similaires en matière d'emploi»*[50], qui semble large et vague pour l'EDPB[51].

2.1.4 Limitations concernant les transferts ultérieurs

55. Les transferts ultérieurs des données à caractère personnel par le destinataire initial du transfert original de données ne devraient être autorisés que si le nouveau destinataire (c'est-à-dire le destinataire du transfert ultérieur) est également soumis à des règles (y compris des règles contractuelles) assurant un niveau de protection adéquat et suivant les instructions pertinentes lors du traitement des données pour le compte du responsable du traitement. Le niveau de protection des personnes dont les données sont transférées ne doit pas être compromis par le transfert ultérieur. Le destinataire initial des données transférées depuis l'UE doit s'assurer que les garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation. Ces

[45] Critères de référence pour l'adéquation au RGPD, section 3.A.8.
[46] Projet de décision, annexe I, section II.2 a).
[47] Projet de décision, annexe I, section III.12 a).
[48] Avis 01/2016 du GT art. 29, point 2.2.2.
[49] Projet de décision, annexe I, section III.9.b i), considérant 15 et note de bas de page 27.
[50] Projet de décision, annexe I, section III.9.b iv).
[51] Avis 01/2016 du GT art. 29, point 2.2.7.

transferts ultérieurs de données ne devraient avoir lieu qu'à des fins limitées et précises et tant que ce traitement a un fondement juridique[52].

56. Conformément au principe du CPD sur la responsabilité des transferts ultérieurs, ceux-ci ne peuvent avoir lieu qu'à des fins limitées et spécifiées, sur la base d'un contrat entre l'organisation CPD et le tiers (ou d'un accord comparable au sein d'un même groupe d'entreprises) et uniquement si ce contrat exige que le tiers assure le même niveau de protection que celui garanti par les principes du CPD[53].

57. L'EDPB tient à réitérer les préoccupations exprimées dans l'avis 01/2016 du GT art. 29 concernant l'exemption de la nécessité de conclure des contrats pour les transferts intragroupe entre responsables du traitement[54]. En ce qui concerne les données RH, l'EDPB ne comprend toujours pas la raison d'être de l'exemption de l'obligation de conclure un contrat avec un tiers responsable du traitement en cas de transferts ultérieurs pour des «besoins opérationnels occasionnels liés à l'emploi»[55].

58. En outre, l'EDPB souhaiterait réitérer la demande du GT art. 29[56] selon laquelle les organisations liées par le cadre devraient évaluer, avant un transfert ultérieur, que les exigences obligatoires de la législation nationale du pays tiers applicable au destinataire ne compromettraient pas la continuité de la protection des personnes concernées dont les données sont transférées[57].

59. L'EDPB maintient que les transferts ultérieurs de données à caractère personnel vers des pays tiers pourraient interférer avec les droits fondamentaux des personnes et invite la Commission à préciser que les garanties imposées par le destinataire initial à l'importateur dans le pays tiers doivent être effectives à l'égard de la législation du pays tiers, avant un transfert ultérieur dans le cadre du CPD[58].

2.1.5 Prise de décision et profilage automatisés

60. Les décisions prises sur le seul fondement d'un traitement automatisé (prise de décision individuelle automatisée), y compris le profilage, et qui produisent des effets juridiques pour la personne concernée ou qui ont des répercussions significatives pour celle-ci, ne peuvent avoir lieu que dans certaines conditions prévues dans le cadre légal du pays tiers. Dans le cadre européen, ces conditions correspondent notamment à la nécessité d'obtenir le consentement explicite de la personne concernée ou à la nécessité de cette décision pour la conclusion d'un contrat. Si la décision ne respecte pas les conditions fixées dans le cadre juridique du pays tiers, la personne concernée devrait avoir le

[52] Critères de référence pour l'adéquation au RGPD, section 3.A.9.
[53] Projet de décision, annexe I, section II.3.
[54] Projet de décision, annexe I, section III.10.b i), qui fait référence à «ou à d'autres instruments intragroupe (par exemple, les programmes de conformité et de contrôle)» qui ne devraient apparemment pas être contraignants.
[55] Projet de décision, annexe I, section III.9.e (i), faisant référence à des exemples tels que la couverture d'assurance.
[56] Avis 01/2016 du GT art. 29, point 2.2.3, p. 21.
[57] À la lumière de l'arrêt *Schrems II*, l'EDPB a précisé davantage les obligations des exportateurs et des importateurs de données en ce qui concerne les transferts ultérieurs dans un certain nombre de lignes directrices et de recommandations:voir les recommandations 01/2020 de l'EDPB sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau de protection des données à caractère personnel de l'UE (version 2.0, adoptée le 18 juin 2021), les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, les lignes directrices 04/2021 sur les codes de conduite en tant qu'outils de transfert (version 2.0 adoptée le 22 février 2022), les recommandations 1/2022 sur la demande d'agrément et sur les éléments et principes figurant dans les règles d'entreprise contraignantes pour le responsable du traitement (adoptées le 14 novembre 2022), et les lignes directrices 07/2022 sur la certification en tant qu'outil pour les transferts (adoptées après consultation publique le 14 février 2023).
[58] Avis 01/2016 du GT art. 29, point 2.2.3, p. 21.

droit de ne pas y être soumise. La législation du pays tiers devrait, dans tous les cas, prévoir les garanties nécessaires, notamment le droit d'être informé des raisons particulières sous-tendant la décision et la logique concernée, de corriger des informations inexactes ou incomplètes et de contester la décision si elle est adoptée sur une base factuelle incorrecte[59].

61. Le CPD ne prévoit pas de garanties juridiques spécifiques lorsque les personnes font l'objet de décisions produisant des effets juridiques les concernant ou les affectant de manière significative et fondées uniquement sur un traitement automatisé de données destiné à évaluer certains aspects personnels les concernant, tels que leur rendement au travail, leur solvabilité, leur fiabilité ou leur comportement.

62. Comme indiqué dans l'avis 01/2016 du GT art. 29 et par l'EDPB dans ses avis antérieurs sur les décisions d'adéquation concernant le Japon et la Corée du Sud[60], l'EDPB estime que les évolutions rapides dans le domaine de la prise de décision et du profilage automatisés — de plus en plus au moyen de technologies basées sur l'IA — nécessitent une attention particulière à cet égard[61].

63. L'EDPB prend note des arguments de la Commission selon lesquels l'absence de règles spécifiques dans le CPD sur la prise de décision automatisée est peu susceptible d'avoir des conséquences sur le niveau de protection des données à caractère personnel collectées dans l'Union (étant donné que toute décision fondée sur un traitement automatisé serait généralement prise par le responsable du traitement dans l'Union qui a une relation directe avec la personne concernée)[62].. Toutefois, de l'avis de l'EDPB, il ne peut être exclu que la prise de décision automatisée puisse être utilisée par un responsable du traitement établi aux États-Unis en ce qui concerne les données transférées en vertu du projet de décision (par exemple, dans le contexte professionnel, pour évaluer la performance au travail, pour les assurances, le logement).

64. L'EDPB se félicite des références faites par la Commission aux garanties spécifiques prévues par la législation américaine pertinente dans différents domaines[63]. Toutefois, pour l'EDPB, le niveau de protection des personnes semble varier en fonction des règles sectorielles, le cas échéant, qui s'appliquent à la situation en cause. Il existe un risque que certaines situations ne soient pas couvertes parce qu'elles ne relèvent pas du champ d'application des actes visés. En outre, le contenu des droits individuels relatifs à la prise de décision automatisée est décrit différemment dans les différents actes.

65. Dans ce contexte, l'EDPB considère que le CPD devrait contenir des règles spécifiques concernant la prise de décision automatisée afin de fournir des garanties suffisantes, y compris le droit pour la personne de connaître la logique sous-jacente, de contester la décision et d'obtenir une intervention humaine lorsque la décision lui porte préjudice de manière significative[64].

2.2 Mécanismes en matière de procédure et d'application

[59] Critères de référence pour l'adéquation au RGPD, section 3.B.3.
[60] Avis 28/2018 de l'EDPB relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, adopté le 5 décembre 2018; Avis 32/2021 de l'EDPB relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par la république de Corée, adopté le 24 septembre 2021.
[61] Voir, notamment, C-634/21, OQ/Land Hesse (SCHUFA Holding e.a.), demande de décision préjudicielle (pendante).
[62] Projet de décision, considérants 33 et 34.
[63] Voir le projet de décision, considérant 35.
[64] Voir également le troisième rapport d'examen conjoint, point 76.

66. L'EDPB note que le CPD continue de s'appuyer sur un système d'autocertification, même si la Commission le qualifie de système de «certification».

67. L'EDPB rappelle les améliorations obtenues au cours des précédents examens conjoints, par exemple en ce qui concerne le rôle du ministère du commerce, le processus de (ré-)autocertification (...), le contrôle du respect des principes du CPD par les entreprises (par exemple, au moyen de contrôles inopinés ou de l'utilisation de questionnaires de conformité) et la détection et le traitement des fausses déclarations de participation (par exemple, au moyen de recherches sur l'internet).

68. Dans le même temps, le GT art. 29 et l'EDPB avaient fait part de leurs préoccupations concernant un certain manque de contrôle du respect des exigences du bouclier de protection des données[65]. En particulier, l'EDPB souscrit aux constatations de la Commission à l'issue du troisième examen annuel du bouclier de protection des données selon lesquelles, dans le cadre du bouclier de protection des données, les contrôles inopinés effectués par le ministère du commerce étaient généralement limités à des exigences formelles (par exemple, l'absence de réponse de la part des points de contact désignés ou l'inaccessibilité de la politique de protection de la vie privée d'une entreprise en ligne)[66]. The EDPB considers that . L'EDPB considère que les contrôles de conformité concernant les exigences davantage liées à des questions de fond sont essentiels.

69. L'EDPB rappelle également l'importance d'une surveillance efficace (y compris du respect des exigences de fond) et du respect de l'application du CPD. Cet aspect fera l'objet d'un suivi attentif de la part de l'EDPB, y compris dans le cadre des examens périodiques.

70. En ce qui concerne le respect de l'application, l'EDPB prend note des engagements renouvelés figurant dans les lettres de la Commission fédérale du commerce (FTC)[67] et du ministère des transports (DoT)[68], à savoir donner la priorité à l'enquête sur les violations présumées du CPD, prendre des mesures coercitives appropriées à l'égard des entités formulant des allégations de participation fausses ou trompeuses, surveiller les ordonnances d'exécution concernant les violations du CPD et coopérer avec les autorités chargées de la protection des données de l'UE. À cet égard, l'EDPB reconnaît également que la FTC a indiqué qu'elle comptait axer davantage ses efforts de respect de l'application sur les violations substantielles du CPD et qu'elle avait l'intention d'enquêter (également) de sa propre initiative. Ces aspects feront l'objet d'un suivi attentif de la part de l'EDPB, y compris dans le cadre des examens périodiques.

2.3 Mécanismes de recours

71. L'EDPB se félicite de la présentation claire, dans le projet de décision, des sept voies de recours offertes aux personnes concernées de l'UE, si leurs données à caractère personnel sont traitées en violation du CPD[69].

[65] Voir le troisième rapport d'examen conjoint, point 7.
[66] Rapport de la Commission au Parlement européen et au Conseil sur le troisième examen annuel du fonctionnement du bouclier de protection des données UE–États-Unis [COM(2019) 495 final du 23.10.2019], p. 4.
[67] Projet de décision, annexe IV
[68] Projet de décision, annexe V
[69] Voir le projet de décision, considérant 67.

72. Ces différents mécanismes de recours sont établis conformément aux exigences du principe des voies de recours, de l'exécution et de la responsabilité et du principe supplémentaire n° 11 «Règlement des litiges et respect de l'application» publié par le ministère du commerce et mentionné à l'annexe I du projet de décision[70].

73. Comme l'a souligné la Commission dans son projet de décision, *«la personne concernée devrait bénéficier d'un recours administratif et juridictionnel effectif»*[71]. Cela fait écho à l'exigence de l'article 45, paragraphe 2, point a), du RGPD, selon laquelle la Commission, dans son évaluation du caractère adéquat du niveau de protection dans un pays tiers, doit tenir compte, en particulier, d'un «recours administratif et juridictionnel effectif pour les personnes concernées dont les données à caractère personnel sont transférées»[72]. Cette exigence est également rappelée par les critères de référence pour l'adéquation au RGPD[73].

74. L'EDPB note que ces mécanismes de recours sont les mêmes que ceux inclus dans l'ancien bouclier de protection des données, qui avait fait l'objet d'observations de la part du GT art. 29[74].

75. En ce qui concerne le mécanisme d'arbitrage, l'EDPB note que cette option n'est pas disponible en ce qui concerne les exceptions aux principes du CPD[75] et renvoie donc à son commentaire formulé au point 33.

76. En ce qui concerne les voies de recours juridictionnel supplémentaires disponibles en vertu du droit américain, l'EDPB souhaiterait également obtenir de plus amples informations sur la législation mentionnée[76] et renvoie à l'observation qu'il a formulée au point 21.

77. En outre, l'EDPB se félicite de la lettre de la FTC décrivant son intention de travailler en étroite collaboration avec les APD de l'UE[77]. L'EDPB se félicite également de la hiérarchisation des plaintes par la FTC, bien qu'elle ne donne pas la certitude à la personne concernée que ses plaintes seront traitées dans tous les cas.

78. En ce qui concerne la possibilité, dans certains cas, pour les personnes physiques d'introduire leurs plaintes auprès d'une APD de l'UE, l'EDPB souhaiterait obtenir des informations supplémentaires i) sur la question de savoir si la possibilité pour l'APD de l'UE de donner des conseils sur les mesures correctives ou compensatoires pourrait inclure une recommandation concernant des amendes ou l'utilisation de pouvoirs d'enquête et ii) dans quelle mesure l'action de l'APD de l'UE serait prise en compte comme élément de preuve pour les mesures coercitives prises par la FTC ou le DoT[78].

79. L'efficacité des mécanismes de recours fera l'objet d'un suivi attentif de la part de l'EDPB, notamment dans le cadre des examens périodiques.

[70] Projet de décision, annexe I, section II.7 et III.11 et annexe I de l'annexe I.
[71] Voir le projet de décision, considérant 64.
[72] Voir également le considérant 141 du RGPD faisant référence à l'article 47 de la charte des droits fondamentaux en ce qui concerne le droit à un recours juridictionnel effectif dans l'Union.
[73] Critères de référence pour l'adéquation au RGPD, p. 8.
[74] Voir en particulier l'avis 01/2016 du GT art. 29, section 2.2.6, point a).
[75] Projet de décision, annexe I de l'annexe I, point A.
[76] Voir le projet de décision, considérant 85.
[77] Projet de décision, annexe IV.
[78] Projet de décision, annexe I, III.5.b iii).

3 ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DE L'UNION EUROPÉENNE ET UTILISATION DE CELLES-CI PAR LES AUTORITÉS PUBLIQUES AU ÉTATS-UNIS

3.1 Accès et utilisation à des fins répressives

3.1.1 L'accès des services répressifs aux données à caractère personnel devrait être fondé sur des règles claires, précises et accessibles

80. L'EDPB se félicite des informations et explications plus détaillées, par rapport à la précédente décision d'adéquation, prévues dans le projet de décision en ce qui concerne l'accès aux données à caractère personnel et leur utilisation par les autorités publiques américaines à des fins répressives. Le projet de décision, dans son annexe VI, contient également une lettre du ministère américain de la justice, division pénale, «fournissant un bref aperçu des principaux outils d'enquête utilisés pour obtenir des données commerciales et d'autres informations auprès de sociétés aux États-Unis à des fins de répression pénale ou d'intérêt public (en matière civile et réglementaire), ainsi que les limitations d'accès qui accompagnent ces compétences». Selon la lettre, tous les processus juridiques décrits dans la lettre sont utilisés pour obtenir des informations auprès d'entreprises aux États-Unis, indépendamment de la nationalité ou du lieu de résidence de la personne concernée, et découlent soit de la Constitution américaine directement (le quatrième amendement), soit du droit écrit et procédural, ou des lignes directrices et des politiques du ministère de la justice. Cette vue d'ensemble ne couvre pas les outils d'enquête en matière de sécurité nationale utilisés par les services répressifs dans le domaine du terrorisme ni d'autres enquêtes de sécurité nationale[79].

