DÉCISION D'EXÉCUTION (UE) 2023/1795 DE LA COMMISSION

du 10 juillet 2023

constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis

[notifiée sous le numéro C(2023) 4745]

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([1]), et notamment son article 45, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) Le règlement (UE) 2016/679 ([2]) fixe les règles applicables au transfert de données à caractère personnel, par des responsables du traitement ou des sous-traitants au sein de l'Union, vers des pays tiers et à des organisations internationales, dans la mesure où ces transferts relèvent de son champ d'application. Le chapitre V de ce règlement définit les règles applicables aux transferts internationaux de données. Bien que les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union européenne soient nécessaires au développement du commerce transfrontière et de la coopération internationale, le niveau de protection conféré aux données à caractère personnel au sein de l'Union ne doit pas être compromis par des transferts vers des pays tiers ou des organisations internationales ([3]).

(2) En vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679, la Commission peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers assure(nt) un niveau de protection adéquat. Dans cette circonstance, les transferts de données à caractère personnel vers un pays tiers peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation, comme prévu à l'article 45, paragraphe 1, et au considérant 103 dudit règlement.

(3) Comme précisé à l'article 45, paragraphe 2, du règlement (UE) 2016/679, l'adoption d'une décision d'adéquation doit reposer sur une analyse approfondie de l'ordre juridique du pays tiers, en ce qui concerne tant les règles applicables aux importateurs de données que les limitations et les garanties en matière d'accès des autorités publiques aux données à caractère personnel. Dans son évaluation, la Commission doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est garanti dans l'Union [considérant 104 du règlement (UE) 2016/679]. Cette question doit être évaluée au regard de la législation de l'Union, notamment le règlement (UE) 2016/679, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «Cour de justice») ([4]).

([1]) JO L 119 du 4.5.2016, p. 1.
([2]) Par souci de clarté, une liste des abréviations utilisées dans la présente décision figure à l'annexe VIII.
([3]) Voir considérant 101 du règlement (UE) 2016/679.
([4]) Voir, plus récemment, arrêt de la Cour dans l'affaire C-311/18, Facebook Ireland et Schrems (ci-après l'«arrêt Schrems II»), EU:C:2020:559.

(4) Comme l'a précisé la Cour de justice dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner ([5]) (ci-après l'«arrêt Schrems»), il n'est pas nécessaire de constater un niveau de protection identique. En particulier, les moyens auxquels ce pays tiers a recours aux fins de la protection des données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils s'avèrent, en pratique, effectifs afin d'assurer un niveau de protection adéquat ([6]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de l'Union. Il s'agit plutôt de déterminer si le système étranger offre, dans son ensemble, par l'essence de ses droits en matière de protection des données et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau requis de protection ([7]). En outre, selon cet arrêt, lors de l'application de ce principe, la Commission devrait notamment évaluer si le cadre juridique du pays tiers en question prévoit des règles destinées à limiter les ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale, et offre une protection juridique efficace contre des ingérences de cette nature ([8]). Les critères de référence pour l'adéquation du comité européen de la protection des données, qui ont pour but de préciser davantage ce principe, fournissent également des orientations à cet égard ([9]).

(5) Le principe applicable à de telles ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données a été précisé par la Cour de justice dans son arrêt du 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Limited et Maximillian Schrems (l'«arrêt Schrems II»), qui a invalidé la décision d'exécution (UE) 2016/1250 de la Commission ([10]) relative à un précédent cadre transatlantique de flux de données, le bouclier de protection des données UE - États-Unis. La Cour de justice a considéré que les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de données transférées depuis l'Union vers les États-Unis à des fins de sécurité nationale n'étaient pas encadrées d'une manière à répondre à des exigences essentiellement équivalentes à celles requises, en droit de l'Union, au regard de la nécessité et de la proportionnalité de ces ingérences dans le droit à la protection des données ([11]). La Cour de justice a également estimé qu'il n'existait pas de recours devant un organe qui offre aux personnes dont les données ont été transférées vers les États-Unis des garanties essentiellement équivalentes à celles requises à l'article 47 de la Charte sur le droit à un recours effectif ([12]).

(6) À la suite de l'arrêt Schrems II, la Commission a entamé des pourparlers avec le gouvernement américain en vue d'adopter une éventuelle nouvelle décision d'adéquation qui respecterait les exigences de l'article 45, paragraphe 2, du règlement (UE) 2016/679 telles qu'elles ont été interprétées par la Cour de justice. À la suite de ces discussions, les États-Unis ont adopté, le 7 octobre 2022, le décret présidentiel n° 14086 sur le renforcement des garanties pour les activités de renseignement d'origine électromagnétique menées par les États-Unis (Executive Order 14086, ci-après l'«EO 14086»), qui est complété par un règlement instituant la Cour chargée du contrôle de la protection des données («Data Protection Review Court») publié par le procureur général des États-Unis (ci-après le «règlement AG») ([13]). En outre, le cadre qui s'applique aux entités commerciales traitant des données transférées depuis l'Union en vertu de la présente décision — le «cadre de protection des données UE - États-Unis» (ci-après le «CPD UE - États-Unis» ou le «CPD») — a été mis à jour.

(7) La Commission a soigneusement analysé la législation et les pratiques des États-Unis, y compris l'EO 14086 et le règlement AG. Sur la base des constatations exposées aux considérants 9 à 200, elle conclut que les États-Unis assurent un niveau de protection adéquat des données à caractère personnel transférées, en vertu du CPD UE - États-Unis, par un responsable du traitement ou un sous-traitant de l'Union ([14]) vers des organisations certifiées aux États-Unis.

([5]) Arrêt dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner (ci-après l'«arrêt Schrems»), EU:C:2015:650, point 73.

([6]) Arrêt Schrems, point 74.

([7]) Voir communication de la Commission au Parlement européen et au Conseil intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», COM(2017) 7 du 10.1.2017, section 3.1, p. 6.

([8]) Arrêt Schrems, points 88 et 89.

([9]) Comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rev. 01, disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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).

([11]) Arrêt Schrems II, point 185.

([12]) Arrêt Schrems II, point 197.

([13]) Titre 28 du CFR, partie 302.

([14]) La présente décision présente un intérêt pour l'EEE. L'accord sur l'Espace économique européen (accord EEE) prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La décision du Comité mixte intégrant le règlement (UE) 2016/679 dans l'annexe XI de l'accord EEE a été adoptée par le Comité mixte de l'EEE le 6 juillet 2018 et est entrée en vigueur le 20 juillet 2018. Le règlement est donc couvert par ledit accord. Aux fins de la décision, les références faites à l'Union et aux États membres de l'Union doivent donc être comprises comme incluant également les États de l'EEE.

(8) La présente décision a pour effet de permettre aux transferts de données à caractère personnel par des responsables du traitement et sous-traitants de l'Union ([15]) vers des organisations certifiées aux États-Unis d'avoir lieu sans qu'aucune autorisation doive être obtenue. Elle n'a aucune incidence sur l'application directe du règlement (UE) 2016/679 à ces organisations lorsque les conditions relatives au champ d'application territorial dudit règlement, définies à son article 3, sont remplies.

2. LE CADRE DE PROTECTION DES DONNÉES UE - ÉTATS-UNIS

2.1. Champ d'application personnel et matériel

2.1.1. *Organisations certifiées*

(9) Le CPD UE - États-Unis repose sur un système de certification en vertu duquel les organisations américaines s'engagent à respecter une série de principes de protection de la vie privée — les «principes du cadre de protection de la vie privée UE - États-Unis», y compris les principes complémentaires (conjointement les «principes») — qui sont publiés par le ministère américain du commerce et qui figurent à l'annexe I de la présente décision ([16]). Pour pouvoir prétendre à une certification en vertu du CPD UE - États-Unis, une organisation doit être soumise aux pouvoirs d'enquête et d'exécution de la Federal Trade Commission (FTC) ou du ministère américain des transports ([17]). Les principes s'appliquent dès la certification. Comme expliqué plus en détail aux considérants 48 à 52, les organisations participant au CPD UE - États-Unis sont tenues de recertifier leur adhésion aux principes sur une base annuelle ([18]).

2.1.2. *Définition de «données à caractère personnel» et notions de «responsable du traitement» et de «mandataire»*

(10) La protection offerte par le CPD UE - États-Unis s'applique à toutes les données à caractère personnel transférées de l'Union vers des organisations aux États-Unis qui ont certifié leur adhésion aux principes auprès du ministère du commerce, à l'exception des données collectées à des fins de publication, de diffusion ou d'autres formes de communication publique, ainsi que les informations qui ont été publiées antérieurement, puis archivées ([19]). Ces informations ne peuvent donc pas être transférées sur la base du CPD UE - États-Unis.

(11) Les principes définissent les données à caractère personnel/informations à caractère personnel de la même manière que le règlement (UE) 2016/679, c'est-à-dire comme suit: «toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application [du RGPD], qui est transférée de l'Union européenne vers une organisation américaine et qui est enregistrée sous quelque forme que ce soit» ([20]). En conséquence, elles couvrent également les données de recherche pseudonymisées (ou «codées») (y compris lorsque la clé n'est pas communiquée à l'organisation américaine destinataire) ([21]). De même, la notion de traitement est définie comme suit: «toute activité ou ensemble d'activités effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion, l'effacement ou la destruction» ([22]).

(12) Le CPD UE - États-Unis s'applique aux organisations américaines qui sont considérées comme des responsables du traitement (c'est-à-dire une personne ou une organisation qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel) ([23]) ou des sous-traitants (c'est-à-dire des mandataires agissant pour le compte d'un responsable du traitement) ([24]). Les sous-traitants américains doivent être

([15]) La présente décision n'influe pas sur les exigences du règlement (UE) 2016/679 qui s'appliquent aux entités (responsables du traitement et sous-traitants) de l'Union transférant les données, par exemple en matière de limitation des finalités, de minimisation des données, de transparence et de sécurité des données [voir également article 44 du règlement (UE) 2016/679].

([16]) Voir, à cet égard, arrêt Schrems, point 81, dans lequel la Cour de justice a confirmé qu'un système d'autocertification peut assurer un niveau de protection adéquat.

([17]) Annexe I, section I.2. La FTC a une compétence étendue en ce qui concerne les activités commerciales, à quelques exceptions près, par exemple en ce qui concerne les banques, les compagnies aériennes, les activités d'assurance et de transporteur public des fournisseurs de services de télécommunications (bien que la décision de la Cour d'appel du neuvième circuit des États-Unis du 26 février 2018 dans l'affaire FTC/AT&T ait confirmé que la FTC est compétente pour les activités de transporteur non public de ces entités). Voir également annexe IV, section 2. Le ministère des transports est compétent pour faire respecter les règles par les compagnies aériennes et les agents de billetterie (pour le transport aérien), voir l'annexe V, section A.

([18]) Annexe I, section III.6.

([19]) Annexe I, section III.2.

([20]) Annexe I, section I.8.a.

([21]) Annexe I, section III.14.g.

([22]) Annexe I, section I.8.b.

([23]) Annexe I, section I.8.c.

([24]) Voir, par exemple, l'annexe I, section II.2.b, et les sections II.3.b et 7.d, qui indiquent clairement que les agents agissent pour le compte d'un responsable du traitement, sous réserve des instructions de ce dernier et en vertu d'obligations contractuelles spécifiques.

contractuellement tenus d'agir uniquement sur instruction du responsable européen du traitement et d'aider ce dernier à répondre aux demandes des personnes qui exercent leurs droits en vertu des principes ([25]). En outre, en cas de sous-traitance, un responsable du traitement doit conclure avec le sous-traitant ultérieur un contrat garantissant le même niveau de protection que celui offert par les principes et prendre les mesures nécessaires pour en assurer la bonne mise en œuvre ([26]).

2.2. **Les principes du cadre de protection des données UE - États-Unis**

2.2.1. ***Limitation et choix des finalités***

(13) Les données à caractère personnel devraient être traitées de manière licite et loyale. Elles doivent être collectées dans un but précis et n'être utilisées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

(14) En vertu du CPD UE - États-Unis, cela est assuré par différents principes. Premièrement, en vertu du principe «Intégrité des données et limitation des finalités», de la même manière qu'en vertu de l'article 5, paragraphe 1, point b), du règlement (UE) 2016/679, une organisation ne peut pas traiter des données à caractère personnel d'une manière incompatible avec la finalité pour laquelle elles ont été initialement collectées ou avec une finalité approuvée ultérieurement par la personne concernée ([27]).