81. L'EDPB note que le projet de décision et son annexe VI traitent principalement des autorités répressives et réglementaires fédérales[80] et ne font pas spécifiquement référence aux statuts du droit national qui prévoient ces procédures pour obtenir des informations. L'annexe VI mentionne également qu'«il existe d'autres bases juridiques permettant aux entreprises de contester les demandes de données émanant d'agences administratives sur la base de leurs secteurs spécifiques et des types de données qu'elles possèdent», en donnant en outre plusieurs exemples non exhaustifs, tels que la loi sur le secret bancaire et ses règlements d'exécution[81], la loi sur la publication d'informations en matière de crédit équitable[82] et la loi sur le droit à la vie privée financière[83]. L'EDPB note que la base juridique applicable à une demande d'accès donnée dépend de la nature des données demandées, de la nature de l'entreprise, de la nature des procédures judiciaires (pénales, administratives, liées à d'autres intérêts publics) et de la nature de l'entité demandant l'accès. Étant donné que toutes les règles applicables visant à limiter l'accès des services répressifs aux données transférées aux États-Unis sont fondées sur la Constitution, les lois ordinaires et les politiques transparentes du ministère de la justice, l'EDPB reconnaît l'accessibilité de ces règles et invite la Commission à tenir compte de cet élément dans le projet de décision. Il découle de l'annexe VI que ces règles s'appliquent indépendamment de la nationalité ou du lieu de résidence de la personne concernée et intègrent généralement les exigences du quatrième amendement (bien qu'ils aillent souvent au-delà de cela et prévoient des protections supplémentaires).

[79] Projet de décision, note de bas de page 1 de l'annexe VI.
[80] Voir projet de décision, considérants 90 à 93.
[81] Titre 31 de l'USC, article 5318. Titre 31 du CFR, chapitre X.
[82] Titre 15 de l'USC, article 1681b.
[83] Titre 12 de l'USC, article 3401 à 3423.

82. En conclusion, l'EDPB prend note de l'évaluation plus détaillée figurant dans le projet de décision par rapport à la précédente décision d'adéquation en ce qui concerne l'accès des autorités répressives fédérales. En ce qui concerne l'accès des autorités répressives nationales, l'EDPB prend également acte du fait que, conformément à l'annexe VI, les protections du droit des États doivent être au moins égales à celles de la Constitution américaine, y compris, mais pas exclusivement, celles du quatrième amendement. L'EDPB invite la Commission à poursuivre l'évaluation de l'élément de protection du droit au niveau des États dans les futurs réexamens.

3.1.2 La nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées.

83. L'EDPB note dûment que la demande d'accès à des données à des fins répressives peut, en général, être considérée comme poursuivant un objectif légitime. Toutefois, dans le même temps, de telles interférences ne sont acceptables que lorsqu'elles sont nécessaires et proportionnées[84].

84. Selon une jurisprudence constante de la CJUE, le principe de proportionnalité exige que les actes législatifs portant ingérence dans le droit à la vie privée et au droit à la protection des données à caractère personnel «soient appropriés pour réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs»[85]. Par conséquent, l'appréciation de la nécessité et de la proportionnalité est, en principe, toujours effectuée par rapport à une mesure spécifique envisagée par la législation.

85. Les autorités américaines précisent à l'annexe VI que les procureurs fédéraux et les agents d'enquête fédéraux peuvent avoir accès à des documents et à d'autres informations enregistrées auprès d'organisations au moyen de «plusieurs types de procédures juridiques obligatoires, y compris les injonctions du grand jury, les injonctions administratives et les mandats de perquisition» et peuvent acquérir d'autres communications «en vertu des autorités fédérales chargées des écoutes téléphoniques et des enregistrements graphiques»[86]. De plus, les agences investies de responsabilités civiles et réglementaires peuvent adresser des injonctions aux organisations afin d'accéder «à des documents professionnels, à des informations électroniques ou à d'autres éléments tangibles»[87]. Les processus eux-mêmes sont également expliqués aux considérants 90 à 93 du projet de décision. L'EDPB note à cet égard une évolution positive, mentionnée dans le projet de décision, dans la jurisprudence américaine en ce qui concerne les informations stockées électroniquement[88].

---

[84] Voir l'arrêt de la Cour de justice du 6 octobre 2020 dans les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., ECLI:EU:C:2020:791 (ci-après l'«arrêt de la CJUE La Quadrature du Net»), point 140. Voir également le guide de l'EDPB pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, 11 avril 2017, et les lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, 19 décembre 2019.

[85] Voir l'arrêt de la Cour de justice du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238 (ci-après «Arrêt Digital Rights Ireland de la CJUE»), point 46 et jurisprudence citée.

[86] Projet de décision, annexe VI, p. 2.

[87] Projet de décision, annexe VI, p. 4.

[88] Voir le projet de décision, note de bas de page 146. Dans un arrêt de 2018, la Cour suprême des États-Unis a confirmé qu'une exception relative au mandat de perquisition ou au mandat d'arrêt est également requise pour que les autorités répressives aient accès aux enregistrements historiques de localisation des téléphones mobiles, qui donnent un aperçu complet des mouvements d'un utilisateur et que l'utilisateur puisse raisonnablement s'attendre à ce que ces informations soient privées [Timothy Ivory Carpenter c. États-Unis d'Amérique, n° 16 à 402, 585 U.S. (2018)].

86. L'annexe VI précise en outre que ces procédures judiciaires sont non discriminatoires et utilisées en général pour obtenir des informations auprès de «sociétés» aux États-Unis, qu'elles soient certifiées ou non dans le cadre de la protection des données des États-Unis et de l'UE, et «indépendamment de la nationalité ou du lieu de résidence de la personne concernée».

87. En outre, l'annexe VI contient des conclusions concernant les garanties prévues par le quatrième amendement de la Constitution des États-Unis, selon lequel les perquisitions et les saisies effectuées par les autorités répressives exigent principalement un mandat ordonné par le tribunal sur la base d'exigences de présomption sérieuse et de particularité, et fait référence au fait que, dans des cas exceptionnels où l'exigence du mandat ne s'applique pas, l'application de la loi est soumise à un critère du caractère raisonnable en vertu du quatrième amendement[89]. Une personne faisant l'objet d'une fouille ou dont les biens font l'objet d'une perquisition peut agir pour réclamer la suppression des preuves obtenues ou dérivées d'une fouille ou perquisition illicite si ces preuves sont présentées à son encontre au cours d'un procès pénal[90].

88. En conclusion, l'EDPB note que le système d'outils d'enquête utilisés pour obtenir des données commerciales et d'autres informations auprès d'entreprises américaines à des fins de répression pénale ou d'intérêt public — y compris les limitations et les garanties d'accès — fournit un système de mesures complet, mais aussi complexe, reflétant, entre autres, la nature fédérale du gouvernement des États-Unis.

89. Ainsi, le système de mesures d'enquête en matière répressive aux États-Unis pourrait être considéré comme satisfaisant de manière générale aux exigences de nécessité et de proportionnalité en ce qui concerne les droits fondamentaux à la vie privée et à la protection des données.

3.1.3 Il devrait exister un mécanisme indépendant de contrôle

90. L'EDPB prend dûment note du fait que la plupart des procédures décrites dans le projet de décision et dans l'annexe VI présupposent l'intervention d'une décision de justice avant que les autorités n'obtiennent l'accès aux données (par exemple, les ordonnances de justice relatives aux enregistreurs graphiques et aux dispositifs de traçage[91], les ordonnances de surveillance en vertu de la loi fédérale sur les écoutes téléphoniques[92], les mandats de perquisition — règles fédérales de procédure pénale, article 41[93]). Toutefois, il semble que tous n'exigent pas l'intervention a priori d'un tribunal. Par exemple, les autorités civiles et réglementaires «peuvent émettre des injonctions»[94]. Dans ces cas, il existe toutefois la possibilité d'un contrôle juridictionnel a posteriori du caractère raisonnable de l'ordonnance, étant donné qu'«un destinataire d'une injonction administrative peut contester l'exécution de cette ordonnance en justice»[95].

91. En outre, le projet de décision décrit la supervision des services répressifs fédéraux par divers organes, depuis le contrôle interne par les agents chargés de la protection de la vie privée et des libertés civiles jusqu'au contrôle externe effectué par l'inspecteur général et les commissions spécifiques du Congrès américain[96]. La Commission européenne fournit des informations nuancées et détaillées et parvient

[89] Voir projet de décision, annexe VI, p. 2.
[90] Voir le projet de décision, considérant 90.
[91] Voir le projet de décision, considérant 92.
[92] Voir le projet de décision, annexe VI, p. 3.
[93] Voir le projet de décision, considérant 90, et l'annexe VI, p. 3.
[94] Voir le projet de décision, annexe VI, p. 4, ainsi que le considérant 91.
[95] Voir le projet de décision, annexe VI, p. 4, ainsi que le considérant 91.
[96] Voir le projet de décision, considérants 103 à 106.

généralement à des conclusions compréhensibles. L'EDPB s'abstiendra donc de reproduire les constatations factuelles et les appréciations dans le présent avis.

92. Sur la base des informations disponibles, l'EDPB note qu'en ce qui concerne l'accès des autorités répressives aux données détenues par les entreprises aux États-Unis, un mécanisme de surveillance indépendant assez solide est en place.

3.1.4 Les particuliers devraient disposer de voies de recours effectives

93. Selon la jurisprudence de la CJUE, un particulier doit disposer d'un recours effectif pour faire valoir ses droits lorsqu'il estime qu'ils ne sont pas ou n'ont pas été respectés. Dans l'arrêt Schrems I, la CJUE a expliqué qu'«une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la charte. En effet, l'article 47, premier alinéa, de la charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article.»[97]

94. Le projet de décision[98] et son annexe VI contiennent des informations supplémentaires sur les voies de recours possibles découlant d'une loi ordinaire, qui seraient accessibles aux particuliers lorsque des autorités publiques obtiennent illégalement l'accès à leurs données.

95. À cet égard, selon la Commission[99], le titre 5 du Code des États-Unis, article 702 [loi sur la procédure administrative, *Administrative Procedure Act*(APA)], prévoit qu'une personne subissant un dommage en raison d'une action d'une agence, ou est lésée ou affectée par l'action d'une agence au sens d'une loi pertinente, peut intenter un recours juridictionnel.

96. En outre, la loi sur les communications stockées (*Stored Communications Act*, SCA), promulguée en tant que titre II de la loi sur la protection de la vie privée des communications électroniques, prévoit que toute personne lésée par une violation de ce chapitre dans laquelle le comportement constitutif de la violation est mené sciemment ou de manière intentionnelle peut, dans le cadre d'une action civile, demander dédommagement auprès de la personne ou de l'entité, autre que les États-Unis, qui a commis cette violation, le cas échéant[100]. En outre, toute personne lésée par une violation volontaire de ce chapitre ou du chapitre 119 peut intenter une action devant un tribunal de première instance (*United States District Court*) contre les États-Unis afin de récupérer des dommages-intérêts[101].

97. En outre, le projet de décision contient également des informations sur le droit d'accès aux archives des agences fédérales en vertu de la loi sur la liberté de l'information (*Freedom of Information Act*, FOIA)[102] et de plusieurs autres lois qui donnent aux individus le droit d'intenter une action contre une autorité publique ou un fonctionnaire américain en ce qui concerne le traitement de leurs données à caractère personnel, tels que la *Wiretap Act*, la *Computer Fraud and Abuse Act*, la *Federal Torts Claim Act*, la *Right to Financial Privacy Act* et la *Fair Credit Reporting Act*[103].

[97] Arrêt Schrems I de la CJUE, point 95.
[98] Voir projet de décision, considérants 107 à 112.
[99] Voir le projet de décision, considérant 109.
[100] Titre 18 de l'USC, article 2707.
[101] Titre 18 de l'USC, article 2712.
[102] Voir le projet de décision, considérant 111.
[103] Voir le projet de décision, considérant 112.

98. L'EDPB se félicite donc des éclaircissements fournis par la Commission quant au nombre de voies de recours juridiques sur lesquelles les particuliers peuvent s'appuyer. L'EDPB invite également la Commission à préciser si ces voies de recours permettent à la personne concernée d' «avoir accès aux données à caractère personnel la concernant ou d'obtenir la rectification ou l'effacement de ces données», comme l'exige la CJUE.

3.1.5 Utilisation ultérieure des informations recueillies

3.1.5.1 Utilisation ultérieure des données transférées auxquelles les services répressifs ont accès aux États-Unis

99. L'EDPB note avec satisfaction que le projet de décision évalue l'utilisation ultérieure des données auxquelles les services répressifs ont accès aux États-Unis. Cependant, il regrette qu'un seul exemple des motifs pour lesquels les informations peuvent être diffusées soit donné[104]. À cet égard, l'EDPB recommande à la Commission d'inclure des précisions supplémentaires dans le projet de décision sur les principes et garanties applicables à la poursuite de l'utilisation des données, telles que celles figurant dans la loi sur la protection de la vie privée (titre 5 de l'USC, article 552a)[105].

3.1.5.2 Transferts ultérieurs en dehors des États-Unis

100. L'EDPB note en outre que la Commission européenne fait également référence aux transferts ultérieurs des autorités répressives des États-Unis vers des autorités de pays tiers, mais à nouveau uniquement en ce qui concerne les lignes directrices du procureur général pour les opérations intérieures du FBI (AGG-DOM)[106]. L'EDPB estime que ces informations et cette appréciation sont essentielles afin de permettre la réalisation d'une évaluation complète du niveau de protection garanti par le cadre législatif et les pratiques américains en lien avec les divulgations et les utilisations ultérieures au niveau international. Étant donné que la Commission n'a donné qu'un seul exemple, limité, concernant la question des transferts ultérieurs en dehors des États-Unis dans leur ensemble, l'EDPB invite la Commission à préciser davantage les règles et garanties applicables aux transferts ultérieurs, à l'utilisation ultérieure et à la divulgation d'informations à caractère personnel collectées à des fins répressives aux États-Unis et transférées ensuite vers des pays tiers, notamment au moyen d'accords internationaux.

3.2 Accès et utilisation à des fins de sécurité nationale

101. De manière générale, l'EDPB reconnaît que les États disposent d'un large pouvoir d'appréciation en matière de sécurité nationale, ce que reconnaît également la Cour européenne des droits de l'homme (CEDH). L'EDPB rappelle également que, comme il le souligne dans ses recommandations mises à jour sur les garanties essentielles européennes pour les mesures de surveillance[107], l'article 6, paragraphe 3, du traité sur l'Union européenne dispose que les droits fondamentaux énoncés dans la convention européenne des droits de l'homme constituent des principes généraux du droit de l'Union. Toutefois, comme le rappelle la CJUE dans sa jurisprudence, ladite convention ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement incorporé dans l'ordre juridique

[104] Voir le projet de décision, considérant 102.
[105] Voir les lignes directrices du procureur général pour les opérations intérieures du FBI (AGG-DOM), page 36, point B 1) g).
[106] Voir le projet de décision, considérant 102.
[107] Voir recommandations 02/2020 du CEPD sur les garanties essentielles européennes pour les mesures de surveillance.

de l'Union[108]. Dès lors, le niveau de protection des droits fondamentaux exigé par l'article 45 du RGPD doit être déterminé sur la base des dispositions dudit règlement, lues à la lumière des droits fondamentaux consacrés par la charte de l'UE. Cela étant, conformément à l'article 52, paragraphe 3, de la charte, les droits contenus dans cette dernière et les droits correspondants garantis par la convention européenne des droits de l'homme doivent avoir la même signification et la même portée que ceux énoncés dans la convention européenne des droits de l'homme: partant, comme l'a rappelé la CJUE, il convient de tenir compte de la jurisprudence de la CEDH relative aux droits déjà prévus dans la charte des droits fondamentaux de l'Union européenne en tant que seuil de protection minimale en vue de l'interprétation des droits correspondants de la charte de l'UE[109]. Toutefois, conformément à l'article 52, paragraphe 3, dernière phrase, de la charte, *«[c]ette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue»*.

102. Par conséquent, dans l'évaluation qui suit, l'EDPB a tenu compte de la jurisprudence de la CouEDH, dans la mesure où la charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la CJUE, ne confère pas un niveau de protection plus élevé qui prescrirait des conditions différentes de celles de la jurisprudence de la CouEDH.

103. Plusieurs instruments juridiques prévoient la possibilité, pour les services de renseignement américains, de collecter et de continuer à accéder aux données et de les traiter dans le cadre juridique américain.

104. Comme l'a rappelé la Commission européenne dans son projet de décision, *«les agences de renseignement américaines ne peuvent demander l'accès à des données à caractère personnel transférées à des organisations situées aux États-Unis à des fins de sécurité nationale qu'en vertu de la loi sur la surveillance et le renseignement étranger (FISA) ou des dispositions légales autorisant l'accès au moyen de lettres de sécurité nationale»*[110]. *«Les agences de renseignement américaines ont également la possibilité de collecter des données à caractère personnel en dehors des États-Unis, ce qui peut inclure des données à caractère personnel en transit entre l'Union et les États-Unis»* en vertu du décret présidentiel n° 12333 (EO 12333)[111].

105. En ce qui concerne les régimes spécifiques de collecte de données, en particulier l'article 702 de la FISA et l'EO 12333, l'EO 14086 prévoit désormais de nouvelles règles visant à renforcer les garanties pour les activités américaines de renseignement d'origine électromagnétique. Ces règles générales s'appliquent de manière horizontale et *«doivent être davantage mises en œuvre au moyen de politiques et de procédures émanant des agences, qui les transposent dans des orientations concrètes pour les opérations quotidiennes»*[112]. L'EO 14086 a principalement remplacé la précédente directive présidentielle n° 28 (ci-après la «PPD-28»)[113].

106. Afin d'évaluer le cadre juridique applicable à la collecte, à l'accès et au traitement ultérieur des données à des fins de sécurité nationale, il est donc important d'examiner le cadre juridique spécifique régissant la collecte de données à l'intérieur et à l'extérieur des États-Unis, à savoir l'article 702 de la FISA et l'EO 12333 qui, en tant que tels, n'ont pas changé depuis la précédente révision du bouclier de

[108] Voir arrêt Schrems II de la CJUE, point 98.
[109] Voir arrêt La Quadrature du Net, point 124.
[110] Voir le projet de décision, considérant 115.
[111] Voir le projet de décision, considérant 117.
[112] Voir le projet de décision, considérant 120.
[113] Ce décret présidentiel révoque la PPD-28, à l'exception des sections 3 et 6 de cette directive ainsi que de l'annexe classifiée de celle-ci, qui restent en vigueur. Voir le mémorandum présidentiel sur la sécurité nationale du 7 octobre 2022.

protection des données, en tenant compte du fait que le nouveau décret présidentiel n° 14086 prévoit des garanties à mettre en œuvre également dans le cadre de la collecte de données sur la base de textes spécifiques tels que l'article 702 de la FISA et l'EO 12333.

3.2.1 Garantie A — Le traitement doit être conforme à la loi et fondé sur des règles claires, précises et accessibles

107. Aux fins de son évaluation de l'organisation générale de la collecte de données aux fins de la sécurité nationale, l'EDPB souhaite rappeler la première des quatre «garanties essentielles européennes», selon laquelle «le traitement devrait reposer sur des règles claires, précises et accessibles»[114].

108. Conformément à la jurisprudence constante de la CJUE, toute limitation du droit à la protection des données à caractère personnel doit être prévue par la loi et la base juridique permettant l'ingérence dans un tel droit doit elle-même définir la portée de la limitation à l'exercice du droit concerné[115]. En outre, la CJUE a rappelé que cette «réglementation doit être légalement contraignante en droit interne»[116]. À cet égard, la jurisprudence de la Cour européenne des droits de l'homme précise que le terme «loi» doit être compris dans son sens matériel et non dans son sens formel. Il peut s'agir de l'adoption de textes de rang infralégislatif et d'actes réglementaires pris par un ordre professionnel, par délégation du législateur, dans le cadre de son pouvoir normatif autonome, et de «droit non écrit». Pour être une «loi», une norme doit au moins être suffisamment accessible et formulée avec suffisamment de précision[117].

109. Le degré de précision requis doit être mesuré par rapport à l'étendue de la limitation du droit[118]. En outre, en ce qui concerne la «prévisibilité» de la loi, la CEDH a rappelé dans l'arrêt Zakharov que, dans le cadre de mesures de surveillance secrètes, telles que l'interception de communications, «la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence». Toutefois, des règles claires et détaillées sur les mesures de surveillance secrètes sont essentielles pour prévenir les risques d'arbitraire lorsqu'un pouvoir dévolu à l'exécutif est exercé en secret. «La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes»[119].

110. En outre, la CJUE a précisé que l'évaluation du droit du pays tiers applicable devrait se concentrer sur la question de savoir s'il peut être invoqué et opposé par des particuliers devant une juridiction. Les droits accordés aux personnes concernées devraient notamment pouvoir faire l'objet d'un recours et les particuliers doivent se voir accorder des droits opposables aux autorités publiques[120], ce qui n'était pas le cas dans le contexte de l'ancienne PPD-28. L'EO 14086 qui, selon l'EDPB, est considéré comme

[114] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020. Voir les points 175 et 180 de l'arrêt Schrems II et l'avis 1/15 (Accord PNR UE-Canada) du 26 juillet 2017, point 139 et jurisprudence citée.
[115] Voir arrêt Schrems II de la CJUE, points 174 à 175 et jurisprudence citée. Voir également, en ce qui concerne l'accès des autorités publiques des États membres, l'arrêt Privacy International, C-623/17, ECLI:EU:C:2020:790 (ci-après l'«arrêt Privacy International de la CJUE»), point 65, et arrêt La Quadrature du Net de la CJUE, point 175.
[116] Arrêt Privacy International de la CJUE, point 68.
[117] CEDH, Sunday Times c. Royaume-Uni (n° 1), 26 avril 1979, CE:ECHR:1979:0426JUD000653874 (ci-après l'«arrêt de la CEDH Sunday Times c. Royaume-Uni n° 1»), point 49.
[118] CEDH, arrêt Sunday Times c. Royaume-Uni n° 1, point 49.
[119] CEDH, Zakharov c. Russie, 4 décembre 2015 (ci-après l' «arrêt de la CEDH dans l'affaire Zakharov»), point 229.
[120] Arrêt Schrems II de la CJUE, point 181.

ayant le même effet juridique au sein de l'ordre juridique américain que la PPD-28 (c'est-à-dire contraignante pour l'exécutif), prévoit des possibilités d'actions contre des autorités publiques. Une évaluation détaillée des nouveaux droits opposables des personnes concernées est fournie dans la section consacrée aux voies de recours.

111. Les considérants 114 à 152 du projet de décision et l'annexe VII fournissent un résumé de certains aspects du cadre juridique applicable, des limitations de la collecte, de la conservation et de la diffusion, de la conformité et de la surveillance, de la transparence et des voies de recours. Le système juridique américain pour les activités de renseignement se compose d'un certain nombre de documents, parmi lesquels des rapports, des politiques et des procédures de différentes agences. À cet égard, l'évaluation de l'EDPB se concentre sur un nombre limité de questions qu'il juge cruciales.

112. Selon les considérants 115 à 119 du projet de décision, l'accès aux données à caractère personnel transférées par les autorités de sécurité nationales américaines ne peut avoir lieu que dans le cadre de la FISA, en vertu d'autres dispositions légales (titre 12 du code des États-Unis, article 3414; titre 15 du code des États-Unis, articles 1681u et 1681v; et titre 18 du code des États-Unis, article 2709) ou, en ce qui concerne les données à caractère personnel en transit, sur la base de l'EO 12333. Il ressort des considérants 116 et 118 du projet de décision que la Commission concentre son évaluation, en ce qui concerne l'accès aux données à caractère personnel par les autorités américaines chargées de la sécurité nationale, sur les articles 105, 302, 402, 501 et 702 de la FISA (activités de renseignement extérieur ciblant des personnes non américaines situées en dehors des États-Unis) et sur l'EO 12333 (activités de renseignement extérieur sur les données à caractère personnel en transit), comme étant les plus pertinents. L'avis de l'EDPB se limite donc à l'évaluation de ces dispositions effectuée par la Commission, en tenant compte des limitations et des garanties énoncées dans l'EO 14086[121].

113. À cet égard, il convient de noter que tous les instruments juridiques mentionnés dans le projet de décision sont accessibles au grand public (aux États-Unis et en dehors) et disponibles en ligne. En outre, les exigences énoncées dans l'EO sont contraignantes pour l'ensemble des services de renseignement[122] et s'appliquent de manière transversale à toutes les activités ayant pour finalité le renseignement étranger.

114. La notion de «renseignement d'origine électromagnétique» n'est pas définie dans l'EO 14086. Ce dernier renvoie aux définitions figurant dans l'EO 12333 pour définir le champ d'application du renseignement étranger et du contre-espionnage, qui sont définis de manière large. À cet égard, même s'il a été soutenu que, depuis l'introduction de la FISA, l'EO 12333 ne peut être utilisé que pour la collecte de données en dehors du territoire des États-Unis, l'EDPB rappelle que l'EO 12333 lui-même, qui reste intact, n'est pas suffisamment détaillé en ce qui concerne sa portée géographique, la mesure dans laquelle les données peuvent être collectées, conservées ou diffusées, ou la nature des infractions susceptibles de donner lieu à une surveillance ou le type d'informations pouvant être collectées ou utilisées. En principe, toutes les collectes de données de renseignement étranger relevant du champ d'application de l'EO 12333 peuvent avoir lieu à la discrétion du président des États-Unis[123]. Toutefois, selon l'EDPB, l'objectif principal de l'EO 14086 est de fixer les limites de la collecte et du traitement

121 Ce décret présidentiel révoque la PPD-28, à l'exception des sections 3 et 6 de cette directive ainsi que de l'annexe classifiée de celle-ci, qui restent en vigueur. Voir le mémorandum présidentiel sur la sécurité nationale du 7 octobre 2022.

122 Voir le projet de décision, considérant 120.

123 En vertu de l'article II de la Constitution américaine, la responsabilité de garantir la sécurité nationale, y compris en particulier la collecte de renseignements étrangers, relève de l'autorité du président en tant que commandant en chef des forces armées.

des données à caractère personnel dans le contexte du renseignement étranger, quel que soit le programme de surveillance utilisé et le lieu où les données sont obtenues. L'EDPB comprend donc que les garanties supplémentaires prévues au titre de l'EO 14086 s'appliquent également dans le contexte des programmes de surveillance applicables aux données à caractère personnel en transit au titre de l'EO 12333[124].

115. À cet égard, l'EO 14086 énumère douze objectifs légitimes qui devraient être poursuivis lors de la collecte de renseignements d'origine électromagnétique et cinq objectifs pour lesquels la collecte de renseignements d'origine électromagnétique ne doit pas être effectuée[125], ainsi que six objectifs légitimes pour l'utilisation des données collectées en masse[126]. Si certains d'entre eux sont assez précis (par exemple, le «sauvetage des otages»), d'autres sont plus généraux (par exemple, la «sécurité mondiale»). L'EO 14086 établit également une liste d'objectifs interdits, qui comprennent notamment la suppression ou la restriction d'«intérêts légitimes en matière de protection de la vie privée»[127]. L'EO 14086 prévoit également la possibilité pour le président des États-Unis d'ajouter d'autres objectifs à la liste pour lesquels la collecte est autorisée, qui pourraient, sur décision du président, ne pas être rendus publics si le président estime que cela constituerait un risque pour la sécurité nationale des États-Unis[128]. Ces mises à jour ne peuvent être autorisées qu'«à la lumière de nouveaux impératifs de sécurité nationale».

116. Les objectifs ne peuvent pas, à eux seuls, être invoqués par les services de renseignement pour justifier la collecte de renseignements d'origine électromagnétique, mais ils doivent être étayés, à des fins opérationnelles, par des priorités plus concrètes pour lesquelles des renseignements d'origine électromagnétique peuvent être collectés. L'EO 14086 détaille la procédure de validation des priorités pour lesquelles des renseignements d'origine électromagnétique peuvent être collectés[129]. L'EDPB comprend que le processus de définition des priorités validées en matière de renseignement repose en principe sur l'avis du directeur des services de renseignement et reconnaît qu'il devrait en principe inclure l'évaluation du délégué à la protection des libertés civiles (*Civil Liberties Protection Officer*, CLPO) du bureau du directeur du renseignement national, avec lequel le directeur peut être en désaccord, auquel cas cet avis «inclut l'évaluation du CLPO et l'avis du directeur lors de la présentation du cadre national des priorités en matière de renseignement (NIPF) au président»[130].

117. Toutefois, l'EDPB note également que, selon la définition de *«priorité validée en matière de renseignement»*, ces priorités signifient, pour *«la plupart des activités américaines de collecte de renseignements d'origine électromagnétique»*[131], une priorité validée au titre de la section 2, point b) iii), de l'EO (décrite au paragraphe précédent). Le processus de validation peut, dans certains cas, différer de ce processus dans des *«circonstances très limitées»*, auquel cas le président ou le chef d'un élément de la communauté des services de renseignement peut fixer une priorité, *«dans la mesure du possible»*, conformément aux critères fixés par la même section 2 b) iii) A) 1 à 3), qui inclut l'exigence d'une prise en compte appropriée de la vie privée et des libertés civiles de toutes les personnes, mais sans l'intervention du CLPO.

[124] Voir le projet de décision, considérant 134.
[125] Voir décret présidentiel n° 14086 (ci-après l'«EO 14086»), section 2, point b), ii), A, 1 à 5.
[126] Voir le projet de décision, considérant 134, et l'EO 14086, section 2, point c) ii).
[127] Voir l'EO 14086, section 2, point b) ii) A 2.
[128] Voir l'EO 14086, section 2, point b) i) B.
[129] Voir le projet de décision, considérant 129.
[130] Voir l'EO 14086, section 2, point b) iii) B).
[131] Voir l'EO 14086, section 4, point n).

118. L'EO 14086 souligne en outre que «les activités de collecte de renseignements d'origine électromagnétique doivent être aussi adaptées que possible» pour faire progresser une priorité validée en matière de renseignement, que «les services de renseignement examinent la disponibilité, la faisabilité et la pertinence d'autres sources moins intrusives» et qu'ils prévoient des exigences générales en matière de nécessité et de proportionnalité[132].

119. En outre, conformément à la section 5, point h), l'EO 14086 crée le droit d'introduire des plaintes recevables auprès du CLPO et d'obtenir un réexamen des décisions du CLPO par la Cour de contrôle de la protection des données conformément au mécanisme de recours établi à la section 3 dudit décret.

120. Le texte de la FISA semble plus clair et plus précis que l'EO 12333 sur le type d'opérations de renseignement pouvant être mandatées. La FISA et l'EO 12333 doivent désormais être appliqués à la lumière de l'EO 14086 et en particulier en tenant compte, entre autres, des principes de nécessité et de proportionnalité.

121. Les exigences énoncées dans l'EO 14086 doivent être davantage mises en œuvre au moyen de politiques et de procédures émanant des agences, qui les transposent en orientations concrètes pour les opérations quotidiennes. À cet égard, l'EO 14086 accorde aux agences de renseignement américaines un délai d'un an au maximum pour mettre à jour leurs politiques et procédures existantes (c'est-à-dire au plus tard le 7 octobre 2023) afin de les mettre en conformité avec les exigences de l'EO. Ces politiques et procédures actualisées doivent être élaborées en concertation avec le procureur général, le CLPO et le Conseil de surveillance de la vie privée et des libertés civiles (PCLOB) et être rendues publiques dans toute la mesure du possible[133].

122. L'EDPB se féliciterait que non seulement l'entrée en vigueur, mais aussi l'adoption de la décision soient subordonnées, entre autres, à l'adoption de politiques et de procédures actualisées pour mettre en œuvre l'EO 14086 par toutes les agences de renseignement américaines. L'EDPB recommande à la Commission d'évaluer ces politiques et procédures actualisées et de partager cette évaluation avec le comité.

123. Enfin, en ce qui concerne la conservation des données transférées une fois collectées à des fins de sécurité nationale, l'EDPB note que l'EO 14086 garantit que les règles applicables aux données à caractère personnel des ressortissants américains sont également applicables aux données à caractère personnel des ressortissants d'autres pays[134]. Il ressort du projet de décision que ces règles sont prévues à l'article 309 de la loi sur les autorisations en matière de renseignement pour l'exercice fiscal 2015[135], qui fixe une durée maximale de conservation de cinq ans en principe pour toute communication téléphonique ou électronique non publique acquise sans le consentement de la personne. À cet égard, l'EDPB recommande à la Commission de clarifier son évaluation des règles de conservation applicables aux données à caractère personnel des personnes américaines dans la décision.

[132] Voir l'EO 14086, section 2, point c) i), points A) et B).
[133] Voir l'EO 14086, section 2, point c) iv), B) et C).
[134] Projet de décision, considérant 150.
[135] Projet de décision, note de bas de page 272.

3.2.2 Garantie B – la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis devraient être démontrées

3.2.2.1 Garanties horizontales prévues par le nouveau décret présidentiel n° 14086 – Nécessité et proportionnalité

124. Le nouvel EO 14086, qui remplace généralement la PPD-28, vise à établir des règles visant à renforcer les garanties pour les activités de renseignement d'origine électromagnétique des États-Unis, qui seront mises en œuvre par les composantes des services de renseignement dans leurs politiques et procédures internes.

125. L'EO 14086 introduit deux nouvelles exigences en droit américain qui reflètent les exigences rappelées par la CJUE dans son arrêt Schrems II, à savoir que les activités de renseignement d'origine électromagnétique ne doivent être menées que dans la mesure nécessaire pour faire progresser une collecte de renseignements prioritaire validée et uniquement dans la mesure et d'une manière qui soient proportionnées à la priorité validée en matière de renseignement[136].

126. L'EDPB comprend que ces éléments ont été inclus pour refléter les principes de nécessité et de proportionnalité prévus par le droit de l'Union ainsi que par la jurisprudence de la CJUE et de la CEDH, qui visent à garantir que la collecte et le traitement des données soient limités à ce qui est nécessaire et proportionné.

127. À cet égard, l'EDPB rappelle le processus prévu pour la validation des priorités en matière de renseignement ainsi que l'éventuelle dérogation (voir points 116 et 117).

128. En outre, l'EDPB note que ces principes de nécessité et de proportionnalité prévus par l'EO devront être rendus opérationnels et mis en œuvre, dans un délai d'un an, dans les politiques et procédures de chaque composante de la communauté du renseignement[137].