(15) Deuxièmement, avant d'utiliser des données à caractère personnel pour une nouvelle finalité (modifiée) sensiblement différente de la finalité initiale, mais qui reste compatible avec celle-ci, ou afin de les communiquer à un tiers, l'organisation doit donner aux personnes concernées la possibilité de s'opposer au traitement (refus), conformément au principe «Choix» ([28]), par un mécanisme clair, visible et d'accès facile. Il est important de noter que ce principe ne se substitue pas à l'interdiction expresse de procéder à des traitements incompatibles ([29]).

([25]) Annexe I, section III.10.a. Voir également les orientations élaborées par le ministère du commerce, en consultation avec le comité européen de la protection des données, dans le cadre du bouclier de protection des données, qui ont précisé les obligations des sous-traitants américains recevant des données à caractère personnel de l'Union au sein du cadre de protection. Étant donné que ces règles n'ont pas changé, ces orientations/FAQ restent pertinentes dans le CPD UE - États-Unis (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Annexe I, section II.3.b.

([27]) Annexe I, section II.5.a. Les finalités compatibles peuvent inclure l'audit, la prévention de la fraude ou d'autres finalités conformes aux attentes d'une personne raisonnable compte tenu du contexte dans lequel s'inscrit la collecte (voir annexe I, note de bas de page n° 6).

([28]) Annexe I, section II.2.a. Cela ne s'applique pas lorsqu'une organisation transfère des données à caractère personnel à un sous-traitant agissant en son nom et selon ses instructions (annexe I, section II.2.b). Cela dit, dans ce cas, l'organisation doit conclure un contrat et veiller au respect du principe «Responsabilité en cas de transfert ultérieur», tel qu'il est décrit plus en détail au considérant 43. En outre, le principe «Choix» (ainsi que le principe «Notification») peut être limité lorsque des données à caractère personnel sont traitées dans le cadre de contrôles préalables (dans le cadre d'une fusion ou d'un rachat potentiel) ou d'audits, dans la mesure et pendant la durée nécessaire pour satisfaire à des dispositions réglementaires ou à des exigences liées à l'intérêt général, ou dans la mesure où et aussi longtemps que l'application de ces principes porterait atteinte aux intérêts légitimes de l'organisme dans le contexte spécifique des enquêtes préalables ou des audits (annexe I, section III.4). Le principe complémentaire n° 15 (annexe I, section III.15.a et b) prévoit également une exception au principe «Choix» (ainsi qu'aux principes «Notification» et «Responsabilité en cas de transfert ultérieur») pour les données à caractère personnel obtenues auprès de sources accessibles au public (à moins que l'exportateur de données de l'Union n'indique que les informations sont soumises à des restrictions qui nécessitent l'application de ces principes) ou les données à caractère personnel collectées dans des registres ouverts à la consultation du public en général (si ces dernières ne sont pas combinées à des informations non publiques et si les conditions de consultation soient respectées). De même, le principe complémentaire n° 14 (annexe I, section III.14.f) prévoit une exception au principe «Choix» (ainsi qu'aux principes «Notification» et «Responsabilité en cas de transfert ultérieur») pour le traitement de données à caractère personnel par une société d'appareils pharmaceutiques ou médicaux dans le cadre d'activités de contrôle de la sécurité et de l'efficacité du produit, dans la mesure où le respect de ces principes entre en conflit avec les exigences réglementaires.

([29]) Cela vaut pour tous les transferts de données effectués en vertu du CPD UE - États-Unis, y compris lorsqu'ils concernent des données recueillies dans le cadre d'une relation de travail. Si une organisation américaine certifiée peut donc, en principe, utiliser des données relatives aux ressources humaines à d'autres fins qu'une relation de travail (par exemple pour certaines communications publicitaires), elle ne peut le faire que dans le respect des principes «Notification» et «Choix» et doit respecter l'interdiction de traitement incompatible. À titre exceptionnel, une organisation peut utiliser des données à caractère personnel à des fins compatibles supplémentaires sans respecter les principes «Notification» et «Choix», mais uniquement dans la mesure nécessaire et pour aussi longtemps que nécessaire, pour éviter de limiter les capacités de l'organisation dans le cadre de promotions, d'engagements ou d'autres décisions similaires relatives à l'emploi [voir annexe I, section III.9.b (iv)]. L'interdiction faite à l'organisation américaine de prendre des sanctions à l'égard du salarié qui a exprimé son choix, notamment d'entraver sa carrière professionnelle, garantira que, malgré la relation de subordination et de dépendance inhérente, ce dernier ne subira aucune pression et pourra opérer son choix en toute liberté. Voir annexe I, section III.9.b.i).

2.2.2. ***Traitement portant sur des catégories particulières de données à caractère personnel***

(16) Des garanties spécifiques devraient être prévues pour le traitement des «catégories particulières» de données.

(17) Conformément au principe «Choix», des garanties spécifiques s'appliquent au traitement des «informations sensibles», par exemple, les données à caractère personnel concernant le dossier médical ou l'état de santé d'une personne, son origine raciale ou ethnique, ses opinions politiques, ses croyances religieuses ou ses convictions philosophiques, son affiliation à un syndicat, sa sexualité ou toute autre information reçue d'un tiers qui est considérée et traitée par ce tiers comme sensible ([30]). Cela signifie que toute donnée considérée comme sensible en vertu du droit de l'Union en matière de protection des données (y compris les données relatives à l'orientation sexuelle, les données génétiques et les données biométriques) sera considérée comme sensible par les organisations certifiées en vertu du CPD UE - États-Unis.

(18) En règle générale, les organisations doivent obtenir l'accord explicite et positif (c'est-à-dire le consentement) des personnes concernées afin d'utiliser des informations sensibles dans un but qui diffère de l'objectif initial de la collecte ou de tout autre objectif approuvé ultérieurement par la personne concernée (exerçant son droit de consentement), ou afin de les divulguer à des tiers ([31]).

(19) Ce consentement ne doit pas être obtenu dans de rares circonstances semblables aux exceptions comparables prévues par le droit de l'Union en matière de protection des données, par exemple lorsque le traitement de données sensibles est dans l'intérêt vital d'une personne; nécessaire à la constatation d'un droit en justice; ou nécessaire pour dispenser des soins médicaux à des fins de diagnostic ([32]).

2.2.3. ***Exactitude, minimisation et sécurité des données***

(20) Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. Elles doivent également être adéquates, pertinentes et limitées au regard des finalités pour lesquelles elles sont traitées. Enfin, elles doivent en principe être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

(21) En vertu du principe «Intégrité des données et limitation des finalités» ([33]), les données à caractère personnel doivent se limiter à ce qui est pertinent aux fins du traitement. En outre, les organisations doivent prendre les mesures qui s'imposent, dans la limite nécessaire aux finalités du traitement, pour assurer la fiabilité des données à caractère personnel par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité.

(22) En outre, des informations à caractère personnel ne peuvent être conservées sous une forme permettant d'identifier une personne ou de la rendre identifiable (donc sous la forme de données à caractère personnel) ([34]) qu'aussi longtemps que leur utilisation est conforme à la ou aux finalités pour lesquelles elles ont été initialement collectées ou qui ont été approuvées ultérieurement par la personne concernée conformément au principe «Choix». Cette obligation n'empêche pas les organisations de continuer à traiter des informations à caractère personnel pendant des périodes plus longues, mais uniquement aussi longtemps que, et dans la mesure où, ce traitement sert raisonnablement l'une des finalités spécifiques suivantes semblables aux exceptions comparables prévues par le droit de l'Union en matière de protection des données: l'archivage dans l'intérêt public, le journalisme, l'art et la littérature, ainsi que la recherche historique et l'analyse statistique ([35]). Lorsque des données à caractère personnel sont conservées pendant une période plus longue à l'une de ces fins, leur traitement sera soumis aux garanties prévues par les principes ([36]).

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

([30]) Annexe I, section II.2.c.
([31]) Annexe I, section II.2.c.
([32]) Annexe I, section III.1.
([33]) Annexe I, section II.5.
([34]) Voir annexe I, note de bas de page n° 7, qui précise qu'une personne est considérée comme «identifiable» dès lors qu'une organisation ou un tiers pourrait raisonnablement l'identifier, compte tenu des moyens d'identification raisonnablement susceptibles d'être utilisés (en tenant compte, entre autres, du coût et du temps nécessaires à l'identification, ainsi que de la technologie disponible au moment du traitement).
([35]) Annexe I, section II.5.b.
([36]) *Ibidem*.

(24) En vertu du CPD UE - États-Unis, cela est garanti par le principe «Sécurité» qui, de manière semblable à l'article 32 du règlement (UE) 2016/679, oblige à prendre des mesures de sécurité raisonnables et adéquates, qui tiennent compte des risques inhérents au traitement et à la nature des données ([37]).

2.2.4. ***Transparence***

(25) Il convient d'informer les personnes concernées des principales caractéristiques du traitement des données à caractère personnel les concernant.

(26) Cela est garanti par le principe «Notification» ([38]) qui, de manière semblable aux exigences en matière de transparence prévues par le règlement (UE) 2016/679, exige des organisations qu'elles informent les personnes concernées, entre autres, i) de la participation de l'organisation au CPD, ii) du type de données collectées, iii) de la finalité du traitement, iv) du type ou de l'identité des tiers auxquels les données à caractère personnel peuvent être divulguées et des finalités de cette divulgation, v) de leurs droits individuels, vi) de la manière de contacter l'organisation et vii) des voies de recours disponibles.

(27) Cette notification doit être communiquée de manière claire et visible aux personnes concernées lorsque celles-ci sont invitées pour la première fois à fournir les informations à caractère personnel ou dès que possible après cette invitation et, en tout état de cause, avant que les données ne soient utilisées dans un but sensiblement différent de celui pour lequel elles ont été initialement collectées (mais compatible avec celui-ci) ou avant qu'elles ne soient diffusées pour la première fois à un tiers ([39]).

(28) En outre, les organisations doivent rendre publiques leurs politiques en matière de protection de la vie privée qui tiennent compte des principes (ou, dans le cas des données relatives aux ressources humaines, les mettre à la disposition des personnes concernées) et fournir des liens dirigeant vers le site web du ministère du commerce (qui donne davantage de détails sur la certification, les droits des personnes concernées et les mécanismes de recours disponibles), vers la liste des organisations participant au cadre de protection des données (liste du CPD) et vers le site web d'un organe approprié de règlement extrajudiciaire des litiges ([40]).

2.2.5. ***Droits individuels***

(29) Les personnes concernées devraient disposer de certains droits qu'elles peuvent opposer au responsable du traitement ou au sous-traitant, en particulier le droit d'accéder aux données, le droit de s'opposer au traitement et le droit d'obtenir la rectification et l'effacement des données.

(30) Le principe «Accès» ([41]) du CPD UE - États-Unis confère aux personnes physiques de tels droits. En particulier, les personnes concernées ont le droit, sans justification, d'obtenir d'une organisation qu'elle leur confirme le traitement de données à caractère personnel les concernant; qu'elle leur communique ces données; et d'obtenir des informations sur la finalité du traitement, les catégories de données à caractère personnel traitées et les (catégories de) destinataires à qui les données sont divulguées ([42]). Les organisations doivent répondre aux demandes d'accès dans un délai raisonnable ([43]). Une organisation peut fixer une limite acceptable au nombre de fois où les demandes d'accès

([37]) Annexe I, section II.4.a. En outre, en ce qui concerne les données relatives aux ressources humaines, le CPD UE - États-Unis exige des employeurs qu'ils tiennent compte des préférences des salariés en ce qui concerne la protection de leur vie privée en restreignant l'accès aux données à caractère personnel, en rendant certaines données anonymes ou en leur attribuant des codes ou des pseudonymes [annexe I, section III.9.b.iii)].

([38]) Annexe I, section II.1.