3.2.2.2 Garanties spécifiques pour la collecte de renseignements d'origine électromagnétique

129. L'EDPB note également que l'EO 14086 prévoit des limitations concernant les objectifs pour lesquels des données à caractère personnel peuvent et ne peuvent pas être collectées, dans le contexte de la collecte de renseignements d'origine électromagnétique[138].

130. L'EDPB se félicite que l'EO prévoie que la collecte ciblée devrait être prioritaire par rapport à la collecte en vrac[139]. Dans le cadre de la collecte de renseignements d'origine électromagnétique, l'EO fournit une liste de douze objectifs pour lesquels des données peuvent être collectées, qui doivent être étayées en priorités en matière de renseignement (voir point 117), ainsi qu'une liste de cinq objectifs pour lesquels aucune activité de collecte de renseignements d'origine électromagnétique ne doit être menée[140]. En principe, ces dispositions constituent une garantie de la nécessité de la collecte de données.

[136] Voir l'EO 14086, section 2, points a), ii), A et B.
[137] Voir l'EO 14086, section 2, point c) iv) B.
[138] Voir l'EO 14086, section 2, point b) i) A 1 à 12.
[139] Voir l'EO 14086, section 2, point c) ii) A.
[140] Voir l'EO 14086, section 2, points b) ii) A 1 à 5.

131. Toutefois, l'EDPB rappelle que l'EO 14086 prévoit également la possibilité pour le président des États-Unis d'ajouter d'autres objectifs à la liste (voir points 114 et 115)[141].

3.2.2.3 Garanties spécifiques pour la collecte en vrac

132. Dans son arrêt Schrems I, la CJUE a souligné que «*la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations en matière de protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire*»[142] et a jugé qu'«*une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu des communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la charte*».

133. Dans l'affaire Schrems II[143], en ce qui concerne son analyse de la collecte en vrac en relation avec la lecture corrélative de l'EO 12333 et de la PPD-28, et en particulier des points 183 à 185, la Cour a souligné, ainsi qu'il a été rappelé ci-dessus, que la possibilité d'une collecte en vrac, «*qui permet, dans le cadre des programmes de surveillance fondés sur l'E.O. 12333, d'accéder à des données en transit vers les États-Unis sans que cet accès fasse l'objet d'une quelconque surveillance judiciaire, n'encadre, en tout état de cause, pas de manière suffisamment claire et précise la portée d'une telle collecte en vrac de données à caractère personnel* ».

134. L'EDPB note donc que la CJUE n'a pas exclu, par principe, la collecte en vrac, mais a considéré, dans sa décision Schrems II, que pour que cette collecte en vrac ait lieu légalement, des limites suffisamment claires et précises doivent être en place pour délimiter le champ d'application de cette collecte en vrac.

135. L'EDPB reconnaît également que, tout en remplaçant la PPD-28, l'EO 14086 prévoit de nouvelles garanties et limites à la collecte et à l'utilisation des données collectées en dehors des États-Unis, étant donné que les limitations de la FISA ou d'autres lois américaines plus spécifiques ne s'appliquent pas.

136. En ce qui concerne la collecte massive de données, l'EDPB note que l'EO 14086 prévoit que la collecte en vrac continue d'être autorisée. En effet, l'EDPB souligne que la définition de la collecte en vrac reste la même que dans la précédente PPD-28: «*renseignement d'origine électromagnétique collecté en vrac: la collecte autorisée de grandes quantités de données de renseignement d'origine électromagnétique qui, pour des raisons techniques ou opérationnelles, sont acquises sans discrimination (par exemple, sans utilisation d'identifiants ou de termes de sélection spécifiques)*»[144].

137. Depuis l'arrêt Schrems II, la Cour n'a pas précisé avec précision les garanties requises pour la collecte en vrac. Toutefois, l'EDPB rappelle que la CEDH a rendu d'importantes décisions concernant la collecte en vrac et les garanties pertinentes dans ce contexte.

138. L'EDPB rappelle que la collecte en vrac, en permettant la collecte de grandes quantités de données sans discrimination, présente des risques plus élevés pour les personnes[145] que la collecte ciblée et nécessite donc des garanties supplémentaires.

---

[141] Voir l'EO 14086, section 2, point b) i) B

[142] Arrêt Schrems I de la CJUE, point 92.

[143] Voir l'arrêt Schrems II de la CJUE.

[144] Voir EO 14086, section 4, point b).

[145] Voir, par exemple, CEDH (grande chambre), Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021 (ci-après l' «arrêt de la CEDH Big Brother Watch»), considérant 363, où la Cour indique qu'elle «*n'est pas convaincue que l'acquisition de données de communications connexes par interception en vrac soit nécessairement moins intrusive que l'acquisition de contenus*».

139. L'EDPB note également que la CJUE a développé une jurisprudence supplémentaire concernant la conservation des données relatives au trafic et des données de localisation, ainsi que l'accès ultérieur à ces données conservées par les opérateurs de télécommunications, y compris à des fins de sécurité nationale, qui, bien qu'elles ne puissent pas être considérées comme directement applicables dans ce contexte, pourraient, dans une certaine mesure, être pertinentes dans le cadre de la présente évaluation de la collecte en vrac dans le cadre de l'EO 12333.

1) Limitation de la finalité

140. L'EO prévoit que la collecte en vrac ne devrait avoir lieu qu'après qu'il a été établi que «*les informations nécessaires pour faire progresser une priorité validée en matière de renseignement ne peuvent raisonnablement être obtenues par une collecte ciblée*»[146] et que «*la composante des services de renseignement applique des méthodes et des mesures techniques raisonnables afin de limiter les données collectées à ce qui est nécessaire pour faire progresser une priorité validée en matière de renseignement, tout en réduisant au minimum la collecte d'informations non pertinentes*»[147]. Outre ces garanties, l'EDPB reconnaît également que l'utilisation des données collectées en vrac doit être utilisée pour atteindre un ou plusieurs des six objectifs énumérés[148]. L'EDPB souligne en outre que, bien que ces objectifs soient plus détaillés que ceux fournis dans la précédente PPD-28, généralement remplacée par l'EO 14086, l'ampleur de ces possibilités de collecte reste potentiellement large, c'est-à-dire qu'elle englobe des volumes élevés de données.

141. L'EDPB rappelle également ici que l'EO 14086 prévoit également la possibilité pour le président des États-Unis d'ajouter d'autres objectifs à la liste (voir point 115)[149].

2) Autorisation indépendante préalable

142. L'EDPB souligne que la Cour européenne des droits de l'homme accorde une importance considérable à l'autorisation indépendante préalable dans le contexte de la collecte massive de données à des fins de sécurité nationale. En effet, la Cour a jugé en particulier que «*afin de réduire autant que possible le risque d'abus du pouvoir d'interception en masse, la Cour considère que le processus doit être encadré par des "garanties de bout en bout", c'est-à-dire qu'au niveau national, la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ — dès la définition de l'objet et de l'étendue de l'opération, et que les opérations devraient faire l'objet d'une supervision et d'un contrôle indépendant opéré a posteriori. Ces facteurs sont, de l'avis de la Cour, des garanties fondamentales, qui constituent la pierre angulaire de tout régime d'interception en masse conforme aux exigences de l'article 8.*»[150]

143. L'EDPB relève également le point suivant de ce jugement en grande chambre, dans lequel la Cour de Strasbourg souligne par ailleurs qu'elle «*partage l'avis de la chambre selon lequel, si l'autorisation judiciaire constitue une "garantie importante contre l'arbitraire", elle n'est pas une "exigence nécessaire" (voir points 318 à 320 de l'arrêt de la chambre). Néanmoins, l'interception en vrac devrait être autorisée par un organisme indépendant, c'est-à-dire un organe indépendant de l'exécutif*»[151].

[146] EO 14086, section 2, point c) ii) A).
[147] EO 14086, section 2, point c) ii) A).
[148] EO 14086, section 2, point c) ii) B).
[149] EO 14086, section 2, point c) ii) C).
[150] Voir l'arrêt de la CEDH Big Brother Watch, point 350.
[151] Voir l'arrêt de la CEDH Big Brother Watch, point 351.

144. Dans ce contexte, l'EDPB note que l'EO ne prévoit pas une telle autorisation préalable indépendante pour la collecte en vrac, et que cela n'est pas prévu non plus dans le cadre de l'EO 12333 (voir la section ci-dessous sur l'EO 12333).

3) Règles de conservation

145. L'EDPB rappelle qu'un autre ensemble important de garanties est constitué par les règles relatives à la durée de la collecte et de la conservation des données. À cet égard, la CEDH a souligné que «*le droit national devrait fixer une limite concernant la durée de l'interception, la procédure à suivre pour examiner, utiliser et stocker les données obtenues, les précautions à prendre lors de la communication des données à d'autres parties, et les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites*»[152], étant donné que ces garanties «*sont également pertinentes pour l'interception en vrac*»[153].

146. À cet égard, l'EDPB comprend que l'EO prévoit des règles concernant la conservation des données à caractère personnel collectées au moyen de renseignements d'origine électromagnétique, y compris en vrac[154]. L'EDPB note que, conformément à la section 2, point c) iii) A), de l'EO 14086, chaque composante des services de renseignement qui traite les informations à caractère personnel collectées au moyen du renseignement d'origine électromagnétique établit et applique des politiques et des procédures conçues pour réduire au minimum la diffusion et la conservation des informations à caractère personnel collectées au moyen du renseignement d'origine électromagnétique. Toutefois, ces règles ne prévoient pas de durée de conservation spécifique, mais renvoient plutôt, d'une manière générale, aux mêmes règles applicables à la conservation des données concernant des personnes américaines et aux situations dans lesquelles aucune décision définitive de conservation n'a été prise. L'EDPB craint donc que ces durées de conservation, comme pour la collecte ciblée (voir point 122), ne soient pas clairement définies dans ce décret en ce qui concerne les données collectées en vrac. Il invite la Commission à souscrire à son évaluation sur la nécessité et la proportionnalité des périodes de conservation applicables aux ressortissants américains ainsi que les informations disponibles concernant les périodes de conservation dans la pratique lorsqu'aucune décision définitive de conservation n'a été prise en vertu du droit américain, comme dans son état actuel, le projet de décision se bornant à rappeler cette règle générale dans un seul paragraphe succinct[155] et dans une note de bas de page[156] qui ne permet pas de déterminer si ces périodes de conservation sont nécessaires et proportionnées. Étant donné que, comme l'a souligné la CEDH, il s'agit d'une garantie essentielle pour que les personnes concernées puissent exercer leurs droits dans un contexte où une mesure particulièrement intrusive est prise pour collecter leurs données, l'EDPB invite la Commission européenne à fournir des éclaircissements supplémentaires concernant les différentes périodes de conservation dans la pratique.

4) Garanties concernant la «diffusion»

147. En outre, l'EDPB rappelle que, pour garantir l'effectivité de la nécessité et de la proportionnalité ainsi que le principe de limitation de la finalité, la CEDH a également reconnu l'importance des règles

[152] Voir l'arrêt de la CEDH Big Brother Watch, point 348.
[153] Voir l'arrêt de la CEDH Big Brother Watch, point 348.
[154] Voir EO 14086, section 2, points c) iii) A) 2) a) à c).
[155] Voir le projet de décision, considérant 150.
[156] Voir le projet de décision, note de bas de page 271.

prévues par la loi concernant la diffusion ultérieure des données collectées, y compris dans le cadre de la collecte en vrac[157].

148. La section 2 c) iii) A) 1) c) de l'EO 14086 dispose que les informations sur les personnes non américaines qui ont été collectées dans le cadre d'activités de renseignement d'origine électromagnétique ne peuvent être diffusées que si une personne autorisée et dûment formée a des motifs raisonnables de penser que les informations à caractère personnel seront protégées de manière appropriée et que le destinataire a besoin de connaître ces informations.

149. Compte tenu de ce qui précède, l'EDPB comprend que les dispositions relatives à la diffusion au titre de l'EO 14086 ne prévoient pas non plus d'interdiction expresse de diffusion à d'autres fins que celles de la sécurité nationale lorsqu'il s'agit de diffuser auprès des autorités compétentes américaines[158]. L'EDPB invite la Commission à clarifier davantage les règles et garanties applicables en l'espèce.

150. L'EDPB craint donc que les données acquises par les autorités compétentes des services de renseignement ne soient ensuite diffusées aux autorités compétentes des États-Unis aux fins de la lutte contre la criminalité, y compris les infractions graves, dans le cadre d'enquêtes pénales, offrant ainsi aux services répressifs, sans autres restrictions spécifiques, la possibilité d'obtenir des données dont la collecte directe leur aurait été interdite; le comité invite donc la Commission à poursuivre l'examen de ce point.

151. Dans le contexte spécifique des transferts ultérieurs (diffusion à des destinataires extérieurs au gouvernement des États-Unis, y compris à un gouvernement étranger ou à une organisation internationale[159]), l'EDPB rappelle qu'il est d'avis que la protection accordée aux données devrait également être maintenue dans le contexte des transferts ultérieurs, y compris dans le domaine de la sécurité nationale[160].

152. À cet égard, l'EO prévoit certaines garanties, à savoir l'obligation de tenir dûment compte de l'objectif de la diffusion — sans toutefois exiger expressément que la finalité de la diffusion soit également la protection de la sécurité nationale —, de la nature et l'étendue des informations à caractère personnel diffusées ainsi que de l'incidence potentiellement néfaste sur la ou les personnes concernées avant de procéder à la diffusion des données.

153. Bien que l'EDPB reconnaisse que certaines de ces garanties, en particulier la prise en compte de l'«*incidence potentiellement néfaste*»[161] sur la ou les personnes concernées, reflètent certaines exigences de la CEDH, il souligne également que la Cour de Strasbourg exige en outre une obligation juridiquement contraignante «*d'analyser et de déterminer si le destinataire étranger de renseignements offre un niveau minimal acceptable de garanties*»[162], ce que l'EDPB ne trouve pas expressément dans les dispositions de l'EO relatives à la diffusion à des destinataires étrangers. L'EDPB invite donc la Commission à poursuivre l'évaluation de cet élément.

154. L'EDPB note également que la Commission européenne n'a pas examiné, dans le cadre de son évaluation de l'adéquation, l'existence d'accords internationaux existants conclus avec des pays tiers

[157] Voir l'arrêt de la CEDH Big Brother Watch, point 348.
[158] Voir l'EO 14086, section 2, point c) iii) A) 1).
[159] Voir l'EO 14086, section 2, point c) iii) A) 1) d) en particulier.
[160] Voir par exemple l'avis 14/2021 de l'EDPB concernant le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 constatant le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni. Adopté le 13 avril 2021, points 4.3.2.1 et 4.3.2.2.
[161] Voir l'EO 14086, section 2 c) iii) A) 1) d).
[162] Voir CEDH (grande chambre), affaire Centrum För Rättvisa c. Suède, 25 mai 2021, point 326.

ou des organisations internationales susceptibles de prévoir des dispositions spécifiques concernant le transfert international de données à caractère personnel par les services de renseignement vers des pays tiers. L'EDPB considère que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers aux fins de la coopération en matière de renseignement est susceptible d'affecter le cadre juridique en matière de protection des données tel qu'il a été évalué.

155. L'EDPB invite donc la Commission européenne à préciser s'il existe de tels accords, à quelles conditions ils peuvent être conclus et à évaluer si les dispositions des accords internationaux sont susceptibles d'avoir une incidence sur le niveau de protection accordé aux données à caractère personnel transférées depuis l'EEE par le cadre législatif et les pratiques en matière de transferts ultérieurs à des fins de sécurité nationale.

5) Collecte temporaire en vrac pour soutenir la phase technique initiale de la collecte ciblée

156. L'EDPB rappelle que, dans le cadre du dernier examen conjoint du bouclier de protection des données, les discussions ont principalement porté sur l'interprétation et l'application du motif supplémentaire (situation/scénario) pour la collecte en vrac prévu par la première phrase de la note de bas de page 5 de la section 2 de la PPD28, qui prévoyait que «*les limitations contenues dans cette section ne s'appliquent pas aux données de renseignement d'origine électromagnétique qui sont temporairement acquises pour faciliter la collecte ciblée*». Les autorités américaines ont expliqué à l'époque la signification des «*données de renseignement d'origine électromagnétique qui sont acquises temporairement pour faciliter la collecte ciblée*». L'EDPB a compris de ces discussions que cette note de bas de page signifiait que les données pouvaient être collectées en vrac — et indépendamment des six finalités prévues — si elles étaient collectées temporairement, en vue d'établir un identifiant pour un objectif défini. Il s'agirait donc d'un motif supplémentaire de collecte de données en vrac et, dans ce cas, seuls les principes généraux de la section 1 de la PPD-28 auraient encore été applicables. Comme rappelé ci-dessus, dans l'arrêt Schrems II, la CJUE a considéré qu'en ce qui concerne la collecte en vrac, l'EO 12333 combiné à la PPD-28 ne délimitent pas «*de manière suffisamment claire et précise la portée de cette collecte massive de données à caractère personnel*»[163].