([39]) Annexe I, section II.1.b. Le principe complémentaire n° 14 (annexe I, section III.14.b et c) prévoit des dispositions spécifiques pour le traitement des données à caractère personnel dans le contexte de la recherche en matière de santé et des essais cliniques. En particulier, ce principe permet aux organisations de traiter les données d'un essai clinique même après qu'une personne s'est retirée de l'essai, si cela a été clairement indiqué dans la notification communiquée lorsque la personne a accepté de participer à l'essai. De même, lorsqu'une organisation participant au CPD UE - États-Unis reçoit des données à caractère personnel à des fins de recherche dans le domaine de la santé, elle ne peut les utiliser que pour une nouvelle activité de recherche, conformément aux principes «Notification» et «Choix». Dans ce cas, la notification à la personne devrait en principe fournir des informations sur toute utilisation spécifique future des données (par exemple, des études associées). Lorsqu'il n'est pas possible d'inclure dès le départ toutes les utilisations futures des données (parce qu'une nouvelle utilisation à des fins de recherche pourrait résulter d'un nouvel examen des données ou d'évolutions médicales/en matière de recherche), il convient d'indiquer que les données peuvent être utilisées pour des activités de recherche médicale et pharmaceutique futures non planifiées à l'avance. Si cette utilisation ultérieure n'est pas compatible avec les finalités générales de recherche pour lesquelles les données ont été collectées (c'est-à-dire si les nouvelles finalités sont sensiblement différentes de la finalité initiale, mais toujours compatibles avec celle-ci, voir considérants 14 et 15), un nouveau consentement doit être obtenu. Voir également les restrictions/exceptions particulières au principe «Notification» décrites à la note de bas de page n° 28.

([40]) Annexe I, section III.6.d.

([41]) Voir également le principe complémentaire «Accès» (annexe I, section III.8).

([42]) Annexe I, section III.8.a.i) et ii).

([43]) Annexe I, section III.8.i.

déposées au cours d'une période donnée seront satisfaites et peut exiger le paiement d'une redevance qui n'est pas excessive, par exemple dans le cas de demandes manifestement excessives ([44]).

(31) Le droit d'accès ne peut être restreint que dans des circonstances exceptionnelles semblables à celles prévues par le droit de l'Union en matière de protection des données, notamment dans les cas susceptibles d'entraîner une violation des droits d'autres personnes; dans les cas où la charge de travail ou la dépense qu'occasionnerait le droit d'accès sont disproportionnées par rapport aux risques pesant sur la vie privée de la personne concernée (bien que les coûts et la charge ne constituent pas des facteurs décisifs lorsqu'il s'agit de déterminer le caractère raisonnable de l'accès); pour autant que la diffusion des données risque de porter atteinte à d'importants intérêts publics, tels que la sécurité nationale, la défense ou la sécurité publique; dans les cas où les informations contiennent des informations commerciales confidentielles; ou lorsque les informations à caractère personnel sont traitées uniquement à des fins statistiques ou de recherche ([45]). Tout refus ou toute restriction du droit d'accès doivent être nécessaires et dûment justifiés et il incombe à l'organisation de prouver que ces conditions sont respectées ([46]). Lors de cette évaluation, l'organisation doit notamment tenir compte des intérêts de la personne concernée ([47]). S'il est possible de séparer les informations d'autres données faisant l'objet d'une restriction, l'organisation doit procéder à la séparation des données protégées et divulguer les informations restantes ([48]).

(32) Les personnes concernées ont également le droit d'obtenir la rectification ou la modification des données inexactes, ainsi que la suppression des données qui ont été traitées en violation des principes ([49]). En outre, comme expliqué au considérant 15, les personnes ont le droit de s'opposer au traitement de leurs données (refus) pour des finalités sensiblement différentes de celles pour lesquelles les données ont été collectées (mais compatibles avec celles-ci) et à la divulgation de leurs données à des tiers. Lorsque les données à caractère personnel sont utilisées à des fins de marketing direct, les personnes concernées disposent d'un droit général de refuser le traitement à tout moment ([50]).

(33) Les principes ne traitent pas spécifiquement de la question des décisions relatives à la personne concernée reposant uniquement sur le traitement automatisé de données à caractère personnel. Cependant, pour ce qui est des données à caractère personnel qui ont été collectées dans l'Union, toute décision fondée sur un traitement automatisé sera généralement prise par le responsable du traitement de l'Union (qui est en relation directe avec la personne concernée) et relève par conséquent directement du règlement (UE) 2016/679 ([51]). Cela inclut les cas de transfert dans lesquels le traitement est effectué par un opérateur économique étranger (américain, par exemple) en tant qu'agent (sous-traitant) agissant au nom du responsable du traitement de l'Union (ou en tant que sous-traitant ultérieur agissant au nom du sous-traitant de l'Union ayant obtenu les données auprès d'un responsable du traitement de l'Union qui les a collectées) qui prend ensuite la décision sur cette base.

(34) Cela a été confirmé par une étude commandée par la Commission en 2018 dans le cadre du deuxième examen annuel du fonctionnement du bouclier de protection des données ([52]), qui a conclu qu'à l'époque, aucune donnée n'indiquait qu'une prise de décision automatisée était normalement effectuée par les organisations participant au bouclier de protection des données sur la base des données à caractère personnel transférées dans le cadre de ce bouclier.

([44]) Annexe I, section III.8.f.i) et ii) et section III.8.g.

([45]) Annexe I, section III.4; section 8.b, c, e; section 14.e, f; et section 15.d.

([46]) Annexe I, section III.8.e.ii). L'organisation doit informer la personne concernée des motifs du refus/de la limitation et communiquer les coordonnées d'une personne à contacter pour plus d'informations, section III.8.a.iii).

([47]) Annexe I, section III.8.a.ii) et iii).

([48]) Annexe I, section III.8.a.i).

([49]) Annexe I, section II.6 et section III.8.a.i).

([50]) Annexe I, section III.8.12.

([51]) Inversement, il peut exister exceptionnellement un lien direct entre l'organisation américaine et la personne concernée dans l'Union, ce qui découle généralement du fait que cet opérateur cible cette personne dans l'Union en lui offrant des biens ou des services ou en suivant son comportement. Dans un tel scénario, l'organisation américaine elle-même relèvera du règlement (UE) 2016/679 (article 3, paragraphe 2); elle doit donc se conformer directement au droit de l'Union en matière de protection des données.

([52]) SWD(2018) 497 final, section 4.1.5. L'étude s'est concentrée sur i) la mesure dans laquelle les organisations participant au bouclier de protection des données aux États-Unis prennent des décisions concernant les personnes sur la base du traitement automatisé des données à caractère personnel transférées par des entreprises de l'Union dans le cadre du bouclier de protection des données; et ii) les garanties pour les personnes concernées que la loi fédérale américaine prévoit pour ce type de situations et les conditions pour que ces garanties s'appliquent.

(35) En tout état de cause, dans les domaines dans lesquels il est très probable que les entreprises recourent au traitement automatisé de données à caractère personnel pour prendre des décisions concernant les personnes (par exemple, l'octroi de crédits, les offres de prêts immobiliers, les décisions de recrutement, l'emploi, le logement et l'assurance), le droit américain offre des protections spécifiques contre les décisions négatives ([53]). Le droit américain prévoit généralement que les personnes ont le droit d'être informées des raisons exactes de la décision (par exemple, le refus d'un crédit), de contester les informations incomplètes ou inexactes (ainsi que le recours à des facteurs illégaux) et de demander réparation. Dans le domaine du crédit à la consommation, le Fair Credit Reporting Act (FCRA) et l'Equal Credit Opportunity Act (ECOA) contiennent des garanties qui offrent aux consommateurs une forme de droit à l'explication et un droit de contestation de la décision. Ces lois s'appliquent à un grand nombre de domaines, notamment le crédit, l'emploi, le logement et l'assurance. En outre, certaines lois antidiscrimination, telles que le titre VII du Civil Rights Act et le Fair Housing Act, protègent les personnes physiques contre les modèles utilisés dans les prises de décision automatisées qui pourraient donner lieu à une discrimination sur la base de certaines caractéristiques, et leur accordent le droit de contester de telles décisions, y compris les décisions automatisées. En ce qui concerne les informations relatives à la santé, la règle de confidentialité du Health Insurance Portability and Accountability Act (HIPAA) crée certains droits semblables à ceux du règlement (UE) 2016/679 en ce qui concerne l'accès aux renseignements personnels en matière de santé. En outre, les orientations des autorités américaines exigent que les prestataires médicaux reçoivent des informations leur permettant d'informer les personnes des systèmes de prise de décision automatisée utilisés dans le secteur médical ([54]).

(36) Par conséquent, ces règles offrent des protections semblables à celles prévues par le droit de l'Union en matière de protection des données dans le cas improbable où des décisions automatisées seraient prises par l'organisation participant au CPD UE - États-Unis elle-même.

2.2.6. ***Limitations concernant les transferts ultérieurs***

(37) Le niveau de protection conféré aux données à caractère personnel qui sont transférées de l'Union vers des organisations aux États-Unis ne doit pas être compromis par le transfert ultérieur de ces mêmes données vers un destinataire se trouvant aux États-Unis ou dans un pays tiers.

(38) En vertu du principe «Responsabilité en cas de transfert ultérieur» ([55]), des règles particulières s'appliquent aux transferts dits «ultérieurs», c'est-à-dire aux transferts de données à caractère personnel d'une organisation participant au CPD UE - États-Unis à un responsable du traitement ou à un sous-traitant tiers, que ce dernier soit situé aux États-Unis ou dans un pays tiers en dehors des États-Unis (et de l'Union). Tout transfert ultérieur ne peut avoir lieu i) qu'à des fins limitées et spécifiques, ii) que sur la base d'un contrat entre l'organisation participant au CPD UE - États-Unis et le tiers ([56]) [ou d'un dispositif comparable en cas de transfert intragroupe ([57])] et iii) que si ce contrat oblige le tiers à prévoir le même niveau de protection que celui qui est garanti par les principes.

(39) Cette obligation d'offrir le même niveau de protection que celui qui est garanti par les principes, lue en liaison avec le principe «Intégrité des données et limitation des finalités», signifie notamment que le tiers ne peut traiter les informations à caractère personnel qui lui ont été transmises qu'à des fins qui ne sont pas incompatibles avec les finalités pour lesquelles elles ont été collectées ou qui ont été approuvées ultérieurement par la personne concernée (conformément au principe «Choix»).

([53]) Voir, par exemple, l'Equal Credit Opportunity Act (15 U.S.C. § 1691 et suivants), le Fair Credit Reporting Act (15 USC § 1681 et suivants) ou le Fair Housing Act (42 U.S.C. § 3601 et suivants). En outre, les États-Unis ont souscrit aux principes de l'Organisation de coopération et de développement économiques sur l'intelligence artificielle, qui comprennent notamment des principes de transparence, d'explicabilité, de sécurité et de responsabilité.

([54]) Voir, par exemple, les orientations disponibles à l'adresse suivante: 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Voir annexe I, section II.3, et le principe complémentaire «Contrats obligatoires pour les transferts ultérieurs» (annexe I, section III.10).

([56]) À titre d'exception à ce principe général, une organisation peut transférer ultérieurement les données à caractère personnel d'un petit nombre d'employés sans conclure de contrat avec le destinataire pour les besoins opérationnels occasionnels liés à l'emploi, par exemple la réservation d'un vol, d'une chambre d'hôtel ou la couverture d'assurance. Toutefois, dans ce cas également, l'organisation doit respecter les principes «Notification» et «Choix» (voir annexe I, section III.9.e).

([57]) Voir le principe complémentaire «Contrats obligatoires pour les transferts ultérieurs» (annexe I, section III.10.b). Bien que ce principe autorise également des transferts qui reposent sur des instruments non contractuels (programmes de mise en conformité et de contrôle intragroupe, par exemple), le texte indique clairement que ces instruments doivent toujours «garanti[r] la continuité de la protection des informations à caractère personnel conformément aux principes». En outre, étant donné que l'organisation américaine certifiée restera responsable du respect des principes, elle aura tout intérêt à utiliser des instruments réellement efficaces dans la pratique.

(40) Le principe «Responsabilité en cas de transfert ultérieur» devrait également être lu en liaison avec le principe «Notification» et, en cas de transfert ultérieur à un responsable du traitement dans un pays tiers ([58]), avec le principe «Choix», selon lequel les personnes concernées doivent être informées (entre autres) du type/de l'identité de tout destinataire tiers, de la finalité du transfert ultérieur, ainsi que du choix qu'elles ont de s'opposer (refus) à ce transfert ou, en cas de données sensibles, d'y consentir expressément (consentement).