157. L'EDPB note qu'une dérogation autorisant ce type de collecte en vrac est toujours prévue dans l'EO 14086[164]; toutefois, l'EDPB se félicite que cette dérogation ait été réduite par rapport à la PPD-28 et que des garanties supplémentaires soient prévues au titre de l'EO 14086.

158. L'EDPB comprend que le nouvel EO 14086 prévoit des garanties qui restent applicables dans le contexte de ce type de collecte technique temporaire de masse, en particulier les principes généraux de nécessité et de proportionnalité en ce qui concerne la priorité validée en matière de renseignement lorsque les données sont acquises sans discrimination avant qu'une collecte ciblée n'ait lieu [section 2, points a) et b), et section 2, point c) i), de l'EO 14086]. L'EDPB comprend également que cette collecte en vrac à l'appui d'une collecte ultérieure ciblée de renseignements d'origine électromagnétique est également soumise aux garanties supplémentaires prévues à partir de la sous-section 2) c) iii)[165].

159. Toutefois, l'EDPB rappelle également — voir le point 117 ci-dessus — que la définition de la «priorité validée en matière de renseignement» prévoit une procédure dérogatoire qui n'impliquerait pas la CLPO du bureau du directeur du renseignement national.

[163] Arrêt Schrems II de la CJUE, point 183.

[164] Voir l'EO 14086, section 2, point c) ii) D) et le projet de décision, note de bas de page 226.

[165] Voir les sections précédentes pour de plus amples informations sur ces dispositions.

160. Toutefois, l'EDPB note toujours que les garanties de la sous-section relative à la collecte en vrac ne s'appliquent pas à la collecte temporaire en vrac utilisée pour soutenir la phase technique initiale de l'activité ciblée de collecte de renseignements d'origine électromagnétique, comme indiqué à la section 2, point c) ii) D), de l'EO 14086, ce qui signifie notamment que, dans ce contexte, les données collectées en vrac peuvent être utilisées à d'autres fins que celles énumérées à la sous-section 2, point c) ii). L'EDPB souhaiterait obtenir des éclaircissements dans le projet de décision sur les finalités pour lesquelles les données collectées en vrac dans ce contexte peuvent être utilisées, ainsi que sur l'application des limitations énoncées à la sous-section 2, point c) i), pour la collecte de renseignements d'origine électromagnétique en général (à savoir uniquement pour les objectifs légitimes qui y sont énumérés) dans le contexte de la collecte temporaire en vrac dans le projet de décision.

161. En conclusion, l'EDPB souligne également que cette dérogation pour la collecte temporaire en vrac en vue d'une collecte ciblée et les garanties restantes à appliquer restent obscures, notamment en ce qui concerne les garanties de l'EO 14086 qui s'appliqueraient à quel stade (collecte en vrac, collecte plus ciblée), et invite la Commission à poursuivre l'évaluation de ces éléments et à évaluer ces aspects également dans la pratique lors des futurs examens conjoints.

162. En outre, bien que l'EDPB regrette également que, même si la notion de «temporairement» a été légèrement plus détaillée dans l'EO que dans la PPD-28, elle semble toujours, selon l'EDPB, signifier que tant que l'objectif n'a pas été défini, la collecte en vrac pourrait se poursuivre. À cet égard, l'EDPB rappelle la nécessité de disposer de règles claires et précises et souligne à cet égard la garantie essentielle que ces règles constituent pour les personnes concernées.

163. En conclusion, en ce qui concerne les garanties applicables à la collecte en vrac, l'EDPB demeure préoccupé par le fait que, malgré les garanties supplémentaires prévues au titre de l'EO 14086, la possibilité de collecter des données en vrac, c'est-à-dire sans discrimination, est toujours prévue, sans garanties essentielles telles que l'autorisation préalable de collecter ces données — notamment dans la situation dérogatoire de la collecte technique temporaire de masse — compte tenu également de la nécessité de nouvelles clarifications et des préoccupations exprimées concernant la limitation stricte de la finalité à l'accès ultérieur aux données, des règles claires et strictes en matière de conservation des données et des garanties plus strictes concernant la diffusion des données collectées en vrac, notamment dans le contexte de transferts ultérieurs.

164. De manière générale, l'EDPB souligne que la décision susmentionnée de la CEDH montre une fois de plus l'importance d'un contrôle complet par des autorités de contrôle indépendantes. L'EDPB souligne qu'une surveillance indépendante à toutes les étapes du processus d'accès des pouvoirs publics à des fins de sécurité nationale constitue une garantie importante contre les mesures de surveillance arbitraires et donc pour l'évaluation d'un niveau adéquat de protection des données. La garantie d'indépendance des autorités de contrôle au sens de l'article 8, paragraphe 3, de la charte vise à assurer un contrôle efficace et fiable du respect des règles de protection des personnes à l'égard du traitement des données à caractère personnel. Cela s'applique en particulier lorsque, en raison de la nature de la surveillance secrète, la personne concernée est empêchée de demander un réexamen ou de participer directement à une procédure de recours avant ou pendant l'exécution de la mesure de surveillance.

165. L'EDPB rappelle qu'il est d'avis que l'évaluation de l'adéquation dépend de toutes les circonstances de l'espèce, en particulier de l'efficacité de la surveillance ex post et des voies de recours prévues par le cadre juridique.

3.2.2.4 Cadre juridique organisant une collecte spécifique à des fins de sécurité nationale par les éléments de la CI à l'intérieur et à l'extérieur du territoire des États-Unis

166. Dans son arrêt Schrems II, la CJUE a souligné, en ce qui concerne l'article 702 de la FISA, que ce texte «*ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non américaines potentiellement visées par ces programmes*»[166]. La Cour considère dès lors que «*dans ces conditions (...), cet article n'est pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui garanti par la charte (...), selon laquelle une base légale qui permet des ingérences dans les droits fondamentaux doit, pour satisfaire au principe de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné et prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales*»[167].

167. En ce qui concerne l'EO 12333, la Cour a relevé qu'il «*ne confère pas de droits opposables aux autorités américaines devant les tribunaux*»[168] et a également conclu que «*dans le cadre des programmes de surveillance fondés sur l'EO 12333, l'accès à des données en transit vers les États-Unis sans que cet accès fasse l'objet d'une quelconque surveillance judiciaire, n'encadre, en tout état de cause, pas de manière suffisamment claire et précise la portée d'une telle collecte en vrac de données à caractère personnel*»[169], à la suite de l'analyse des conditions dans lesquelles la collecte en vrac pouvait avoir lieu en vertu de ce décret, en liaison avec la PPD-28.

168. En ce qui concerne ces régimes spécifiques de collecte de données, l'EO 14086 prévoit désormais de nouvelles règles.

3.2.2.4.1 Collecte de données à des fins de sécurité nationale au titre de l'article 702

169. L'EDPB rappelle que les conclusions relatives à la FISA 702[170] selon lesquelles «*dans la pratique, les "personnes non américaines" bénéficient également des restrictions d'accès et de conservation requises par les procédures de minimisation et/ou de ciblage des différentes agences en raison du coût et de la difficulté d'identifier et de supprimer les informations relatives aux personnes américaines pour un grand nombre de données, ce qui signifie que l'ensemble des données est généralement traité conformément aux normes les plus élevées des États-Unis en matière de données*», ont été saluées dans le dernier rapport du PCLOB.

170. Selon ces constatations, «*le programme ne fonctionne pas par la collecte de communications en vrac*». Les rapports de 2014 et 2021 sur la transparence statistique publiés par l'ODNI ont confirmé cette conclusion. En outre, selon le rapport du PCLOB, les «sélecteurs», tels qu'une adresse électronique ou un numéro de téléphone, sont utilisés pour cibler la surveillance.

171. Toutefois, l'EDPB rappelle également que, dans le même temps, dans le contexte de l'article 702, il a été précisé lors du dernier réexamen du bouclier de protection des données qu'une «personne» devant être identifiée comme cible pouvait désigner plusieurs personnes utilisant le même identifiant, à condition que toutes ces personnes ne soient pas des ressortissants américains et remplissent les

[166] Voir arrêt Schrems II de la CJUE, point 180.
[167] Voir arrêt Schrems II de la CJUE, point 180.
[168] Voir arrêt Schrems II de la CJUE, point 182.
[169] Voir arrêt Schrems II de la CJUE, point 183.
[170] Voir le rapport du PCLOB sur le programme de surveillance mis en œuvre conformément à l'article 702 de la FISA, page 100.

critères applicables pour être ciblées. L'EDPB rappelle également que, lors du troisième examen conjoint annuel du bouclier de protection des données en 2019, des précisions supplémentaires dans le contexte du programme UPSTREAM ont été demandées pour exclure l'accès massif et indifférencié aux données à caractère personnel de ressortissants non américains[171].

172. En outre, l'EDPB rappelle que le fait que la collecte au titre de l'article 702 de la FISA soit justifiée par le fait qu'«*un objectif important de l'acquisition est d'obtenir des informations de renseignement extérieur*» laisse subsister une certaine incertitude quant à sa finalité et à sa nécessité. L'EDPB note toutefois que, conformément à l'EO 14086, section 2, points a) A) et B), les activités de renseignement d'origine électromagnétique ne sont menées qu'après qu'il a été établi que ces activités sont nécessaires pour faire progresser une priorité validée et uniquement dans la mesure et d'une manière qui soient proportionnées à cette priorité et qu'elles soient aussi adaptées que possible pour faire progresser la priorité validée, en tenant dûment compte des facteurs pertinents tels que le caractère intrusif de la collecte, le caractère sensible des données, et qu'elles n'aient pas une incidence disproportionnée sur la vie privée et les libertés civiles. L'EDPB attend encore de nouvelles clarifications sur la manière dont ces mesures seront concrètement rendues opérationnelles et mises en œuvre, notamment dans le cadre de l'application de l'article 702 de la FISA.

173. À cet égard, en l'absence d'un accès direct à ces informations en soi, l'EDPB a demandé une évaluation indépendante de la nécessité et de la proportionnalité de la définition des «cibles» et de la notion de «renseignement extérieur» au titre de l'article 702 de la FISA (y compris dans le contexte du programme UPSTREAM) à la suite de son renouvellement. L'EDPB considère que son appel précédent en faveur d'une évaluation indépendante plus approfondie du processus d'application des sélecteurs dans des cas spécifiques («choix des sélecteurs») ainsi que d'une clarification supplémentaire dans le contexte du programme UPSTREAM est pertinent. Par conséquent, compte tenu du nouvel EO 14086, l'EDPB demande des informations supplémentaires afin d'évaluer et de contrôler également comment et dans quelle mesure les principes de nécessité et de proportionnalité nouvellement introduits seront appliqués dans la pratique dans ce contexte et espère que cela sera également évalué dans le cadre des futurs réexamens conjoints.

174. L'EDPB se félicite que le Conseil de surveillance de la vie privée et des libertés civiles (PCLOB), en tant qu'agence de surveillance indépendante, ait décidé de mener «un projet de supervision pour examiner le programme de surveillance que la branche exécutive gère conformément à l'article 702 de la loi sur la surveillance et le renseignement étranger (FISA), en prévision de la date d'expiration de décembre 2023 pour l'article 702 et de l'examen par le public et le Congrès de sa nouvelle autorisation»[172]. L'EDPB se félicite également du fait que «l'examen couvre certains domaines prioritaires d'enquête, comprenant, entre autres, les questions de personnes américaines concernant les informations collectées au titre de l'article 702, et la collecte "en amont" menée conformément à l'article 702»[173] et «comprend également l'examen de la valeur et de l'efficacité passées et prévues du programme, ainsi que de l'adéquation des garanties existantes en matière de protection de la vie privée et des libertés civiles»[174]. L'EDPB souligne par conséquent que l'accès aux conclusions du PCLOB dans ce rapport sur l'article 702 serait nécessaire pour évaluer de manière adéquate et exhaustive les garanties de protection de la vie privée fournies et appliquées dans le cadre de ce programme de surveillance.

---

[171] Voir le troisième rapport d'examen conjoint, page 17, point 83.

[172] Voir l'AVIS DU PCLOB LE PROJET DE SUPERVISION EXAMINANT L'ARTICLE 702 DE LA LOI SUR LA SURVEILLANCE ET LE RENSEIGNEMENT ÉTRANGER (FISA).

[173] Voir ci-dessus.

[174] Voir ci-dessus.

175. Compte tenu du nouvel EO 14086, l'EDPB demande en outre des informations supplémentaires afin d'évaluer et de contrôler également comment et dans quelle mesure les principes de nécessité et de proportionnalité nouvellement introduits, ainsi que les autres garanties prévues dans ce texte, seront appliqués dans la pratique dans ce contexte.

3.2.2.4.2 Collecte de données à des fins de sécurité nationale en vertu du décret présidentiel n° 12333

176. Comme l'a reconnu la CJUE dans son arrêt Schrems II, l'analyse des lois du pays tiers pour lequel le caractère adéquat est examiné ne devrait pas se limiter aux lois et pratiques permettant une surveillance à l'intérieur des frontières physiques de ce pays, mais devrait également inclure une analyse des fondements juridiques du droit de ce pays tiers qui lui permettent d'exercer une surveillance en dehors de son territoire en ce qui concerne les données de l'Union. Les limitations nécessaires à l'accès des pouvoirs publics aux données devraient s'étendre aux données à caractère personnel «en transit» vers le pays pour lequel le caractère adéquat est reconnu.

177. L'EDPB se félicite du rapport public rédigé par le PCLOB sur le décret présidentiel n° 12333 et publié en avril 2021, mais note que ce rapport reste très général étant donné que la plupart des constatations sont classifiées.

178. Dans ce contexte, une fois de plus, compte tenu de l'incertitude et du manque de clarté sur la manière dont l'EO 12333 était appliqué, et vu l'importance de clarifier la manière dont il sera appliqué à la lumière du nouvel EO 14086, l'EDPB souligne l'importance des rapports du PCLOB attendus sur ce texte[175]. Toutefois, l'EDPB comprend que la majeure partie de son contenu restera probablement classifié, de sorte qu'aucune autre information sur le fonctionnement concret de l'EO 12333 et sur sa nécessité et sa proportionnalité ne serait mise à la disposition du public, ni de l'EDPB.

179. L'EDPB accueillerait donc particulièrement favorablement le rapport du PCLOB sur l'application de l'EO 14086 qui n'est pas classifié mais totalement accessible une fois qu'il sera achevé, y compris sur les parties qui évalueraient la manière dont les garanties de l'EO 14086 seront appliquées à la collecte de données au titre de l'EO 12333. L'EDPB invite également la Commission à être particulièrement attentive à ce point dans le cadre des futurs examens conjoints.

180. D'une manière générale, en ce qui concerne les différents instruments juridiques prévoyant la possibilité pour les agences de renseignement américaines de collecter et de continuer à accéder aux données et de les traiter dans le cadre juridique américain, l'EDPB souhaiterait obtenir des éclaircissements quant à leur interaction avec le nouvel EO 14086 et espère que l'adoption de ces nouvelles garanties permettrait de répondre aux préoccupations exprimées précédemment dans les avis précédents de l'EDPB à leurs yeux.

181. L'EDPB invite également la Commission à être particulièrement attentive à ces aspects dans le cadre des futurs examens conjoints.

[175] Le rapport général sur l'EO 12333 est resté pour l'essentiel classifié — seule une brève version publique a été publiée, de même que le rapport et les recommandations sur les activités de lutte contre le terrorisme menées par la CIA en vertu de l'EO 12333, qui ne sont que partiellement déclassifiés.

3.2.2.4.3 Rapport du PCLOB

182. L'EDPB se félicite que l'EO 14086 prévoie également l'obligation pour le PCLOB de produire un rapport concernant la mise en œuvre de l'EO. L'EDPB souligne que ce rapport devrait inclure une évaluation de cette possibilité spécifique offerte par l'EO de collecter des données, aux fins énumérées pour une collecte ciblée, ainsi qu'en vrac, y compris pour des raisons techniques, afin de mieux comprendre les termes clés de l'EO 14086 et la manière dont ils sont concrètement compris et appliqués dans les différents programmes de surveillance. Ce rapport serait également nécessaire pour évaluer la manière dont l'EO sera mis en œuvre dans les procédures et politiques internes des composantes des services de renseignement.

3.2.3 Garantie C — Contrôle

3.2.3.1 Introduction

183. Les activités de renseignement des États-Unis sont soumises à un processus de surveillance à plusieurs niveaux. La structure de surveillance aux États-Unis peut être divisée en contrôles internes et externes. Toutes les composantes des services de renseignement disposent d'agents chargés de la surveillance et du respect des règles, qui exercent un contrôle périodique sur les activités de renseignement d'origine électromagnétique, y compris les agents chargés de la protection de la vie privée et des libertés civiles et les inspecteurs généraux. En outre, il existe des organes de contrôle externes, tels que le Conseil de surveillance de la vie privée et des libertés civiles (PCLOB) et le Conseil de surveillance du renseignement.