(41) L'obligation d'offrir le même niveau de protection que celui qui est garanti par les principes s'applique à tout tiers intervenant dans le traitement des données ainsi transférées indépendamment de leur localisation (aux États-Unis ou dans un autre pays tiers). Elle s'applique également lorsque le destinataire tiers initial communique à son tour ces données à un autre destinataire tiers, à des fins de sous-traitance par exemple.

(42) En tout état de cause, le contrat avec le destinataire tiers doit prévoir que ce dernier prévient l'organisation participant au CPD UE - États-Unis s'il constate qu'il n'est plus en mesure de respecter cette obligation. Dans ce cas, il y a lieu de mettre fin au traitement ou de prendre d'autres mesures raisonnables et appropriées pour remédier à la situation ([59]).

(43) Des protections supplémentaires sont prévues en cas de transfert ultérieur à un mandataire tiers (c'est-à-dire un sous-traitant). En pareil cas, l'organisation américaine doit s'assurer que le mandataire n'agit que sur ses instructions et prendre des mesures raisonnables et appropriées: i) pour garantir que le mandataire traite effectivement les informations à caractère personnel qui lui sont transférées d'une manière compatible avec les obligations qui incombent à l'organisation en vertu des principes; et ii) pour mettre fin et remédier au traitement non autorisé dès qu'elle en est avertie ([60]). Le ministère du commerce peut demander à l'organisation de fournir une synthèse ou une copie représentative des dispositions relatives à la protection de la vie privée contenues dans son contrat ([61]). Si des problèmes de respect des principes se posent dans la chaîne de (sous-)traitance, l'organisation qui agit en tant que responsable du traitement des données à caractère personnel devra en principe en assumer la responsabilité, conformément au principe «Voies de recours, application et responsabilité», sauf si elle prouve que le fait générateur du dommage ne lui est pas imputable ([62]).

2.2.7. ***Responsabilité***

(44) Selon le principe de responsabilité, les entités traitant des données sont tenues de mettre en place les mesures techniques et organisationnelles appropriées pour s'acquitter effectivement de leurs obligations en matière de protection des données et doivent être en mesure de démontrer le respect de ces obligations, en particulier à l'autorité de contrôle compétente.

(45) Une fois qu'une organisation a pris volontairement la décision de certifier ([63]) son adhésion au CPD UE - États-Unis, elle doit obligatoirement respecter et faire respecter les principes. En vertu du principe «Voies de recours, application et responsabilité» ([64]), les organisations participant au CPD UE - États-Unis doivent mettre en place des mécanismes efficaces pour garantir le respect des principes. Les organisations doivent également prendre des mesures pour vérifier ([65]) que leurs politiques en matière de protection de la vie privée sont conformes aux principes et que ces politiques sont effectivement respectées. Pour ce faire, elles peuvent soit mettre en place un système d'auto-évaluation, qui doit comprendre des procédures internes visant à garantir que les salariés sont formés à la mise en œuvre des politiques en matière de protection de la vie privée et qu'il est procédé à des examens périodiques et objectifs du respect de ces politiques, soit organiser un contrôle extérieur fondé sur la méthode de l'audit, des vérifications aléatoires ou l'utilisation d'outils technologiques.

([58]) Les personnes concernées ne pourront pas s'opposer au transfert lorsque les données à caractère personnel sont transférées à un tiers agissant en tant que mandataire chargé d'effectuer des travaux pour le compte et selon les instructions de l'organisation américaine. Néanmoins, un contrat doit avoir été signé avec le mandataire et il incombera à l'organisation américaine de garantir la protection offerte par les principes en exerçant ses pouvoirs d'instruction.

([59]) La situation est différente selon que le tiers est un responsable du traitement ou un sous-traitant (mandataire). Dans le premier cas de figure, le contrat conclu avec le tiers doit prévoir que ce dernier met fin au traitement ou prend d'autres mesures raisonnables ou appropriées pour remédier à la situation. Dans le deuxième cas de figure, il incombe à l'organisation qui participe au CPD UE - États-Unis — en tant qu'organisation responsable du traitement sur les instructions de laquelle le mandataire agit — de prendre ces mesures. Voir annexe I, section II.3.

([60]) Annexe I, section II.3.b.

([61]) *Ibidem*.

([62]) Annexe I, section II.7.d.

([63]) Voir également le principe complémentaire «Autocertification» (annexe I, section III.6).

([64]) Voir également le principe complémentaire «Résolution des litiges et application des décisions» (annexe I, section III.11).

([65]) Voir également le principe complémentaire «Vérification» (annexe I, section III.7).

(46) En outre, les organisations doivent conserver des archives sur la mise en œuvre de leurs pratiques dans le cadre du CPD UE - États-Unis et remettre celles-ci, sur demande, dans le cadre d'une enquête ou d'une réclamation pour non-conformité, à une instance de recours indépendante ou à une autorité répressive compétente ([66]).

2.3. **Gestion, surveillance et contrôle de l'application des règles**

(47) Le CPD UE - États-Unis sera géré et surveillé par le ministère du commerce. Le cadre prévoit des mécanismes de surveillance et d'application destinés à vérifier et à garantir que les organisations participant au CPD UE - États-Unis respectent les principes et qu'il sera remédié à tout manquement à cet égard. Ces mécanismes sont définis dans les principes (annexe I) et dans les engagements pris par le ministère du commerce (annexe III), la FTC (annexe IV) et le ministère des transports (annexe V).

2.3.1. ***(Re)certification***

(48) Afin d'obtenir la certification du CPD UE - États-Unis (ou renouveler la certification chaque année), les organisations doivent déclarer publiquement qu'elles s'engagent à respecter les principes, divulguer publiquement leurs politiques en matière de protection de la vie privée et mettre pleinement en œuvre ces politiques ([67]). Dans le cadre de leur demande de (re)certification, les organisations doivent transmettre au ministère du commerce les informations suivantes: le nom de l'organisation concernée, une description des finalités pour lesquelles l'organisation traitera les données à caractère personnel, les données à caractère personnel qui seront couvertes par la certification, ainsi que la méthode de vérification choisie, le mécanisme de recours indépendant compétent et l'instance réglementaire compétente pour faire respecter les principes ([68]).

(49) Les organisations peuvent recevoir des données à caractère personnel en vertu du CPD UE - États-Unis dès le moment où le ministère du commerce les inscrit sur la liste du CPD. Afin de garantir la sécurité juridique et d'éviter les «fausses déclarations», les organisations qui sont certifiées pour la première fois ne sont pas autorisées à mentionner publiquement leur adhésion aux principes avant que le ministère du commerce n'ait déterminé que la déclaration de certification de l'organisation est complète et n'ait ajouté l'organisation à la liste du CPD ([69]). Afin de pouvoir continuer à se prévaloir du CPD pour recevoir des données à caractère personnel depuis l'Union, ces organisations doivent recertifier chaque année leur participation au cadre. Lorsqu'une organisation se retire du CPD UE - États-Unis, quelle qu'en soit la raison, elle doit supprimer toute déclaration publique laissant croire qu'elle continue à participer au cadre ([70]).

(50) Comme le montrent les engagements énoncés à l'annexe III, le ministère du commerce vérifiera si les organisations satisfont à toutes les exigences de certification et si elles ont mis en place une politique (publique) de protection de la vie privée contenant les informations requises par le principe «Notification» ([71]). S'appuyant sur l'expérience acquise lors de la procédure de (re)certification dans le cadre du bouclier de protection des données, le ministère du commerce effectuera un certain nombre de contrôles, notamment pour vérifier si les dispositions de protection de la vie privée des organisations incluent un lien dirigeant vers le formulaire d'introduction des réclamations sur le site web du mécanisme de règlement des litiges concerné et, lorsque plusieurs entités et filiales d'une organisation sont incluses dans une déclaration de certification, si les politiques de protection de la vie privée de chacune de ces entités satisfont aux exigences de certification et sont facilement accessibles pour les personnes concernées ([72]). En outre, le cas échéant, le ministère du commerce effectuera des contrôles croisés avec la FTC et le ministère des transports pour vérifier que les organisations sont soumises à la surveillance de l'organisme de surveillance indiqué dans leur déclaration de (re)certification, et travaillera avec les organes de règlement extrajudiciaire des litiges pour vérifier que les organisations se sont inscrites auprès du mécanisme de recours indépendant indiqué dans leur déclaration de (re)certification ([73]).

([66]) Annexe I, section III.7.
([67]) Annexe I, section I.2.
([68]) Annexe I, section III.6.b, et annexe III, voir section intitulée «Vérifier le respect des exigences en matière d'autocertification».
([69]) Annexe I, note de bas de page n° 12.
([70]) Annexe I, section III.6.h.
([71]) Annexe I, section III.6.a et note de bas de page n° 12, et annexe III, voir la section intitulée «Vérifier le respect des exigences en matière d'autocertification».
([72]) Annexe III, section intitulée «Vérifier le respect des exigences en matière d'autocertification».
([73]) De même, le ministère du commerce travaillera avec le tiers qui sera le dépositaire des fonds collectés dans le cadre d'une redevance du panel d'autorités chargées de la protection des données (APD) (voir considérant 73) afin de vérifier que les organisations qui choisissent les APD comme mécanisme de recours indépendant ont payé la redevance pour l'année concernée. Voir annexe III, section intitulée «Vérifier le respect des exigences en matière d'autocertification».

(51) Le ministère du commerce informera les organisations que, pour mener à terme le processus de (re)certification, elles doivent résoudre tous les problèmes constatés au cours de l'examen. Si une organisation ne répond pas dans le délai fixé par le ministère du commerce (par exemple, en ce qui concerne le renouvellement de la certification, le processus devrait être mené à terme dans un délai de 45 jours) ([74]) ou si le processus de certification n'est pas mené à terme, la déclaration sera considérée comme abandonnée. Dans ce cas, toute fausse déclaration concernant la participation au CPD UE - États-Unis ou l'adhésion aux principes peut donner lieu à l'adoption de mesures d'exécution par la FTC ou le ministère des transports ([75]).

(52) Pour que le CPD UE - États-Unis soit valablement appliqué, les parties intéressées, telles que les personnes concernées, les exportateurs de données et les autorités nationales chargées de la protection des données (APD) doivent être en mesure d'identifier les organisations qui adhèrent aux principes. Afin de garantir cette transparence au «point d'entrée», le ministère américain du commerce s'est engagé à tenir et à rendre publique la liste des organisations qui ont certifié leur adhésion aux principes et qui relèvent de la compétence d'au moins une des autorités chargées de l'application du cadre mentionnées aux annexes IV et V de la présente décision ([76]). Le ministère du commerce actualisera la liste en fonction des déclarations de recertification annuelles et chaque fois qu'une organisation se retire ou est radiée du CPD UE - États-Unis. En outre, afin de garantir également la transparence au «point de sortie», le ministère du commerce tiendra et rendra public un registre officiel des organisations qui ont été radiées de la liste en indiquant, dans chaque cas, les raisons de cette radiation ([77]). Enfin, il fournira un lien dirigeant vers la page web de la FTC consacrée au CPD UE - États-Unis, qui énumérera les activités de mise en application de la FTC menées en vertu du cadre ([78]).

2.3.2. ***Contrôle de la conformité***

(53) Le ministère du commerce contrôlera en permanence le respect effectif des principes par les organisations participant au CPD UE - États-Unis au moyen de différents mécanismes ([79]). En particulier, il effectuera des «contrôles ponctuels» auprès d'organisations sélectionnées de manière aléatoire, ainsi que des contrôles ponctuels ad hoc auprès d'organisations spécifiques lorsque des problèmes de conformité potentiels sont constatés (par exemple, signalés au ministère du commerce par des tiers) afin de vérifier si i) le(s) point(s) de contact chargé(s) de traiter les réclamations et les demandes des personnes concernées est (sont) disponible(s) et réactif(s); ii) la politique de protection de la vie privée de l'organisation est facilement accessible, à la fois sur son site web et via un lien sur le site web du ministère du commerce; iii) la politique de protection de la vie privée de l'organisation reste conforme aux exigences en matière de certification et iv) le mécanisme indépendant de résolution des litiges choisi par l'organisation est disponible pour traiter les réclamations ([80]).

(54) S'il est établi de manière crédible qu'une organisation ne respecte pas ses engagements en vertu du CPD UE - États-Unis (notamment si le ministère du commerce reçoit des réclamations ou si l'organisation ne répond pas de manière satisfaisante aux demandes de celui-ci), le ministère du commerce demandera à l'organisation de remplir un questionnaire détaillé ([81]). Une organisation qui ne répond pas de manière satisfaisante et dans les délais au questionnaire sera signalée à l'autorité compétente (la FTC ou le ministère des transports) en vue d'éventuelles mesures répressives ([82]). Dans le cadre de ses activités de contrôle de la conformité au titre du bouclier de protection

([74]) Annexe III, note de bas de page n° 2.
([75]) Voir annexe III, section intitulée «Vérifier le respect des exigences en matière d'autocertification».
([76]) Des informations sur la gestion de la liste du CPD figurent à l'annexe III (voir introduction sous la section intitulée «Gestion et supervision du programme du cadre de protection des données par le ministère du commerce) et à l'annexe I (sections I.3, I.4, III.6.d et III.11.g).
([77]) Annexe III, voir introduction sous la section intitulée «Gestion et supervision du programme du cadre de protection des données par le ministère du commerce».
([78]) Voir annexe III, section intitulée «Adapter le site internet du cadre de protection des données à des publics ciblés».
([79]) Voir annexe III, section intitulée «Réaliser d'office périodiquement des contrôles de conformité et des évaluations du programme du cadre de protection des données».
([80]) Dans le cadre de ses activités de contrôle, le ministère du commerce peut utiliser différents outils, notamment pour vérifier si des liens vers les politiques de protection de la vie privée ne sont pas rompus ou pour suivre activement l'actualité et y trouver des rapports établissant de manière crédible des cas de non-conformité.
([81]) Voir annexe III, section intitulée «Réaliser d'office périodiquement des contrôles de conformité et des évaluations du programme du cadre de protection des données».
([82]) Voir annexe III, section intitulée «Réaliser d'office périodiquement des contrôles de conformité et des évaluations du programme du cadre de protection des données».

des données, le ministère du commerce a régulièrement effectué les contrôles ponctuels mentionnés au considérant 53 et a procédé à un suivi permanent des rapports publics, ce qui lui a permis de détecter, de traiter et de résoudre les problèmes de conformité ([83]). Les organisations qui persistent à ne pas respecter les principes seront radiées de la liste du CPD et devront renvoyer ou supprimer les données à caractère personnel reçues dans le cadre de ce dernier ([84]).

(55) Les organisations qui sont rayées de la liste pour d'autres raisons, telles que le retrait volontaire ou la non-recertification, doivent supprimer ou renvoyer les données, ou peuvent les conserver si elles s'engagent chaque année auprès du ministère du commerce à continuer d'appliquer les principes ou si elles assurent une protection adéquate des données à caractère personnel par un autre moyen autorisé (comme, par exemple, un contrat tenant pleinement compte des obligations inscrites dans les clauses contractuelles types adoptées par la Commission en la matière) ([85]). Dans ce cas, l'organisation doit identifier en son sein un point de contact pour toutes les questions liées au CPD UE - États-Unis.

2.3.3. ***Détecter et réprimer les fausses déclarations de participation***

(56) Le ministère du commerce surveillera toutes les fausses déclarations de participation au CPD UE - États-Unis ou les usages abusifs de la marque de certification, d'office et sur la base des réclamations (reçues par les APD, par exemple) ([86]). En particulier, le ministère du commerce vérifiera en permanence que les organisations qui i) se retirent du CPD UE - États-Unis, ii) ne procèdent pas au renouvellement annuel de leur certification (c'est-à-dire qu'elles ont entamé, mais n'ont pas mené à terme le processus de recertification annuel dans les délais impartis ou n'ont même pas entamé le processus de recertification annuelle), iii) sont radiées de la liste des participants, notamment pour «non-respect persistant», ou iv) ne parviennent pas à mener à bien la certification initiale (c'est-à-dire qu'elles ont entamé, mais n'ont pas mené à terme le processus de certification initiale dans les délais impartis), suppriment de toute politique de protection de la vie privée rendue publique les références au CPD UE - États-Unis donnant à penser que l'organisation participe activement au cadre ([87]). Le ministère du commerce effectuera également des recherches sur l'internet pour relever les références faites au CPD UE - États-Unis dans les politiques de protection de la vie privée adoptées par les organisations, notamment afin de détecter toute fausse déclaration par des organisations qui n'ont jamais participé au CPD UE - États-Unis ([88]).

(57) Si le ministère du commerce constate que les références au CPD UE - États-Unis n'ont pas été supprimées ou sont utilisées de manière abusive, il informe l'organisation de la possibilité de saisir la FTC/le ministère des transports ([89]). Si une organisation ne répond pas de manière satisfaisante, le ministère du commerce le signalera à l'organisme compétent en vue d'éventuelles mesures répressives ([90]). Toute fausse déclaration d'une organisation à l'intention du grand public concernant son adhésion aux principes, sous la forme de déclarations ou de pratiques trompeuses, peut donner lieu à l'adoption de mesures d'exécution par la FTC, le ministère des transports ou toute autre autorité américaine chargée de l'application du CPD. Toute fausse déclaration au ministère du commerce peut donner lieu à des poursuites au titre de la loi sur les fausses déclarations (18 U.S.C. § 1001).

([83]) Lors du deuxième examen annuel du bouclier de protection des données, le ministère du commerce a indiqué qu'il avait effectué des contrôles ponctuels auprès de 100 organisations et envoyé des questionnaires de conformité dans 21 cas (après quoi les problèmes détectés ont été corrigés), voir document de travail des services de la Commission SWD(2018) 497 final, p. 9. De même, le ministère du commerce a indiqué, lors du troisième examen annuel du bouclier de protection des données, qu'il avait détecté trois incidents grâce à son suivi des rapports publics et qu'il avait commencé à effectuer des contrôles ponctuels auprès de 30 entreprises tous les mois, ce qui a donné lieu à un suivi au moyen de questionnaires de conformité dans 28 % des cas (après quoi les problèmes détectés ont été immédiatement corrigés ou, dans trois cas, ont été résolus après l'envoi d'une lettre d'avertissement), voir document de travail des services de la Commission SWD(2019) 495 final, p. 8.

([84]) Annexe I, section III.11.g. Il y a non-respect persistant lorsqu'une organisation refuse de se conformer à une décision définitive prise par un organisme d'autoréglementation du respect de la vie privée, une instance indépendante d'instruction des litiges ou une autorité répressive.

([85]) Annexe I, section III.6.f.

([86]) Annexe III, section intitulée «Détecter et traiter les fausses déclarations de participation».

([87]) *Ibidem*.

([88]) *Ibidem*.

([89]) *Ibidem*.

([90]) Dans le cadre du bouclier de protection des données, le ministère du commerce a indiqué lors du troisième examen annuel du cadre qu'il avait constaté 669 cas de fausses déclarations de participation (entre octobre 2018 et octobre 2019), dont la plupart ont été résolus après la lettre d'avertissement du ministère, 143 cas ayant été transmis à la FTC (voir considérant 62 ci-dessous). Voir document de travail des services de la Commission SWD(2019) 495 final, p. 10.

2.3.4. ***Contrôle de l'application des règles***

(58) Pour garantir un niveau adéquat de protection des données dans la pratique, il convient de mettre en place une autorité de contrôle indépendante chargée de surveiller l'application des règles en matière de protection des données et de les faire respecter.

(59) Les organisations participant au CPD UE - États-Unis doivent être soumises à la compétence des autorités américaines — la FTC et le ministère des transports — qui disposent des pouvoirs d'enquête et du pouvoir coercitif nécessaires pour veiller au respect effectif des principes ([91]).

(60) La FTC est une autorité indépendante composée de cinq commissaires, qui sont nommés par le président avec l'avis et le consentement du Sénat ([92]). Les commissaires sont nommés pour un mandat de sept ans et ne peuvent être révoqués par le président que pour inefficacité, manquement au devoir ou acte illégal. La FTC ne peut compter plus de trois commissaires issus du même parti politique et les commissaires ne peuvent, pendant la durée de leur mandat, exercer une autre activité, une autre profession ou un autre emploi.

(61) La FTC peut enquêter sur le respect des principes, ainsi que sur les déclarations mensongères d'adhésion aux principes ou de participation au CPD UE - États-Unis par des organisations qui ont été supprimées de la liste du CPD ou qui ne se sont jamais certifiées ([93]). La FTC peut exiger la mise en conformité par des injonctions administratives ou des décisions judiciaires fédérales (y compris des «consent orders» obtenus par des transactions) ([94]) pour obtenir des injonctions préliminaires ou permanentes ou d'autres mesures correctives, et elle contrôle systématiquement si ces directives sont respectées ([95]). Lorsque les organisations ne se conforment pas à ces injonctions, la FTC peut requérir des amendes administratives et d'autres sanctions, y compris pour tout préjudice causé par le comportement illégal. Chaque consent order adressé à une organisation participant au CPD UE - États-Unis contiendra des dispositions en matière de notification spontanée ([96]) et les organisations seront tenues de publier toute section du CPD UE - États-Unis se rapportant à un rapport de conformité ou d'évaluation soumis à la FTC. Enfin, la FTC maintiendra une liste en ligne des entreprises visées par des injonctions de la FTC ou des décisions de justice dans des affaires portant sur le CPD UE - États-Unis ([97]).

(62) En ce qui concerne le bouclier de protection des données, la FTC a pris des mesures répressives dans environ 22 cas, à la fois pour des violations des exigences spécifiques du cadre (par exemple, le fait de ne pas confirmer au ministère du commerce que l'organisation a continué à appliquer les protections du bouclier de protection des données après s'être retirée du cadre, le fait de ne pas vérifier, par une auto-évaluation ou un contrôle de conformité externe, que l'organisation s'est conformée au cadre) ([98]) et pour de fausses déclarations de participation au cadre (par exemple, par des organisations qui n'ont pas suivi les étapes nécessaires pour obtenir la certification, ou qui ont laissé leur certification expirer, mais ont déclaré de manière mensongère qu'elles continuaient d'y participer) ([99]). Ces mesures répressives résultent notamment de l'utilisation proactive d'injonctions administratives afin d'obtenir des documents de certains participants au bouclier de protection des données et de vérifier ainsi s'il y a eu des violations substantielles des obligations du bouclier ([100]).

([91]) Une organisation participant au CPD UE - États-Unis doit déclarer publiquement son engagement à respecter les principes, publier ses politiques de respect de la vie privée, qui doivent être conformes aux principes, et appliquer les principes dans leur intégralité. Toute non-conformité peut faire l'objet de mesures d'exécution conformément à l'article 5 du Federal Trade Commission Act, qui interdit les pratiques déloyales ou frauduleuses dans le domaine du commerce (15 U.S.C § 45) et à l'article 49 U.S.C. § 41712, qui interdit aux transporteurs et aux agents de billetterie toute pratique déloyale ou frauduleuse relative au transport aérien ou à la vente de transport aérien.

([92]) 15 U.S.C. § 41.

([93]) Annexe IV.

([94]) D'après les informations qu'elle a fournies, la FTC n'est pas compétente pour mener des inspections sur le terrain dans le domaine de la protection de la vie privée. Elle a néanmoins le pouvoir de contraindre les organisations à produire des documents et à fournir des témoignages (voir article 20 du FTC Act) et peut utiliser le système judiciaire pour faire exécuter ces injonctions en cas de non-conformité.

([95]) Annexe IV, section intitulée «Requérir et surveiller les ordonnances».

([96]) Les injonctions de la FTC ou les décisions de justice peuvent exiger des entreprises qu'elles mettent en œuvre des programmes de protection de la vie privée et qu'elles mettent régulièrement à la disposition de la FTC des rapports de conformité ou des évaluations de ces programmes réalisées par des tiers indépendants.

([97]) Annexe IV, section intitulée «Requérir et surveiller les ordonnances».

([98]) Document de travail des services de la Commission SWD(2019) 495 final, p. 11.

([99]) Voir affaires énumérées sur le site web de la FTC, consultables à l'adresse suivante: https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Voir également document de travail des services de la Commission SWD(2017) 344 final, p. 17; document de travail des services de la Commission SWD(2018) 497 final, p. 12, et document de travail des services de la Commission SWD(2019) 495 final, p. 11.