184. L'EDPB rappelle qu'une ingérence a lieu au moment de la collecte des données, mais aussi au moment où une autorité publique accède aux données en vue d'un traitement ultérieur. La CEDH a précisé à de nombreuses reprises que toute ingérence dans le droit à la vie privée et à la protection des données devrait être soumise à un système de contrôle effectif, indépendant et impartial, prévu par un juge ou par un autre organe indépendant[176] (par exemple, une autorité administrative ou un organe parlementaire).

185. Si la CEDH a exprimé sa préférence pour qu'un juge soit responsable de la surveillance, elle n'a pas exclu qu'un autre organe puisse être responsable, «*à condition que l'autorité soit suffisamment indépendante du pouvoir exécutif*»[177] et «*des autorités chargées de la surveillance, et qu'elle [soit] dotée de pouvoirs et de compétences suffisants pour exercer un contrôle effectif et continu*»[178].

186. La CEDH a ajouté que «*le mode de désignation et le statut juridique des membres de l'organe de contrôle*»[179] doivent être pris en compte dans l'appréciation de l'indépendance.

187. La CEDH a également précisé qu'il s'agissait d'examiner si les activités de l'organe de contrôle étaient susceptibles de faire l'objet d'un contrôle public. À titre d'exemple, cela pourrait se faire lorsque les

[176] CEDH, affaire Klass et autres c. Allemagne, 6 septembre 1978 (ci-après l'«arrêt Klass de la CEDH»), points 17 et 51.
[177] Arrêt de la CEDH dans l'affaire Zakharov, point 258; CEDH, Iordachi et autres c. Moldavie, 10 février 2009, points 40 et 51; CEDH, Dumitru Popescu c. Roumanie, 26 avril 2007, points 70 à 73.
[178] CEDH, arrêt Klass, point 56.
[179] CEDH, arrêt Zakharov, point 278.

rapports de supervision annuels au gouvernement ou les rapports publics sont présentés au Parlement et ont été examinés par le Parlement[180].

188. Le contrôle indépendant de la mise en œuvre des mesures de surveillance a également été pris en compte par la CJUE dans l'arrêt Schrems II, étant donné que «*(...) le contrôle exercé par le FISC vise à vérifier si ces programmes de surveillance correspondent à l'objectif d'obtenir des informations en matière de renseignement extérieur, mais ne porte pas sur le point de savoir "si les personnes sont correctement ciblées pour se procurer des informations en matière de renseignement extérieur"*»[181].

3.2.3.2 Surveillance interne

3.2.3.2.1 Inspecteur général

189. L'EDPB reconnaît que les inspecteurs généraux se voient confier un large éventail d'autorisations, nécessaires au suivi des activités de renseignement. En particulier, les inspecteurs généraux ont accès à toutes les informations nécessaires pour évaluer la conformité globale du travail des agences avec la législation, y compris, entre autres, les lois relatives au respect de la vie privée et à la protection des données, et peuvent émettre des injonctions et faire prêter serment à toute personne dans le cadre de l'enquête des inspecteurs généraux.

190. Sur la base de ce qui précède, l'EDPB considère que les inspecteurs généraux disposent généralement de pouvoirs d'enquête étendus. Toutefois, ils ne disposent pas de pouvoirs contraignants en matière de mesures correctives et ne formulent que des recommandations non contraignantes[182].

191. L'EDPB reconnaît qu'en principe, les inspecteurs généraux ne sont pas empêchés et il ne leur est pas interdit d'ouvrir, de réaliser ou de mener à bien un audit ou une enquête, ou d'adresser une ordonnance d'injonction au cours d'un audit ou d'une enquête[183]. Dans ce contexte, l'EDPB note toutefois que les inspecteurs généraux sont placés sous l'autorité, la direction et le contrôle du chef de département concerné, qui peut leur interdire l'accès à l'information, entreprendre une enquête et, entre autres, émettre des injonctions dans les cas où le chef de département estime qu'une telle interdiction est nécessaire pour préserver les intérêts nationaux. Toutefois, le chef de département doit informer les commissions compétentes du Congrès américain de l'exercice de cette autorité[184].

192. L'EDPB note que les inspecteurs généraux ne peuvent être révoqués que par le président des États-Unis, qui doit informer le Congrès des raisons de cette révocation.

193. L'EDPB note que le mécanisme de surveillance interne n'a pas été modifié de manière significative depuis les avis du GT art. 29 puis de l'EDPB. Par conséquent, l'EDPB estime, conformément à l'avis 01/2016 du GT art. 29[185], que, d'une manière générale, des mécanismes de contrôle interne suffisants sont en place.

---

[180] CEDH, arrêt dans l'affaire Zakharov, point 283; CEDH, L. c. Norvège, 9 juin 1990; CEDH, Kennedy c. Royaume-Uni, 18 mai 2010, point 166.
[181] CJUE, arrêt Schrems II, point 179.
[182] Voir le projet de décision, considérant 105.
[183] Loi sur l'inspecteur général de 1978 (Inspector General Act), article 3 point a).
[184] Voir par ex. la loi sur l'inspecteur général de 1978, article 8 (pour le ministère de la défense), article 8 E (pour le DOJ), article 8 G d) 2) A) et B) (pour la NSA), le titre 50 de l'USC, article 403 q b) (pour la CIA), et l'Intelligence Authorization Act For Fiscal Year 2010, article 405 f) (pour le secteur du renseignement).
[185] Avis 01/2016 du GT art. 29.

3.2.3.3 Surveillance interne

194. L'EDPB note qu'outre les organismes mentionnés ci-dessous, divers autres organismes du gouvernement américain supervisent les activités des agences de renseignement américaines, tels que le Conseil de surveillance du renseignement (*Intelligence Oversight Board* — IOB) ou les comités du Congrès. Ces derniers peuvent mener leurs propres enquêtes et rapports.

3.2.3.3.1 Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles — PCLOB)

195. L'EDPB reconnaît le rôle global de surveillance du PCLOB en ce qui concerne le nouveau mécanisme de recours et la mise en œuvre de l'EO 14086.

196. Premièrement, ses nouvelles fonctions prévoient des consultations avec le procureur général en ce qui concerne la nomination des juges de la DPRC et des avocats spéciaux. Deuxièmement, le PCLOB examinera chaque année la procédure de recours, c'est-à-dire le traitement des plaintes recevables par le mécanisme de recours. Il s'agit notamment de savoir si le CLPO et la Cour de contrôle de la protection des données (DPRC) ont traité les plaintes recevables en temps utile, obtiennent un accès complet aux informations nécessaires et fonctionnent conformément à l'EO 14086, ainsi que savoir si les services de renseignement respectent les décisions prises par le CLPO et la DPRC.

197. En outre, le PCLOB doit être consulté lors de la mise à jour par les agences de renseignement de leurs politiques et procédures internes pour mettre en œuvre l'EO 14086. En outre, le PCLOB procédera à un examen des politiques et procédures mises à jour et évaluera leur conformité avec l'EO 14086[186]. Bien que les conclusions du PCLOB ne soient pas contraignantes stricto sensu, le chef de chaque composante des services de renseignement est tenu d'examiner et de mettre en œuvre avec soin toutes les recommandations contenues dans un tel réexamen, ou d'y donner suite, conformément à la législation applicable[187]. L'EDPB invite la Commission à accorder une attention particulière à la question de savoir si et comment les recommandations du PCLOB ont été mises en œuvre au niveau des agences lors des futurs examens, si le projet de décision est adopté.

198. L'EDPB rappelle que le PCLOB, vu qu'il est indépendant, est «encouragé» à agir, mais n'est pas tenu de contrôler si les garanties constituées par l'EO 14086 sont dûment prises en considération et si les services de renseignement se sont pleinement conformés aux exigences de la procédure de recours. Toutefois, l'EDPB comprend que le PCLOB a déclaré dans ses explications supplémentaires à l'EDPB ainsi qu'en public[188] qu'il assumera le rôle prévu dans l'EO 14086.

199. En outre, l'EDPB se félicite que les résultats des rapports du PCLOB soient destinés à être rendus publics. Compte tenu du fait que les différents organes du mécanisme de recours et ceux des services de renseignement doivent en principe mettre en œuvre les recommandations figurant dans les rapports du PCLOB ou y donner suite d'une autre manière, l'EDPB reconnaît que ces recommandations jouent un rôle important dans les garanties de protection de la vie privée.

[186] EO 14086, section 2, point c) iv), et section 2, point c) v).
[187] EO 14086, article 2, point c) v) B).
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

200. L'EDPB note que l'accès du PCLOB à l'information est limité si le président des États-Unis autorise la conduite d'«actions secrètes»[189] par des ministères, agences ou entités du gouvernement des États-Unis[190].

201. À la suite de ses avis antérieurs, l'EDPB considère le PCLOB comme un organe indépendant, dont les recommandations ont contribué de manière importante aux réformes aux États-Unis et dont les rapports ont été une source particulièrement utile pour comprendre le fonctionnement des différents programmes de surveillance, qui constituent un élément essentiel de la structure de surveillance.

202. Toutefois, dans son 3e examen conjoint annuel de l'ancien bouclier de protection des données UE-États-Unis, le comité a déploré que le PCLOB ne lui ait fourni que les mêmes informations que celles communiquées au grand public. En outre, il est regrettable que le PCLOB n'ait pas publié d'autres rapports sur la PPD-28 pour donner suite à son premier rapport afin de fournir des éléments supplémentaires sur la manière dont les garanties de la PPD-28 sont appliquées, ainsi qu'un rapport général actualisé sur l'article 702 de la FISA.

203. Par conséquent, l'EDPB se félicite de l'annonce du PCLOB à l'intention du comité, selon laquelle la publication d'un rapport de suivi sur l'article 702 de la FISA peut être attendue dans un avenir proche. En outre, l'EDPB est convaincu que le PCLOB a informé de sa volonté d'autoriser la publicité de ses rapports concernant l'EO 14086. Toutefois, l'EDPB rappelle que la publication de rapports non classifiés est régie par le droit américain et doit être coordonnée avec les agences des services de renseignement et ne peut être décidée par le PCLOB de sa propre initiative.

204. Par conséquent, si le projet de décision est adopté, l'EDPB rappelle que, lors des futurs examens du cadre de protection des données UE–États-Unis, les experts habilités par l'EDPB devraient être en mesure d'examiner des documents supplémentaires et de discuter d'autres éléments classifiés supplémentaires si nécessaire pour garantir que les informations contenues dans les rapports puissent être correctement évaluées, tout en tenant compte des intérêts nationaux pertinents en matière de sécurité et des dispositions applicables en matière de protection de la vie privée.

205. L'EDPB se félicite de l'indépendance du PCLOB et de sa surveillance de la communauté nationale du renseignement, qui doit se conformer aux recommandations du PCLOB ou y répondre autrement, ce qui figurera dans le rapport du PCLOB au Congrès américain.

206. Compte tenu des exigences de la Cour européenne des droits de l'homme relatives au contrôle public[191] selon lesquelles les rapports d'un organe de contrôle doivent être présentés devant le Parlement et examinés par celui-ci, l'EDPB estime suffisant que le PCLOB soumette ses rapports au moins tous les six mois au président des États-Unis et, en particulier, aux commissions du Congrès du Sénat et de la Chambre des représentants[192], qui sont les organes parlementaires des États-Unis.

[189] Selon le titre 50 du Code des États-Unis, article 3093, point e) 1), le terme «action secrète» désigne une activité ou des activités du gouvernement des États-Unis visant à influencer les conditions politiques, économiques ou militaires à l'étranger, lorsqu'il est prévu que le rôle du gouvernement des États-Unis ne sera pas visible ou reconnu publiquement, mais ne comprend pas 1) les activités dont l'objectif premier est d'acquérir des renseignements, des activités traditionnelles de contre-espionnage [...].

[190] Titre 42 du Code des États-Unis, article 2000ee, point g) 5); Titre 50 du Code des États-Unis, article 3093, point a).

[191] CEDH, arrêt Zakharov, point 283; L. c. Norvège, 9 juin 1990; CEDH, Kennedy c. Royaume-Uni, 18 mai 2010, point 166.

[192] Titre 42 du Code des États-Unis, article 2000ee, point e).

3.2.3.3.2 Cour de surveillance du renseignement étranger (Foreign Intelligence Surveillance Court - FISC)

207. La Cour de surveillance du renseignement étranger est chargée de surveiller la collecte de données à caractère personnel conformément à l'article 702 de la FISA[193] et les décisions de la FISC peuvent faire l'objet d'un recours devant la Cour de contrôle de la surveillance du renseignement étranger (*Foreign Intelligence Surveillance Court of Review* - FISCR).

208. La FISC supervise le processus de certification pour la collecte d'informations en matière de renseignement étranger conformément à l'article 702 de la FISA et autorise la surveillance électronique, les recherches physiques et d'autres mesures d'enquête à des fins de renseignement étranger[194]. La FISC autorise également les procédures de ciblage, de minimisation et d'interrogation des certificats, qui sont juridiquement contraignantes pour les services de renseignement américains[195]. Si la FISC constate que les exigences n'ont pas été respectées, il peut refuser la certification en tout ou en partie et demander la modification des procédures.

209. Si des violations des procédures de ciblage sont constatées, la FISC peut ordonner à l'agence de renseignement compétente de prendre des mesures correctives[196]. Ces mesures peuvent être d'ordre individuel ou structurel, et aller, par exemple, de l'arrêt de l'acquisition de données à la suppression de données obtenues illégalement en passant par le changement de pratique en matière de collecte des données, y compris en ce qui concerne les orientations et les formations destinées au personnel.

210. L'EDPB reconnaît que l'EO 14086 prévoit que le CLPO et la DPRC signalent les violations au procureur général adjoint pour la sécurité nationale, qui les signale à la FISC[197].

211. Comme la CJUE l'a relevé dans sa décision Schrems II, la FISC n'autorise pas de mesures de surveillance individuelles; elle autorise plutôt des programmes de surveillance[198]. Par conséquent, l'EDPB maintient sa préoccupation quant au fait que la FISC n'assure pas un contrôle judiciaire effectif du ciblage de personnes non américaines, ce qui ne semble pas être résolu par le nouvel EO 14086.

212. En ce qui concerne l'autorisation indépendante préalable[199] de surveillance au titre de l'article 702 de la FISA, l'EDPB regrette que, comme il ressort du projet de décision[200] et des explications fournies par le gouvernement américain, la FISC ne semble pas liée par les garanties supplémentaires de l'EO 14086 lorsqu'elle certifie les programmes autorisant le ciblage de personnes non américaines. De l'avis de l'EDPB, les garanties supplémentaires contenues dans ce décret devraient néanmoins être prises en compte dans ce contexte. L'EDPB rappelle que les rapports du PCLOB seraient particulièrement utiles pour évaluer comment les garanties de l'EO 14086 seront mises en œuvre et comment ces garanties sont appliquées lorsque les données sont collectées au titre de l'article 702 de la FISA.

---

[193] Titre 50 du code des États-Unis, article 1881, point a).
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] Titre 50 du code des États-Unis, article 1881a, point i).
[196] Titre 50 du code des États-Unis, article 1803, point h).
[197] EO 14086, section 3, point c) i) D); EO 14086, section 3, point d) i) F).
[198] Arrêt Schrems II de la CJUE, point 179.
[199] En ce qui concerne la collecte de données en vrac au titre de l'EO 12333 lorsque la FISC n'est pas compétente, l'EDPB craint qu'il n'existe pas de procédure d'autorisation préalable pour la collecte de données en vrac (voir également la garantie B).
[200] Voir le projet de décision, considérant 165.

3.2.4 Garantie D – Les particuliers devraient disposer de voies de recours effectives

213. L'EDPB rappelle que des droits effectifs et opposables de la personne sont d'une importance fondamentale pour conclure à l'existence d'un niveau adéquat de protection des données dans un pays tiers. Les personnes concernées doivent disposer d'un recours effectif pour faire valoir leurs droits lorsqu'elles estiment qu'elles ne sont pas ou n'ont pas été respectées. Dans les arrêts Schrems I et II, la CJUE a expliqué qu'«une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la charte»[201].

214. Le système américain relatif aux recours juridictionnels contient une limite importante qui rend très difficile l'introduction de procédures judiciaires contre les mesures de surveillance prises par le gouvernement américain devant les juridictions ordinaires. La constitution américaine impose à une personne de démontrer sa qualité pour agir, c'est-à-dire d'établir un «préjudice concret, particulier et réel ou imminent»[202]. Dans les affaires de surveillance, cette exigence semble être neutralisée par l'absence de notification aux personnes faisant l'objet d'une surveillance, même après la fin de ces mesures.

215. Dans ce contexte, l'EDPB se félicite que l'EO 14086 mette en place un mécanisme de recours spécifique pour traiter et résoudre les plaintes émanant de ressortissants non américains concernant des activités de renseignement d'origine électromagnétique américaines. Dans le cadre de ce nouveau mécanisme, l'exigence de qualité pour agir n'est pas applicable: conformément à la section 4, point k) ii), de l'EO 14086, le demandeur n'est pas tenu de démontrer que ses données ont effectivement fait l'objet de renseignements d'origine électromagnétique aux États-Unis. Les personnes concernées peuvent donc invoquer les garanties prévues par l'EO 14086, y compris celles prévues par d'autres lois et dispositions pertinentes visées à la section 4, point d) iii), de l'EO 14086[203]. À cet égard, le nouveau mécanisme ajoute une voie de recours qui, autrement, n'existerait pas.