([100]) Voir par exemple Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

(63) Plus généralement, la FTC a pris, ces dernières années, des mesures coercitives dans un certain nombre de cas concernant le respect des exigences spécifiques en matière de protection des données qui sont également prévues par le CPD UE - États-Unis, par exemple en ce qui concerne les principes de limitation des finalités et de conservation des données ([101]), de minimisation des données ([102]), de sécurité des données ([103]) et d'exactitude des données ([104]).

(64) Le ministère du commerce est seul compétent pour réglementer les pratiques des compagnies aériennes et partage avec la FTC la compétence en ce qui concerne les pratiques, en matière de respect de la vie privée, des agents de billetterie d'avion dans le cadre de la vente de transport aérien. Les agents du ministère du commerce cherchent d'abord à conclure une transaction et, si cela n'est pas possible, peuvent engager une procédure d'exécution impliquant une audition de témoins devant un juge de droit administratif relevant du ministère qui est habilité à rendre des ordonnances de cessation et à infliger des sanctions civiles ([105]). Les juges de droit administratif bénéficient de plusieurs protections en vertu de l'Administrative Procedure Act (loi de procédure administrative, APA) afin de garantir leur indépendance et leur impartialité. Par exemple, ils ne peuvent être révoqués que pour un motif sérieux, sont chargés des affaires à tour de rôle, ne peuvent exercer des fonctions incompatibles avec leurs devoirs et responsabilités de juges de droit administratif, ne sont pas soumis à la supervision de l'équipe d'enquête de l'autorité qui les emploie (dans ce cas, le ministère du commerce) et doivent exercer leur fonction d'arbitrage/d'exécution en toute impartialité ([106]). Le ministère du commerce s'est engagé à contrôler les ordonnances d'exécution et à veiller à ce que les ordonnances résultant des affaires du CPD UE - États-Unis soient consultables sur son site web ([107]).

2.4. **Recours**

(65) En vue d'une protection adéquate et, en particulier, du respect de ses droits individuels, la personne concernée doit disposer de possibilités de recours administratif et juridictionnel effectif.

(66) Par le principe «Voies de recours, application et responsabilité», le CPD UE - États-Unis exige des organisations qu'elles ménagent des voies de recours aux personnes concernées par le non-respect des principes et donc la possibilité, pour les personnes concernées de l'Union, d'introduire une réclamation en cas de non-respect des principes par les organisations participant au CPD UE - États-Unis, ainsi que de voir ces réclamations tranchées et aboutir si nécessaire à une décision prévoyant une réparation effective ([108]). Dans le cadre de leur certification, les organisations doivent satisfaire aux exigences découlant de ce principe, en prévoyant des mécanismes de recours indépendants facilement accessibles et efficaces qui permettent d'examiner et de trancher toute réclamation et tout litige rapidement et sans frais pour les personnes concernées ([109]).

([101]) Voir, par exemple, l'ordonnance de la FTC dans l'affaire Drizzly, LLC, qui impose notamment à la société 1) de détruire toutes les données à caractère personnel qu'elle a collectées et qui ne lui sont pas nécessaires pour fournir des produits ou des services aux consommateurs, 2) de s'abstenir de collecter ou de stocker des informations à caractère personnel, à moins que cela ne soit nécessaire à des fins spécifiques indiquées dans un tableau de conservation.

([102]) Voir, par exemple, l'ordonnance de la FTC dans l'affaire CafePress (24 mars 2022), qui exige notamment de réduire au minimum la quantité de données collectées.

([103]) Voir, par exemple, l'action répressive de la FTC dans les affaires Drizzly, LLC et CafePress, dans lesquelles elle a exigé des entreprises concernées qu'elles mettent en place un programme de sécurité spécifique ou des mesures de sécurité spécifiques. En outre, en ce qui concerne les violations de données, voir également l'ordonnance de la FTC du 27 janvier 2023 dans l'affaire Chegg, le règlement conclu avec Equifax en 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Voir, par exemple, l'affaire de de RealPage, Inc (16 octobre 2018), dans laquelle la FTC a pris des mesures coercitives au titre du FCRA à l'encontre d'une société de sélection de locataires qui a fourni des informations générales sur des personnes à des propriétaires immobiliers et à des sociétés de gestion de biens immobiliers, sur la base d'informations tirées d'historiques de location, d'informations tirées de registres publics (y compris des antécédents en matière pénale et d'expulsion) et d'informations en matière de crédit, qui ont été utilisées comme facteur pour déterminer l'éligibilité au logement. La FTC a constaté que la société n'avait pas pris de mesures raisonnables pour garantir l'exactitude des informations qu'elle avait fournies sur la base de son outil d'autodécision.

([105]) Voir annexe V, section intitulée «Pratiques en matière de mise en application».

([106]) Voir 5 U.S.C. § 3105, 7521(a), 554(d) et 556(b)(3).

([107]) Annexe V, voir section intitulée «Surveillance et délivrance d'ordonnances d'exécution publiques relatives à des violations du CPD UE - États-Unis».

([108]) Annexe I, section II.7.

([109]) Annexe I, section III.11.

(67) Les organisations peuvent opter pour des mécanismes de recours indépendants, soit dans l'Union, soit aux États-Unis. Comme expliqué plus en détail au considérant 73, cela inclut la possibilité de s'engager, sur une base volontaire, à coopérer avec les APD de l'Union européenne. Lorsque les organisations traitent des données relatives aux ressources humaines, cet engagement à coopérer avec les APD de l'Union est obligatoire. D'autres solutions consistent à recourir à un organisme indépendant de règlement extrajudiciaire des litiges ou à des programmes de protection de la vie privée du secteur privé, dont les règles intègrent les principes. Ces derniers doivent inclure des mécanismes d'application efficaces, conformes aux exigences du principe «Voies de recours, application et responsabilité».

(68) Par conséquent, le CPD UE - États-Unis fournit aux personnes concernées un certain nombre de possibilités de faire valoir leurs droits, d'introduire des réclamations en cas de non-respect des principes par des entreprises participant au cadre et de voir leurs réclamations tranchées et aboutir si nécessaire à une décision prévoyant une réparation effective. Les personnes concernées peuvent introduire une réclamation directement auprès d'une organisation, d'un organisme indépendant de règlement des litiges désigné par l'organisation, des APD nationales, du ministère du commerce ou de la FTC. Dans les cas où leurs réclamations n'ont pas été tranchées par l'un de ces mécanismes de recours ou d'application, les personnes ont également le droit de recourir à l'arbitrage contraignant (annexe 1 de l'annexe I de la présente décision). À l'exception du comité d'arbitrage, qui ne peut être saisi qu'après que certaines voies de recours ont été épuisées, les personnes sont libres de recourir à un ou à plusieurs mécanismes de recours de leur choix, voire à l'ensemble de ceux-ci, et ne sont pas obligées d'en choisir un plutôt que l'autre ou de respecter un ordre spécifique.

(69) Premièrement, les personnes concernées de l'Union peuvent introduire une réclamation en cas de non-conformité aux principes en prenant directement contact avec les organisations participant au CPD UE - États-Unis ([110]). Pour faciliter le règlement des litiges, l'organisation doit mettre en place un mécanisme de recours efficace pour traiter ces réclamations. La politique des organisations en matière de protection de la vie privée doit donc fournir aux personnes des informations claires au sujet d'un point de contact, à l'intérieur ou à l'extérieur de l'organisation, qui traitera les réclamations (y compris tout établissement au sein de l'Union qui peut répondre aux questions ou aux réclamations) et au sujet de l'organisme indépendant de règlement des litiges (voir considérant 70). Dès réception d'une réclamation individuelle, qu'elle ait été introduite par l'intéressé lui-même ou via le ministère du commerce à la suite d'une saisine effectuée par une APD, l'organisation doit fournir une réponse à la personne concernée de l'Union dans un délai de 45 jours ([111]). De même, les organisations sont tenues de répondre rapidement aux questions et autres demandes d'information relatives à leur adhésion aux principes qui leur sont adressées par le ministère du commerce ou une APD ([112]) (lorsque l'organisation s'est engagée à coopérer avec l'APD).

(70) Deuxièmement, les personnes peuvent également introduire une réclamation auprès de l'organisme indépendant de règlement des litiges (aux États-Unis ou dans l'Union) désigné par une organisation pour examiner et traiter définitivement les réclamations individuelles (à moins que celles-ci ne soient manifestement non fondées ou abusives) et mettre gratuitement à la disposition des personnes des voies de recours appropriées ([113]). Les sanctions et les actions correctrices imposées par un tel organisme doivent être suffisamment contraignantes pour garantir que les organisations respectent les principes et devraient prévoir une annulation ou une correction des effets de la non-conformité par l'organisation et, selon les circonstances, la cessation du traitement ultérieur des données à caractère personnel en cause et/ou la suppression de ces données, ainsi que la publicité des constats de non-conformité ([114]). Les organismes de règlement des litiges indépendants désignés par une organisation seront tenus de faire figurer sur leurs sites web publics des informations pertinentes relatives au CPD UE - États-Unis et aux services qu'ils fournissent à ce titre ([115]). Ils doivent publier chaque année un rapport annuel fournissant des statistiques agrégées concernant ces services ([116]).

([110]) Annexe I, section III.11.d.i).
([111]) Annexe I, section III.11.d.i).
([112]) Il s'agit de l'autorité responsable du traitement désignée par le panel d'APD établi dans le principe complémentaire sur le «Rôle des autorités chargées de la protection des données» (annexe I, section III.5).
([113]) Annexe I, section III.11.d.
([114]) Annexe I, sections II.7 et III.11.e.
([115]) Annexe I, section III.11.d.ii).
([116]) Le rapport annuel comprend: 1) le nombre total de réclamations relatives au CPD UE - États-Unis reçues au cours de l'année de référence; 2) les différents types de réclamations reçues; 3) des mesures de la qualité du règlement des litiges, telles que la durée de traitement des réclamations; et 4) les résultats des réclamations reçues, notamment le nombre et les différents types d'actions correctrices ou de sanctions imposées.

(71) Dans le cadre de ses procédures de contrôle de la conformité, le ministère du commerce s'assurera que les organisations participant au CPD UE - États-Unis sont effectivement enregistrées auprès des mécanismes de recours indépendants auprès desquels elles affirment être enregistrées ([117]). Tant les organisations que les mécanismes de recours indépendants compétents sont tenus de répondre rapidement aux questions et aux demandes formulées par le ministère du commerce pour les informations qui ont trait au CPD UE - États-Unis. Le ministère du commerce travaillera avec les mécanismes de recours indépendants pour vérifier qu'ils incluent sur leurs sites web des informations concernant les principes et les services qu'ils fournissent en vertu du CPD UE - États-Unis et qu'ils publient des rapports annuels ([118]).

(72) Si l'organisation ne se conforme pas à la décision d'un organisme de règlement des litiges ou d'autoréglementation, celui-ci devra notifier cette non-conformité au ministère du commerce et à la FTC (ou à une autre autorité américaine compétente pour enquêter sur les cas de non-respect par l'organisation), ou à un tribunal compétent ([119]). Si une organisation refuse de se conformer à une décision définitive d'un organisme d'autoréglementation en matière de protection de la vie privée, d'un organisme indépendant de règlement des litiges en matière de protection de la vie privée ou d'un organisme gouvernemental en matière de protection de la vie privée, quel qu'il soit, ou si un tel organisme constate fréquemment qu'une organisation ne respecte pas les principes, cela peut être considéré comme une non-conformité persistante et, en conséquence, le ministère du commerce retira de la liste du CPD l'organisation qui s'est trouvée en situation de non-conformité, après lui avoir donné un préavis de 30 jours et la possibilité de présenter ses observations ([120]) Si une organisation continue à affirmer qu'elle est certifiée au regard du CPD UE - États-Unis après avoir été retirée de la liste, le ministère en référera à la FTC ou à un autre service répressif ([121]).

(73) Troisièmement, les personnes peuvent également introduire leurs réclamations auprès d'une APD nationale dans l'Union, qui peut faire usage de ses pouvoirs d'enquête et de correction en vertu du règlement (UE) 2016/679. Les organisations sont tenues de coopérer à l'enquête menée par une APD à la suite d'une réclamation et au traitement définitif de la réclamation par l'APD lorsqu'il s'agit du traitement de données relatives à des ressources humaines collectées dans le cadre d'une relation de travail ou lorsque l'organisation concernée s'est volontairement soumise à la surveillance des APD ([122]). En particulier, elles doivent répondre aux questions, se conformer aux avis émis par l'APD, y compris en ce qui concerne les mesures correctrices ou compensatoires, et fournir à l'APD la confirmation écrite que ces mesures ont été prises ([123]). En cas de non-respect de l'avis donné par l'APD, cette dernière renvoie ces cas au ministère du commerce (qui peut retirer des organisations de la liste CPD UE - États-Unis) ou, en vue d'éventuelles mesures coercitives, à la FTC ou au ministère des transports (le défaut de coopération avec les APD ou le non-respect des principes peut donner lieu à une action en vertu du droit américain) ([124]).

(74) Pour faciliter la coopération en vue d'un traitement efficace des réclamations, le ministère du commerce et la FTC ont tous deux mis en place un point de contact spécialisé chargé d'assurer la liaison directe avec les APD ([125]). Ces points de contact apportent un soutien dans le cadre des enquêtes des APD portant sur le respect des principes par une organisation.

(75) L'avis des APD ([126]) n'est émis que lorsque l'on a raisonnablement laissé aux deux parties au litige la possibilité de formuler leurs observations et de soumettre les éléments d'appréciation qu'elles souhaitent. Le panel peut donner son avis aussi rapidement que le respect des principes du procès équitable le permet et, en principe, dans un délai de 60 jours à compter de la réception de la réclamation ([127]). Si une organisation ne se conforme pas à l'avis dans un délai de 25 jours à compter de sa notification et ne fournit aucun motif valable pour expliquer son retard, le panel

([117]) Annexe I, section intitulée «Vérifier le respect des exigences en matière d'autocertification».

([118]) Voir annexe III, section intitulée «Faciliter la coopération avec les organismes de règlement extrajudiciaire des litiges qui fournissent des services liés aux principes». Voir également annexe I, section III.11.d.ii) et iii).

([119]) Voir annexe I, section III.11.e.

([120]) Voir annexe I, section III.11.g, en particulier les points ii) et iii).

([121]) Voir annexe III, section intitulée «Détecter et traiter les fausses déclarations de participation».

([122]) Annexe I, section II.7.b.

([123]) Annexe I, section III.5.

([124]) Annexe I, section III.5.c.ii).

([125]) Annexe III (voir section intitulée «Faciliter la coopération avec les APD») et annexe IV (voir sections intitulées «Hiérarchisation et instruction des dossiers soumis» et «Coopération en matière de mise en application avec les APD»).

([126]) Il convient que les APD établissent le règlement intérieur du panel informel des APD, étant donné qu'elles sont compétentes pour organiser leurs travaux et coopérer entre elles.

([127]) Annexe I, section III.5.c.i).

peut notifier son intention soit de soumettre l'affaire à la FTC (ou à une autre autorité répressive américaine compétente), soit de conclure à un manquement grave à l'engagement de coopérer. Dans le premier cas, cela peut conduire à des mesures coercitives fondées sur l'article 5 du FTC Act (ou sur une disposition législative similaire) ([128]). Dans le deuxième cas, le panel en informera le ministère du commerce, qui considérera le refus de l'organisation de se conformer à l'avis du panel d'APD comme une non-conformité persistante, ce qui entraînera le retrait de l'organisation de la liste du CPD.

(76) Si l'APD à laquelle la réclamation a été adressée n'a pris aucune mesure ou a pris des mesures insuffisantes pour traiter la réclamation, le réclamant a la possibilité de contester ces mesures ou cette absence de mesures devant les juridictions nationales de l'État membre de l'Union concerné.

(77) Les personnes peuvent également introduire des réclamations auprès d'APD même lorsque le panel d'APD n'a pas été désigné comme un organisme de règlement des litiges de l'organisation. Dans ces cas, les APD peuvent soumettre ces réclamations au ministère du commerce ou à la FTC. Afin de faciliter et de renforcer la coopération en ce qui concerne les réclamations individuelles et les organisations participant au CPD UE - États-Unis qui se trouvent en situation de non-conformité, le ministère du commerce instituera un point de contact ad hoc, qui fonctionnera comme une interface et apportera un soutien dans le cadre des enquêtes des APD portant sur la conformité d'une organisation aux principes ([129]). De même, la FTC s'est engagée à mettre en place un point de contact ad hoc ([130]).

(78) Quatrièmement, le ministère du commerce s'est engagé à recevoir et examiner les réclamations relatives au non-respect des principes par une organisation et à faire tout ce qui est en son pouvoir pour les traiter définitivement ([131]). À cette fin, il prévoit des procédures spéciales applicables aux APD lorsqu'elles soumettent des réclamations à un point de contact ad hoc, suivent l'évolution de ces réclamations et assurent le suivi avec les organisations, pour faciliter le règlement des litiges ([132]). Afin d'accélérer le traitement des réclamations individuelles, le point de contact est en contact direct avec l'APD concernée en ce qui concerne les problèmes de conformité et, en particulier, tient celle-ci informée de l'état des réclamations dans un délai maximal de 90 jours à compter de la saisine ([133]). Cela permet aux personnes concernées d'introduire des réclamations pour non-conformité d'organisations participant au CPD UE - États-Unis directement auprès de leur APD nationale, ces réclamations étant ensuite transmises au ministère du commerce, qui est l'autorité américaine chargée de gérer le CPD UE - États-Unis.

(79) Si, sur la base de ses vérifications d'office de réclamations ou de toute autre information, le ministère du commerce conclut qu'une organisation ne s'est pas conformée, de manière persistante, aux principes de protection de la vie privée, elle retirera cette organisation de la liste du CPD ([134]). Le refus de se conformer à une décision définitive d'un organisme d'autoréglementation en matière de protection de la vie privée, d'un organisme indépendant de règlement des litiges en matière de protection de la vie privée ou d'un organisme gouvernemental en matière de protection de la vie privée, quel qu'il soit, y compris une APD, sera considéré comme une non-conformité persistante ([135]).

(80) Cinquièmement, une organisation participant au CPD UE - États-Unis doit être soumise à la compétence des autorités américaines, notamment la FTC ([136]), qui dispose des pouvoirs d'enquête et du pouvoir coercitif nécessaires pour veiller au respect effectif des principes. Cette dernière examine en priorité les saisines pour non-conformité aux principes effectuées par les organismes de règlement des litiges indépendants ou les organismes d'autoréglementation, le ministère du commerce et les APD (agissant de leur propre initiative ou sur la base de réclamations), afin de déterminer si l'article 5 du FTC Act a été violé ([137]). La FTC s'est engagée à créer une procédure de saisine uniforme, à désigner un point de contact en son sein pour les saisines effectuées par l'APD et à échanger des informations sur les saisines. En outre, elle peut accepter les réclamations qui lui sont directement adressées par des personnes physiques et ouvrir des enquêtes sur le CPD UE - États-Unis de sa propre initiative, notamment dans le cadre de ses enquêtes générales sur les aspects relatifs à la protection de la vie privée.

([128]) Annexe I, section III.5.c.ii).
([129]) Voir annexe III, section intitulée «Faciliter la coopération avec les APD».
([130]) Voir annexe IV, sections intitulées «Hiérarchisation et instruction des dossiers soumis» et «Coopération en matière de mise en application avec les APD».
([131]) Annexe III, voir par exemple section intitulée «Faciliter la coopération avec les APD».
([132]) Annexe I, section II.7.e, et annexe III, section intitulée «Faciliter la coopération avec les APD».
([133]) *Ibidem*.
([134]) Annexe I, section III.11.g.
([135]) Annexe I, section III.11.g.
([136]) Une organisation participant au CPD UE - États-Unis doit déclarer publiquement son engagement à respecter les principes, publier ses politiques de respect de la vie privée, qui doivent être conformes aux principes, et appliquer les principes dans leur intégralité. La non-conformité peut être sanctionnée en vertu de l'article 5 du FTC Act, qui interdit les actes commerciaux déloyaux ou frauduleux ou les actes déloyaux ou frauduleux affectant le commerce.
([137]) Voir également les engagements similaires pris par le ministère des transports, annexe V.

(81) Sixièmement, en tant que mécanisme de recours «en dernier ressort», au cas où aucune des autres voies de recours disponibles n'aurait permis de traiter de manière définitive et satisfaisante la réclamation de la personne concernée de l'Union, celle-ci peut recourir à un arbitrage contraignant par le «panel du cadre de protection des données UE - États-Unis» (panel du CPD UE - États-Unis) ([138]). Les organisations doivent informer les personnes qu'elles ont la possibilité de faire appel à un arbitrage contraignant et, lorsqu'une personne a notifié à une organisation qu'elle recourait à cette possibilité, l'organisation en question est tenue de donner suite ([139]).

(82) Ce panel du CPD UE - États-Unis est composé d'un groupe d'au moins dix arbitres qui seront désignés par le ministère du commerce et la Commission sur la base de leur indépendance, de leur intégrité, ainsi que de leur expérience de la législation américaine en matière de protection de la vie privée et de la législation de l'Union européenne en matière de protection des données. Pour chaque litige individuel, les parties sélectionnent dans ce groupe un panel constitué d'un, de deux ou de trois ([140]) arbitres.

(83) L'International Centre for Dispute Resolution (ICDR), la division internationale de l'American Arbitration Association (AAA), a été choisi par le ministère du commerce pour administrer les arbitrages. Les procédures devant le panel du CPD UE - États-Unis seront régies par un ensemble de règles d'arbitrage convenues et un code de conduite pour les arbitres désignés. Le site web de l'ICDR-AAA fournit des informations claires et concises sur le mécanisme d'arbitrage et la procédure de demande d'arbitrage.

(84) Les règles d'arbitrage convenues entre le ministère du commerce et la Commission complètent le CPD UE - États-Unis qui contient plusieurs éléments facilitant l'accès des personnes concernées de l'Union à ce mécanisme: i) lorsqu'elle prépare l'introduction d'une demande d'arbitrage auprès du panel, la personne concernée peut être assistée par son APD nationale; ii) l'arbitrage aura lieu aux États-Unis, mais les personnes concernées de l'Union peuvent choisir d'y participer par vidéoconférence ou téléconférence, qui sera mise à leur disposition gratuitement; iii) la langue utilisée dans la procédure d'arbitrage sera en règle générale l'anglais, mais l'interprétation lors de l'audience d'arbitrage et la traduction seront en principe mises gratuitement à disposition de la personne concernée sur demande motivée; iv) enfin, chaque partie doit supporter ses propres honoraires d'avocat si elle est représentée par un avocat devant le panel, mais le ministère du commerce créera un fonds alimenté par les contributions annuelles des organisations participant au CPD UE - États-Unis, qui couvrira les coûts éligibles à la procédure d'arbitrage, dans la limite des plafonds qui seront déterminés par les autorités américaines en concertation avec la Commission ([141]).

(85) Le panel du CPD UE - États-Unis a le pouvoir d'imposer les mesures d'équité personnalisées et non pécuniaires ([142]) qui seront nécessaires pour remédier à la non-conformité aux principes. Au moment de statuer, le panel prendra en considération toute autre mesure correctrice déjà obtenue par d'autres mécanismes du CPD UE - États-Unis, mais les personnes peuvent toujours recourir à l'arbitrage si elles estiment que ces mesures sont insuffisantes. Cela permet aux personnes concernées de l'Union de recourir à la procédure d'arbitrage dans tous les cas où, du fait de l'action ou de l'inaction des organisations participant au CPD UE - États-Unis, des mécanismes de recours indépendants ou des autorités américaines compétentes (la FTC, par exemple), la réclamation de ces personnes n'a pas été traitée de manière définitive et satisfaisante. Il n'est pas possible de recourir à l'arbitrage lorsqu'une APD est habilitée à statuer sur la réclamation en question en ce qui concerne l'organisation participant au CPD UE - États-Unis, c'est-à-dire dans les cas où l'organisation est tenue de coopérer avec les APD et de se conformer à leurs avis en matière de traitement des données relatives à des ressources humaines collectées dans le cadre d'une relation de travail, ou s'est elle-même engagée à le faire. Les personnes peuvent demander l'exécution de la décision d'arbitrage devant les tribunaux américains en vertu du Federal Arbitration Act, ce qui garantit l'accès à une voie de recours dans le cas où une entreprise se trouve en situation de non-conformité.