216. Le nouveau mécanisme se compose de deux niveaux: Au premier niveau, les personnes peuvent déposer une plainte auprès du délégué à la protection des libertés civiles du bureau du directeur du renseignement national (CLPO). Au deuxième niveau, les personnes ont la possibilité de former un recours contre la décision du CLPO devant un organe nouvellement créé, appelé «Cour de contrôle de la protection des données» *(Data Protection Review Court* - DPRC). Les sections suivantes se concentrent principalement sur le deuxième niveau du mécanisme de recours. L'EDPB considère que le CLPO, en tant que fonctionnaire du gouvernement, n'est pas doté d'un degré suffisant d'indépendance par rapport au pouvoir exécutif et ne peut donc, en soi, satisfaire de manière adéquate aux exigences découlant de l'article 47 de la charte. Cette évaluation a été confirmée à plusieurs reprises par la Commission.

3.2.4.1 L'établissement de la DPRC sur la base d'un décret présidentiel est-il suffisant en soi?

217. La DPRC n'est pas une juridiction ordinaire établie par le Congrès en vertu de l'article III de la Constitution américaine, mais se fonde sur un décret présidentiel émis par le président des États-Unis. Bien que l'EDPB soit conscient de la considération sous-jacente, à savoir le fait d'éviter l'obligation de

[201] Arrêt Schrems I de la CJUE, point 95; arrêt Schrems II de la CJUE, point 187.
[202] Clapper c. Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.
[203] L'EO 14086, section 5, point h), crée explicitement le droit pour les personnes concernées d'introduire des réclamations conformément au mécanisme de recours.

démontrer sa qualité pour agir (voir également le point 215), et qu'il l'accueille favorablement d'une manière générale, cela soulève une question fondamentale: ce mécanisme de recours peut-il satisfaire (en tout ou en partie) aux exigences de l'article 47 de la charte? En vertu de cette disposition, toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal établi préalablement par la loi.

218. Alors que le libellé anglais de l'article 47 de la charte fait référence à un «tribunal», d'autres versions linguistiques donnent la préférence au mot «juridiction»[204]. L'arrêt Schrems II de la CJUE a rappelé que «les personnes concernées doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données»[205]. Toutefois, dans le même contexte d'appréciation du caractère adéquat du niveau de protection des données, la CJUE considère qu'une protection juridictionnelle effective contre de telles ingérences peut être assurée non seulement par une juridiction, mais également par un organe qui offre des garanties substantiellement équivalentes à celles exigées par l'article 47 de la charte[206]. De même, la convention européenne des droits de l'homme dispose que «[t]oute personne dont les droits et libertés ont été violés dispose d'un recours effectif devant une autorité nationale»[207], qui, selon une jurisprudence constante de la CEDH, ne doit pas nécessairement être une autorité judiciaire[208]. Au contraire, les pouvoirs et les garanties procédurales dont dispose une autorité, en particulier la question de savoir si elle est indépendante du pouvoir exécutif et si elle garantit l'équité de la procédure, sont pertinents pour apprécier l'efficacité du recours devant cette autorité[209]. Il apparaît que les deux juridictions ne fondent pas leur appréciation sur des critères purement formalistes, mais considèrent les garanties matérielles comme décisives.

219. Dans l'arrêt Schrems II, la CJUE a accordé une attention particulière à l'existence d'un recours effectif dans le domaine de l'accès aux données à caractère personnel en matière de sécurité nationale. L'EDPB prend acte du fait que, ce faisant, la CJUE n'a pas examiné l'élément «préalablement établi par la loi» de l'article 47 de la charte, alors même que le mécanisme du médiateur du bouclier de protection des données n'était pas non plus fondé sur le droit législatif américain. Au lieu d'aborder cette question, la CJUE a examiné différents aspects pour son critère d'adéquation, tels que l'absence de pouvoirs de correction. Par conséquent, l'arrêt Schrems II ne fournit aucune indication sur l'appréciation de la notion d'«établi préalablement par la loi» au sens de l'article 47 de la charte. Toutefois, il existe d'autres arrêts dans lesquels la CJUE a formulé des observations à ce sujet. Faisant écho à la jurisprudence constante de la CEDH à cet égard, la CJUE a rappelé dans ses affaires C-487/19 et C-132/20 que l'introduction de l'expression «préalablement établi par la loi» vise à garantir que l'organisation du système judiciaire dans une société démocratique ne dépend pas du pouvoir discrétionnaire du pouvoir exécutif, mais qu'elle est régie par la loi émanant du législateur dans le respect des règles régissant sa compétence[210]. Ainsi qu'il ressort de cette déclaration, le droit à un tribunal établi préalablement par la loi est très étroitement lié à la garantie d'indépendance.

[204] Par exemple, «Gericht» dans la version allemande.
[205] Arrêt Schrems II de la CJUE, point 194.
[206] Arrêt Schrems II de la CJUE, point 197.
[207] Article 13 de la convention européenne des droits de l'homme.
[208] CEDH, arrêt Klass, point 67; CEDH, arrêt Big Brother Watch, point 359.
[209] CEDH, arrêt Klass, point 67; CEDH, arrêt Big Brother Watch, point 359.
[210] Voir CJUE, C-487/19, arrêt du 6 octobre 2021, W.Ż, ECLI:EU:C:2021:798, et C-132/20, arrêt du 29 mars 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, points 129 et 121.

220. Dans ce contexte, l'EDPB conclut que, dans le cadre de l'évaluation du caractère adéquat du niveau de protection, le mécanisme de recours spécifique créé au titre de l'EO 14086 par opposition à un recours dans les juridictions visées à l'article III n'est pas en soi insuffisant. L'analyse du niveau de protection à cet égard dépend de la question de savoir si les garanties prévues dans l'EO 14086 et complétées par le règlement relatif au procureur général garantissent suffisamment l'indépendance de la DPRC par rapport aux autres pouvoirs.

221. La Commission devrait contrôler en permanence si les règles énoncées dans l'EO 14086 et ses dispositions complémentaires, en particulier celles destinées à favoriser l'indépendance de la DPRC, sont pleinement mises en œuvre et fonctionnent efficacement dans la pratique. En outre, toute modification du cadre devrait faire l'objet d'un examen attentif en ce qui concerne l'incidence sur l'évaluation de la Commission conformément au projet de décision. À cet égard, l'EDPB note que les modifications apportées à l'EO 14086 et au règlement relatif au procureur général peuvent entraîner l'adoption d'actes d'exécution immédiatement applicables suspendant, abrogeant ou modifiant la décision d'adéquation[211].

3.2.4.2 Indépendance suffisante vis-à-vis de l'exécutif

222. Dans son arrêt Schrems II, la CJUE a souligné que l'indépendance de la juridiction ou de l'organe doit être assurée, en particulier vis-à-vis de l'exécutif, avec toutes les garanties nécessaires, y compris en ce qui concerne ses conditions de licenciement ou de révocation de la nomination. Plus précisément, la CJUE a critiqué le fait que le médiateur a été nommé par le secrétaire d'État et qu'il lui rend compte directement. Le médiateur a été considéré comme faisant partie intégrante du département d'État américain. La CJUE a également constaté qu'il n'existait pas de garanties particulières concernant le licenciement ou la révocation de la nomination du médiateur, compromettant ainsi l'indépendance du médiateur par rapport au pouvoir exécutif.

223. L'EDPB reconnaît que les dispositions de l'EO 14086 et du règlement complémentaire relatif au procureur général n'imposent pas au procureur général d'obligation de rapport à la DPRC, comme ce serait le cas dans une relation de supérieur à subordonné. La DPRC n'est pas non plus soumise à la «surveillance quotidienne» du procureur général[212]. Ces garanties constituent une amélioration significative par rapport au bouclier de protection des données. Toutefois, la DPRC est établie au sein du pouvoir exécutif, à savoir le ministère de la justice. Pour cette raison, en particulier, la mise en œuvre et le fonctionnement efficace des mesures de sauvegarde dans la pratique seront essentiels pour déterminer si la DPRC, bien qu'elle ne fasse pas partie intégrante du ministère de la justice, en tant qu'entité néanmoins située au sein de l'exécutif, peut être considérée comme suffisamment indépendante dans la pratique. L'EDPB invite la Commission à contrôler attentivement si ces garanties sont pleinement prises en compte dans la pratique. En outre, l'EDPB suggère de clarifier l'expression «surveillance quotidienne» pour que les «juges» de la DPRC ne soient soumis à aucune surveillance. La Commission a confirmé que la notion de «surveillance quotidienne» devait être comprise dans ce sens.

224. Outre les garanties susmentionnées, le CPD UE–États-Unis prévoit certaines garanties concernant la nomination et la révocation des «juges» de la DPRC. Bien qu'ils soient nommés par le procureur général, leur nomination repose sur les critères utilisés pour évaluer les candidats aux postes de juges fédéraux et implique une consultation du PCLOB. La révocation des «juges» avant l'expiration de leur

[211] Voir le projet de décision, considérant 212.
[212] Règlement relatif au procureur général, article 201.7, point d).

mandat ou dans le cadre d'une procédure en cours n'est possible que dans des circonstances clairement définies qui, comme le comprend l'EDPB, sont inspirées des dispositions applicables aux juges fédéraux[213]. L'application de ces règles représente une nouvelle étape dans le renforcement d'indépendance de la DPRC, dont la mise en œuvre dans la pratique sera, à nouveau, fondamentale. Toutefois, il ne ressort pas clairement du projet de décision en tant que tel si et comment le respect de ces exigences sera observé aux États-Unis. Sur la base des explications supplémentaires fournies par la Commission et le gouvernement des États-Unis, l'EDPB comprend que le PCLOB peut tenir compte des dispositions susmentionnées dans son examen annuel de la procédure de recours et que la responsabilité de contrôler et de garantir le respect de toutes les exigences légales de l'inspecteur général au sein du ministère de la justice inclut les exigences de l'EO 14086 et les règlements instituant la DPRC. L'EDPB invite la Commission à clarifier cet aspect dans le projet de décision. Cela étant dit, la Commission devrait tenir compte de ces garanties lorsqu'elle contrôle la pratique réelle du traitement des données à caractère personnel, telle qu'évaluée dans le projet de décision.

225. Le projet de décision n'aborde pas la question de savoir si et, dans l'affirmative, dans quelles conditions le président des États-Unis a le pouvoir de démettre ou de révoquer des «juges» de la DPRC. L'EDPB croit comprendre qu'un tel pouvoir n'existe pas, comme l'a expliqué la Commission européenne, ce qui a été confirmé par des représentants du gouvernement américain. L'EDPB suggère de clarifier cet aspect dans la décision d'adéquation.

226. Les «juges» de la DPRC sont nommés pour un mandat de quatre ans renouvelable et, au moment de leur nomination initiale, ils ne doivent pas avoir été employés dans le pouvoir exécutif au cours des deux années précédentes[214]. Pendant leur mandat en tant que «juges» au sein de la DPRC, ils n'exercent aucune autre fonction officielle ni aucun autre emploi au sein du gouvernement américain[215]. Ils peuvent toutefois, contrairement aux juges fédéraux américains, participer à des activités extrajudiciaires, y compris des activités commerciales, des activités financières, des activités de collecte de fonds à but non lucratif, des activités fiduciaires et pratiquer le droit, lorsque ces activités n'entravent pas l'exercice impartial de leurs fonctions ou l'efficacité ou l'indépendance de la DPRC[216]. L'indépendance de la justice découle non seulement de l'absence d'instructions, mais aussi de l'indépendance personnelle. Dans ce contexte, des facteurs tels que le mandat, la possibilité d'être reconduit et le risque de conflits d'intérêts sont importants. Le mandat de quatre ans prévu respectivement par l'EO 14086 et le règlement AG, tout en étant, par exemple, plus court que les mandats des juges de la CJUE (six ans avec possibilité de reconduction) et de la Cour européenne des droits de l'homme (neuf ans sans possibilité de renouvellement du mandat) ne suscite pas, en tant que tel, de graves préoccupations. L'EDPB n'a connaissance d'aucune jurisprudence imposant un mandat minimal à cet égard[217]. L'EDPB reconnaît également que la possibilité de se livrer à des activités extrajudiciaires est subordonnée à la condition que, pour le dire simplement, elles ne conduisent pas à des conflits d'intérêts compromettant les obligations de la DPRC. L'EDPB comprend, d'après les explications supplémentaires du gouvernement américain, que ces exigences sont également soumises à l'examen et au contrôle du PCLOB et de l'inspecteur général du ministère de la justice (voir

[213] EO 14086, section 3, point d) iv); Règlement AG, article 201.7.
[214] Règlement AG, article 201.3 a).
[215] Règlement AG, article 201.3 c).
[216] Règlement AG, article 201.7 c).
[217] Voir également, mutatis mutandis, CEDH (grande chambre), affaire Centrum För Rättvisa c. Suède, 25 mai 2021, point 346.

point 226 ci-dessus). La manière dont cette exigence sera appliquée et démontrée dans la pratique devrait également être abordée dans le cadre des réexamens conjoints.

227. Conformément à la section 3, point d) i) B), de l'EO 14086, tous les «juges» de la DPRC doivent détenir des habilitations de sécurité pour pouvoir accéder à des informations classifiées, c'est-à-dire pour exercer leur fonction même de juger des affaires de sécurité nationale[218]. En revanche, certaines lois et réglementations européennes en matière d'habilitation de sécurité dispensent les juges de l'obligation d'une habilitation de sécurité dans la mesure où ils exercent des fonctions judiciaires, considérant un contrôle aussi détaillé comme potentiellement contraire à l'indépendance de la justice[219]. Selon les explications fournies par le gouvernement américain, alors qu'un candidat à une nomination judiciaire auprès d'une juridiction américaine fait l'objet d'une vérification approfondie, après avoir été nommé juge fédéral au sein d'une juridiction américaine, un juge fédéral n'est pas tenu d'obtenir une habilitation de sécurité pour accéder à des documents classifiés pertinents pour une affaire.

228. De l'avis de l'EDPB, les circonstances décrites ci-dessus révèlent en partie des différences entre la position et le statut d'un juge fédéral américain et d'un «juge» de la DPRC. Toutefois, les mesures de sauvegarde fournies ne permettent pas de douter de l'indépendance de la DPRC. L'EDPB demande instamment à la Commission que, si le projet de décision était adopté, les garanties susmentionnées soient une priorité lors du premier examen conjoint du CPD UE–États-Unis. En outre, l'EDPB attend de la Commission qu'elle donne suite à son engagement de suspendre, d'abroger ou de modifier la décision, si elle est adoptée, au cas où l'exécutif américain choisirait de restreindre les garanties incluses dans l'EO[220].

3.2.4.3 Pouvoirs de la DPRC

3.2.4.3.1 Accès à l'information

229. Une protection juridictionnelle effective exige qu'une juridiction dispose de pouvoirs d'enquête suffisants pour contrôler la mesure contestée. Dans l'affaire Kadi II, la CJUE a jugé, en ce qui concerne l'article 47 de la charte, que les juridictions de l'Union veillent à ce qu'une décision soit prise sur une base factuelle suffisamment solide[221]. La Cour indique qu'«il incombe au juge de l'Union de procéder à cet examen en demandant, le cas échéant, à l'autorité compétente de l'Union de produire des informations ou des éléments de preuve, confidentiels ou non, pertinents aux fins d'un tel examen»[222], alors que «le secret ou la confidentialité de ces informations ou éléments de preuve ne constituent pas une objection valable»[223].

230. Conformément au considérant 181 du projet de décision, la DPRC examine les déterminations effectuées par le CLPO sur la base, au minimum, du dossier d'enquête du CLPO, ainsi que de toute information et observation fournie par le plaignant, l'avocat spécial ou une agence de renseignement. Le projet de décision indique en outre que la DPRC a accès à toutes les informations nécessaires qu'elle peut obtenir par l'intermédiaire du CLPO. Cette possibilité est fondée sur la disposition de l'article 201.9, point b), du règlement AG, qui autorise la DPRC à «demander au CLPO de l'ODNI de compléter

[218] Voir également l'article 201.11, point b), du règlement AG et le considérant 177 du projet de décision.
[219] Voir par exemple l'article 2, paragraphe 3, de la loi allemande sur l'habilitation de sécurité.
[220] Projet de décision, considérant 212.
[221] CJUE, affaires jointes C-584/10 P, C-593/10 P et C-595/10 P, Commission européenne et autres/Yassin Abdullah Kadi, arrêt du 18 juillet 2013 (ci-après l'«arrêt Kadi II de la CJUE»), point 119.
[222] Arrêt Kadi II de la CJUE, point 120.
[223] Arrêt Kadi II de la CJUE, point 125.

le dossier par des informations explicatives ou clarifiantes spécifiques et que CLPO de l'ODNI formule des constatations factuelles supplémentaires lorsque cela est nécessaire pour permettre aux membres de la DPRC de procéder à son examen». L'EDPB croit comprendre que l'évaluation effectuée par la DPRC n'est donc nullement limitée aux conclusions formulées par le CLPO au premier niveau du nouveau mécanisme de recours. Au contraire, la DPRC peut demander à la fois des informations juridiques supplémentaires et, surtout, d'autres circonstances factuelles aux fins de son analyse de l'existence d'une violation visée. Dans le même temps, l'EDPB note également que ces pouvoirs d'enquête généralement très vastes ne s'étendent pas à l'accès direct aux données détenues sur la personne concernée. La Commission a expliqué que le CLPO fera toujours office d'intermédiaire lorsque la DPRC demande des informations complémentaires. Par conséquent, l'accès de la DPRC aux informations nécessaires pour statuer de manière indépendante sur une demande de réexamen repose, dans une certaine mesure, sur la fourniture par le CLPO des informations nécessaires. L'EDPB reconnaît que le CLPO a l'obligation de «fournir tout soutien nécessaire» à la DPRC et les agences de renseignement sont tenues de donner au CLPO l'accès aux informations nécessaires à la réalisation de l'examen par la DPRC[224]. Toutefois, l'EDPB note également que le CLPO lui-même n'est pas indépendant et mène l'enquête initiale sur la base d'une plainte lors de la première étape de la procédure de recours. Par conséquent, l'EDPB se félicite que le PCLOB vérifie, lors de ses examens annuels du mécanisme de recours, si la DPRC a obtenu un accès complet à toutes les informations nécessaires[225]. En outre, l'EDPB invite la Commission à inclure cet aspect dans les examens conjoints, si le projet de décision est adopté, afin d'examiner les implications de ce système dans la pratique.

3.2.4.3.2 Pouvoirs de réparation

231. L'une des principales lacunes du bouclier de protection des données qui a conduit à son invalidation par la CJUE dans l'affaire Schrems II était l'absence de pouvoirs de recours contraignants pour le médiateur. La CJUE a estimé qu'«aucun élément [...] n'indique que ce médiateur ait le pouvoir d'adopter des décisions contraignantes à l'égard de ces services de renseignement»[226]. Le simple engagement (politique) du gouvernement américain selon lequel les services de renseignement corrigeraient toute violation des règles applicables détectée par le médiateur ne suffisait pas à garantir un niveau de protection substantiellement équivalent à celui garanti par l'article 47 de la charte.

232. En revanche, dans le cadre du nouveau mécanisme de recours, les décisions prises par le CLPO et par la DPRC ont un effet contraignant[227]. L'EDPB reconnaît, d'une part, que cette autorité ne se limite pas à des mesures spécifiques, mais autorise une «réparation appropriée» pour «réparer pleinement» une violation couverte identifiée. En particulier, l'article 4, point a), de l'EO 14086 mentionne explicitement la suppression de données collectées illégalement. D'autre part, l'EDPB note que le libellé de l'article 4, point a), de l'EO 14086 crée une certaine incertitude quant au processus de détermination de cette «réparation appropriée». Si une mesure doit être conçue pour réparer pleinement une violation, il convient également d'examiner «la manière dont une violation similaire à celle constatée a été habituellement traitée»[228]. La signification et l'effet de cette exigence ne sont pas clairs. Par conséquent, l'EDPB invite la Commission à suivre de près les mesures de réparation adoptées dans la pratique.

[224] EO 14086, article 3, point c) i) H), et article 3, point d) iii).
[225] EO 14086, article 3, point e) i).
[226] Arrêt Schrems II de la CJUE, point 196.
[227] EO 14086, article 3, point c) ii), et article 3, point d) ii), respectivement.
[228] EO 14086, article 4, point a).

3.2.4.4 Dépôt d'une plainte dans le cadre du nouveau mécanisme de recours

233. Le mécanisme de recours établi au titre de l'EO 14086 ne s'applique qu'aux plaintes recevables transmises par l'autorité publique compétente dans un État éligible concernant des activités de renseignement d'origine électromagnétique des États-Unis pour toute violation couverte[229]. Par conséquent, pour pouvoir se prévaloir de cette protection juridique, plusieurs conditions doivent être remplies.

3.2.4.4.1 Désignation comme État éligible

234. Tout d'abord, le pays ou l'organisation régionale d'intégration économique, à partir duquel les données ont été transférées aux États-Unis, doit avoir été désigné comme État éligible avant le transfert de données à l'origine de la plainte[230]. Il est évidemment essentiel que le mécanisme de recours prévu soit disponible lorsque la décision d'adéquation entre en application. En conséquence, le considérant 196 du projet de décision prévoit que l'entrée en vigueur de la décision est subordonnée, entre autres, à la désignation de l'Union en tant qu'entité éligible aux fins du mécanisme de recours. En fait, la Commission semble supposer que la désignation interviendra avant l'adoption de la décision, étant donné que le projet inclut déjà un espace réservé à la désignation de l'UE par le procureur général[231] (par opposition à l'inclusion de la désignation comme condition préalable dans le dispositif du projet de décision).

3.2.4.4.2 Atteinte aux intérêts relatifs à la vie privée et aux libertés civiles et qualité pour agir

235. Une «plainte recevable» doit être fondée sur une prétendue «violation couverte», ce qui requiert à son tour une violation portant atteinte aux intérêts relatifs à la vie privée et aux libertés civiles du plaignant[232]. L'EDPB comprend, sur la base des explications supplémentaires de la Commission, que le fait de «porter atteinte» n'implique aucune forme de restriction de la recevabilité d'une plainte. Au contraire, comme la Commission l'a indiqué, un tel effet négatif concernerait toute plainte en rapport avec le traitement de données à caractère personnel pour des activités de renseignement d'origine électromagnétique en violation des dispositions visées à l'article 4, point d) iii), par exemple les garanties de l'EO 14086. L'EDPB regrette que cela ne soit pas précisé dans le texte du projet de décision et invite la Commission à préciser davantage la notion d'«effet négatif» afin de garantir que toute violation des droits des personnes concernées est évaluée et corrigée et qu'il n'y a pas de «gravité» à démontrer pour avoir accès à des voies de recours et à une réparation appropriée.

236. Comme indiqué précédemment, une plainte au titre de l'EO 14086 n'exige pas du demandeur qu'il démontre sa qualité pour agir (voir point 215)[233]. L'EDPB se félicite de la clarification apportée à l'article 4, point k), de l'EO 14086, selon laquelle un «test de conviction» sera appliqué et qu'il n'est pas nécessaire de démontrer que les données du plaignant ont effectivement été consultées dans le contexte d'activités de renseignement d'origine électromagnétique. La mise en place du mécanisme de recours est une étape importante, étant donné que l'exigence de qualité pour agir rend très difficile la contestation des mesures de surveillance devant les juridictions ordinaires des États-Unis.

[229] EO 14086, article 3, point a).
[230] EO 14086, articles 4 d) i) et 4 k) i).
[231] Projet de décision, note de bas de page 320.
[232] EO 14086, article 4, point k) i), et article 4, point d) ii).
[233] Clapper c. Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.

237. Sur la base de ce qui précède, l'EDPB n'envisage pas de recourir aux juridictions ordinaires, auxquelles le projet de décision fait également référence[234], pour offrir un niveau de protection adéquat[235]. À cet égard, l'EDPB rappelle les préoccupations qu'il a déjà exprimées à maintes reprises en ce qui concerne l'exigence de qualité pour agir devant les juridictions ordinaires[236]. En outre, sur la base de déclarations supplémentaires du gouvernement américain, l'EDPB croit comprendre que, si l'EO 14086 n'exclut pas le recours aux juridictions de droit commun, il n'est pas possible de savoir comment une telle juridiction appliquerait ce décret. Cette question pourrait être examinée plus avant lors des futurs réexamens, si le projet de décision est adopté.

3.2.4.4.3 La procédure de réclamation

238. L'EDPB approuve en principe la procédure d'acheminement d'une plainte par l'intermédiaire des autorités de contrôle des États membres et continue de penser que l'identification du plaignant devrait avoir lieu sur le territoire de l'UE. Toutefois, comme dans le cadre du mécanisme du médiateur du bouclier de protection des données, le projet de décision prévoit qu'une personne concernée qui souhaite introduire une telle réclamation doit la soumettre à une autorité de contrôle d'un État membre de l'UE compétente pour la surveillance des services de sécurité nationale et/ou le traitement de données à caractère personnel par les autorités publiques[237]. À cet égard, l'EDPB rappelle ses préoccupations déjà exprimées dans l'avis du GT art. 29 sur le bouclier de protection des données, par exemple les difficultés potentielles rencontrées par les particuliers pour identifier l'autorité compétente compte tenu de la diversité des mécanismes de surveillance des services nationaux de sécurité dans les États membres[238]. Compte tenu de la participation des autorités nationales chargées de la protection des données à l'application et au contrôle du CPD UE–États-Unis, il est plus approprié de transmettre les plaintes par l'intermédiaire de celles-ci.

3.2.4.5 La décision de la DPRC

239. À l'issue de l'examen de la demande du plaignant, la DPRC ne doit pas révéler si le plaignant faisait ou non l'objet d'activités de renseignement d'origine électromagnétique aux États-Unis. Au lieu de cela, le plaignant est informé que «l'examen n'a révélé aucune violation couverte ou que la Cour de contrôle de la protection des données a rendu une décision nécessitant une réparation appropriée»[239]. Cette réponse standard sert l'objectif généralement légitime de protéger les informations sensibles sur les activités de renseignement américaines. Toutefois, l'EDPB craint que l'EO 14086 ne prévoie aucune dérogation à la réponse standard de la DPRC.

240. Dans l'affaire Kadi II, la CJUE devait statuer, d'une part, sur les intérêts contradictoires du secret d'État et, d'autre part, sur des procédures équitables et, dans la mesure du possible, contradictoires. La CJUE a jugé que, lorsque des considérations impérieuses touchant à la sécurité nationale s'opposent à la divulgation d'informations ou d'éléments de preuve à la personne concernée, il appartient néanmoins au juge d'appliquer, dans le cadre du contrôle juridictionnel, des techniques qui tiennent compte de considérations légitimes de sécurité quant à la nature et aux sources d'information et à la nécessité de garantir suffisamment le respect des droits procéduraux de l'individu, tels que le droit d'être entendu

[234] Projet de décision, considérant 187 et suivants.
[235] Voir également l'arrêt Schrems II de la CJUE, points 191 et 192.
[236] Voir l'avis 01/2016 du GT art. 29, p. 43.
[237] Projet de décision, considérant 169.
[238] Avis 01/2016 du GT art. 29, points 48 et 49.
[239] EO 14086, article 3, point d) i) H). L'article de l'EO 14086 prévoit cette réponse également pour le CLPO.

et l'exigence d'une procédure contradictoire[240]. La CJUE a en outre précisé qu'il appartient au juge, lorsqu'il procède à l'examen de tous les éléments de fait ou de droit produits par l'autorité compétente de l'Union, de vérifier le bien-fondé des motifs invoqués par cette autorité pour s'opposer à cette divulgation[241]. S'il s'avère que les motifs invoqués par l'autorité compétente de l'Union s'opposent effectivement à la communication à la personne concernée d'informations ou d'éléments de preuve, il reste nécessaire de trouver un juste équilibre entre les exigences liées au droit à une protection juridictionnelle effective et celles découlant de la sécurité nationale[242]. Aux fins d'une telle mise en balance, il est loisible de recourir à des possibilités telles que la communication d'un résumé du contenu des informations ou des éléments de preuve en cause[243]. Bien que les conclusions de la juridiction n'imposent pas d'exigences pour la décision rendue par une juridiction, mais portent plutôt sur la décision de l'autorité compétente et sur le déroulement de la procédure judiciaire, elles fournissent des indications sur la mise en balance des intérêts susmentionnés dans le contexte du droit à une protection juridictionnelle effective. Pour plus de précisions, on peut également se référer à l'affaire Big Brother Watch, dans laquelle la CEDH, faisant allusion à l'équité de la procédure et, en particulier, au principe du contradictoire, a jugé que les décisions d'un organe judiciaire ou d'une autre entité indépendante devaient être motivées[244].

241. L'EDPB reconnaît que les décisions de la DPRC sont effectivement motivées. La DPRC est expressément tenue de rendre une décision écrite exposant ses conclusions et précisant toute réparation appropriée[245]. En outre, l'EDPB note que la personne sera informée si les informations relatives à un examen par la DPRC ont été déclassifiées[246]. L'EDPB reconnaît également le rôle des avocats spéciaux prévus dans le nouveau mécanisme de recours, qui comprend la défense de l'intérêt du plaignant en la matière[247]. Toutefois, à la lumière des implications de la jurisprudence de la CJUE et de la CEDH exposées ci-dessus et compte tenu du fait que la décision de la DPRC ne peut faire l'objet d'un recours mais est définitive[248], l'EDPB s'inquiète de l'application générale de la réponse standard de la DPRC. L'EDPB rappelle que le PCLOB examinera de manière indépendante le fonctionnement du nouveau mécanisme de recours et invite la Commission à accorder une attention particulière à cette question, y compris à toute évaluation de cet aspect par le PCLOB, lors des futurs examens de la décision, si elle est adoptée.

4 MISE EN ŒUVRE ET SUIVI DU PROJET DE DÉCISION

242. En ce qui concerne le suivi et le réexamen du projet de décision, l'EDPB note que, selon la jurisprudence de la CJUE, «au regard du fait que le niveau de protection assuré par un pays tiers est susceptible d'évoluer, il incombe à la Commission, après l'adoption d'une décision au titre de [l'article 45 du RGPD], de vérifier de manière périodique si la constatation relative au niveau de protection adéquat

[240] Arrêt Kadi II de la CJUE, point 125.
[241] Arrêt Kadi II de la CJUE, point 126.
[242] Arrêt Kadi II de la CJUE, point 128.
[243] Arrêt Kadi II de la CJUE, point 129.
[244] CEDH, arrêt Big Brother Watch, point 359.
[245] Article 201.9, point g), du règlement AG.
[246] EO 14086, article 3, point d) v).
[247] Article 201.8, point g), du règlement AG.
[248] Article 201.9, point g), du règlement AG.

assuré par le pays tiers en cause est toujours justifiée en fait et en droit. Une telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard»[249].

243. En outre, l'EDPB note que la lettre du DoC prévoit que ce ministère et d'autres agences américaines, le cas échéant, tiendront des réunions périodiques avec la Commission, les autorités de protection des données de l'UE intéressées et les représentants appropriés de l'EDPB[250].

244. L'EDPB considère que la protection accordée par le droit national en ce qui concerne l'accès des services répressifs, la dérogation pour la collecte temporaire en vrac en vue d'une collecte ciblée par les autorités de sécurité nationale américaines, l'application dans la pratique des principes de nécessité et de proportionnalité nouvellement introduits, notamment dans le contexte du programme UPSTREAM, l'interaction entre l'EO 14086 et les différents instruments juridiques américains permettant aux agences de renseignement américaines de collecter et de poursuivre le traitement des données à caractère personnel, ainsi que les politiques et procédures internes de mise en œuvre, la manière dont ces garanties seront également prises en compte dans le cadre de la surveillance exercée par la FISC, la manière dont le mécanisme de recours fonctionnera effectivement, et la question des transferts ultérieurs, des décisions automatisées, de la surveillance et de l'application substantielles et efficaces des principes du CPD ainsi que des voies de recours effectives, mériteront une attention particulière au cours des prochains examens périodiques.

245. L'EDPB note que l'examen du constat d'adéquation aura lieu un an après la date de notification de la décision d'adéquation aux États membres, puis au moins tous les quatre ans[251]. En vue de renforcer encore le suivi continu de la décision d'adéquation, l'EDPB invite la Commission à procéder aux réexamens ultérieurs au moins tous les trois ans.

246. En ce qui concerne la participation concrète de l'EDPB et de ses représentants à la préparation et au déroulement des futurs examens périodiques, le comité réaffirme que toute documentation pertinente devrait être communiquée par écrit au comité, y compris la correspondance, suffisamment longtemps avant les réexamens périodiques. Comme ce fut le cas pour les examens effectués dans le cadre du bouclier de protection des données, l'EDPB recommande que, au plus tard trois mois avant chaque réexamen, les modalités de ce réexamen soient établies et convenues entre la Commission, l'administration américaine et l'EDPB.

247. En outre, l'EDPB note et salue le fait que le considérant 212 du projet de décision fournit des exemples de modifications compromettant le niveau de protection qui peuvent justifier l'ouverture d'une «procédure d'abrogation d'urgence» axée sur les modifications qui pourraient se produire en ce qui concerne le décret présidentiel n° 14086 et le règlement relatif au procureur général.

Pour l'EDPB

La présidente

(Andrea Jelinek)

[249] Arrêt Schrems I de la CJUE, point 76. Voir également le projet de décision, article 3, paragraphe 4.
[250] Projet de décision, annexe III.
[251] Projet de décision, article 3, paragraphe 4.