([138]) Voir annexe I, section intitulée «Modèle d'arbitrage».
([139]) Voir annexe I, sections II.1.a.xi) et II.7.c.
([140]) Le nombre d'arbitres dans chaque panel devra faire l'objet d'un accord entre les parties.
([141]) Annexe I de l'annexe I, section G.6.
([142]) Si les personnes ne peuvent pas réclamer de dommages-intérêts dans le cadre de l'arbitrage, le fait de recourir à l'arbitrage n'empêche pas de réclamer par ailleurs des dommages et intérêts devant les tribunaux américains ordinaires.

(86) Septièmement, si une organisation viole son engagement de respecter les principes et la politique qui a été publiée en matière de protection de la vie privée, il est possible que d'autres voies de recours soient prévues par le droit américain, notamment pour obtenir réparation. Par exemple, les personnes concernées peuvent, sous certaines conditions, former un recours en justice (y compris en réparation) en vertu des lois des États sur la consommation dans les cas de déclarations frauduleuses, d'actes ou de pratiques déloyales ou trompeuses ([143]), et au titre de la responsabilité délictuelle [en particulier les délits d'intrusion dans la vie privée ([144]), d'appropriation du nom ou de l'image ([145]) et de divulgation publique de faits privés ([146])].

(87) Ensemble, les différentes voies de recours décrites ci-dessus garantissent que chaque réclamation concernant le non-respect du CPD UE - États-Unis par des organisations certifiées fera effectivement l'objet d'une décision et de mesures correctives.

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

(88) La Commission a également évalué les limitations et les garanties prévues, y compris les mécanismes de surveillance et de recours individuel prévus par le droit américain en ce qui concerne la collecte et l'utilisation ultérieure par les autorités publiques américaines de données à caractère personnel transférées à des responsables du traitement et des sous-traitants aux États-Unis pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale (ci-après l'«accès des pouvoirs publics») ([147]). Lorsqu'elle a évalué si les conditions dans lesquelles les pouvoirs publics accèdent aux données transférées vers les États-Unis en vertu de la présente décision remplissaient le critère de l'«équivalence substantielle» conformément à l'article 45, paragraphe 1, du règlement (UE) 2016/679, tel qu'il est interprété par la Cour de justice à la lumière de la Charte des droits fondamentaux, la Commission a notamment pris en considération plusieurs critères.

(89) En particulier, toute limitation du droit à la protection des données à caractère personnel doit être prévue par la loi et la base juridique qui permet l'ingérence dans ce droit doit définir elle-même la portée de la limitation de l'exercice du droit concerné ([148]). En outre, pour satisfaire à l'exigence de proportionnalité selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire dans une société démocratique pour répondre à des objectifs spécifiques d'intérêt général équivalents à ceux reconnus par l'Union, cette base juridique doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ([149]). En outre, ces règles et garanties doivent être juridiquement

([143]) Voir par exemple les lois de protection des consommateurs de l'État de Californie [Cal. Civ. Code, §§ 1750-1785 (West) Consumer Legal Remedies Act]; du District of Columbia (D.C. Code §§ 28-3901); de Floride (Fla. Stat. §§ 501.201-501.213, Deceptive and Unfair Trade Practices Act); de l'Illinois (815 Ill. Comp. Stat. 505/1-505/12, Consumer Fraud and Deceptive Business Practices Act); de Pennsylvanie [73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law].

([144]) C'est-à-dire en cas d'ingérence intentionnelle dans les affaires privées ou les préoccupations d'une personne, d'une manière qui serait très offensante pour une personne raisonnable [Restatement (2nd) of Torts, § 652(b)].

([145]) Ce délit s'applique généralement en cas d'appropriation et d'utilisation du nom ou de l'image d'une personne pour faire la publicité d'une entreprise ou d'un produit, ou dans un but commercial similaire [voir Restatement (2nd) of Torts, § 652C].

([146]) C'est-à-dire lorsque des informations concernant la vie privée d'une personne sont rendues publiques, lorsque cela est très offensant pour une personne raisonnable et que ces informations ne constituent pas une préoccupation légitime pour le public [Restatement (2nd) of Torts, §652D].

([147]) Cela est également pertinent à la lumière de la section I.5 de l'annexe I. Conformément à cette section et à l'instar du RGPD, le respect des exigences en matière de protection des données et des droits associés aux principes de protection de la vie privée peut faire l'objet de limitations. Toutefois, ces limitations ne sont pas absolues, et ne peuvent être invoquées qu'à plusieurs conditions, par exemple dans la mesure nécessaire pour se conformer à une décision de justice ou satisfaire à des exigences d'intérêt public, d'application de la loi ou de sécurité nationale. Dans ce contexte et dans un souci de clarté, cette section fait également référence aux conditions énoncées dans l'EO 14086 qui sont évaluées notamment aux considérants 127 à 141.

([148]) Voir arrêt Schrems II, points 174 et 175, et jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, arrêt dans l'affaire C-623/17, Privacy International, EU:C:2020:790, point 65; et affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., ECLI:EU:C:2020:791, point 175.

([149]) Voir arrêt Schrems II, points 176 et 181, et jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, arrêt Privacy International, point 68; et arrêt La Quadrature du Net e.a., point 132.

contraignantes et opposables par les personnes concernées ([150]). En particulier, 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 ([151]).

3.1. **Accès aux données et utilisation de celles-ci par les autorités publiques des États-Unis à des fins répressives**

(90) En ce qui concerne les ingérences dans les données à caractère personnel transférées au titre du CPD UE - États-Unis aux fins de garantir l'application de la loi, le droit des États-Unis impose un certain nombre de limitations à l'accès aux données à caractère personnel et à l'utilisation de celles-ci et prévoit des mécanismes de surveillance et de recours qui sont conformes aux exigences visées au considérant 89 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes. À cet égard, le gouvernement américain (par l'intermédiaire du ministère de la justice) a également donné des garanties concernant les limitations et les protections en vigueur (annexe VI de la présente décision).

3.1.1. ***Bases juridiques, limitations et garanties***

3.1.1.1. *Limitations et garanties concernant la collecte de données à caractère personnel à des fins répressives*

(91) Les données à caractère personnel traitées par des organisations américaines certifiées qui seraient transférées depuis l'Union sur la base du CPD UE - États-Unis peuvent être consultées à des fins répressives par les procureurs fédéraux et les enquêteurs fédéraux des États-Unis selon des procédures différentes, comme expliqué en détail aux considérants 92 à 99. Ces procédures s'appliquent de la même manière lorsque des informations sont obtenues auprès de toute organisation américaine, indépendamment de la nationalité ou du lieu de résidence des personnes concernées ([152]).

(92) Premièrement, à la demande d'un agent fédéral chargé de l'application de la loi ou d'un procureur public, un juge peut délivrer un mandat de perquisition ou de saisie (y compris d'informations stockées par voie électronique) ([153]). Un tel mandat ne peut être délivré que s'il existe une «présomption sérieuse» ([154]) que des «objets saisissables» (preuves d'un délit, objets détenus illégalement ou biens conçus ou destinés à être utilisés ou utilisés pour commettre un délit) sont susceptibles d'être trouvés à l'endroit spécifié par le mandat. Le mandat doit indiquer le bien ou l'objet à saisir et désigner le juge auquel le mandat doit être renvoyé. Une personne faisant l'objet d'une

([150]) Voir arrêt Schrems II, points 181 et 182.

([151]) Voir arrêts Schrems I, point 95, et Schrems II, point 194. À cet égard, la CJUE a notamment souligné que le respect de l'article 47 de la Charte des droits fondamentaux, qui garantit le droit à un recours effectif devant un tribunal indépendant et impartial, «participe également du niveau de protection requis au sein de l'Union [et] dont la Commission doit constater le respect avant que celle-ci adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du [règlement (UE) 2016/679]» (arrêt Schrems II, point 186).

([152]) Voir annexe VI. Voir par exemple, en ce qui concerne le Wiretap Act, le Stored Communications Act et le Pen Register Act (mentionnés plus en détail aux considérants 95 à 98), Suzlon Energy Ltd/Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011).

([153]) Code fédéral de procédure pénale, 41. Dans un arrêt de 2018, la Cour suprême a confirmé qu'un mandat de perquisition ou une dérogation à l'exigence de mandat est également requis 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/États-Unis d'Amérique, n° 16 à 402, 585 U.S. (2018)]. Par conséquent, ces données ne peuvent généralement pas être obtenues auprès d'une société de téléphonie cellulaire sur la base d'une ordonnance judiciaire fondée sur des motifs raisonnables de considérer que les informations sont pertinentes et nécessaires pour une enquête pénale en cours, mais nécessitent de démontrer l'existence d'une présomption sérieuse lorsqu'un mandat est utilisé.

([154]) Selon la Cour suprême, la «présomption sérieuse» est une norme «pratique et non technique» qui fait appel aux «considérations factuelles et pratiques de la vie quotidienne sur lesquelles les hommes raisonnables et prudents […] agissent» [Illinois/Gates, 462 U.S. 213, 232 (1983)]. En ce qui concerne les mandats de perquisition, la présomption sérieuse existe lorsqu'il y a une forte probabilité qu'une perquisition aboutisse à la découverte de preuves d'un délit (id).

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 ([155]). Lorsqu'un détenteur de données (par exemple une entreprise) est tenu de divulguer des données en vertu d'un mandat, il peut notamment contester l'obligation de divulgation au motif qu'elle est indûment contraignante ([156]).

(93) Deuxièmement, une citation à comparaître peut être délivrée par un grand jury (organe d'enquête du tribunal constitué par un juge ou un magistrat) dans le cadre d'enquêtes sur certains délits graves ([157]), généralement à la demande d'un procureur fédéral, afin d'obliger une personne à produire ou à mettre à disposition des documents commerciaux, des informations stockées par voie électronique ou d'autres éléments tangibles. En outre, différents actes législatifs fédéraux autorisent l'utilisation d'injonctions administratives pour obtenir la production ou la mise à disposition de documents professionnels, d'informations électroniques ou d'autres éléments tangibles dans des enquêtes sur des fraudes à l'assurance maladie, des abus d'enfants, la protection des services secrets, des abus de substances illégales et des enquêtes de l'inspecteur général ([158]). Dans les deux cas, les informations doivent être pertinentes pour l'enquête et l'injonction ne peut présenter un caractère déraisonnable, c'est-à-dire être excessive, abusive ou accablante (et peut être contestée par le destinataire de l'assignation pour ces motifs) ([159]).

(94) Des conditions très similaires s'appliquent aux injonctions administratives émises pour demander l'accès à des données détenues par des entreprises aux États-Unis à des fins civiles ou réglementaires («intérêt public»). Le pouvoir des agences investies de responsabilités civiles et réglementaires d'émettre de telles injonctions administratives doit être établi par la loi. L'utilisation d'une injonction administrative est soumise à un «critère du caractère raisonnable», qui exige que l'enquête soit menée conformément à un objectif légitime, que les informations demandées dans le cadre de l'injonction soient pertinentes à cette fin, que l'agence ne dispose pas déjà des informations qu'elle cherche à obtenir avec l'injonction et que les démarches administratives nécessaires pour émettre l'injonction ont été suivies ([160]). La jurisprudence de la Cour suprême a également clarifié la nécessité de mettre en balance l'importance de l'intérêt public dans les informations demandées et l'importance des intérêts personnels et organisationnels en matière de respect de la vie privée ([161]). Bien que le recours à une injonction administrative ne soit pas soumis à l'autorisation préalable d'une juridiction, il fait l'objet d'un contrôle juridictionnel en cas de contestation par le destinataire pour les motifs susmentionnés, ou si l'agence émettrice cherche à faire exécuter l'injonction devant une juridiction ([162]). Outre ces limitations générales, des exigences spécifiques (plus strictes) peuvent découler de certaines lois ([163]).

([155]) Mapp/Ohio, 367 U.S. 643 (1961).

([156]) Voir In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (estimant que «la procédure régulière exige une audition sur la question de la lourdeur avant d'obliger une compagnie de téléphone à fournir» une assistance pour un mandat de perquisition) et In re Application of United States, 616 F.2d 1122 (9th Cir. 1980).

([157]) Le cinquième amendement de la Constitution des États-Unis exige un acte de mise en accusation par un grand jury pour tout «crime capital ou infamant». Le grand jury est composé de 16 à 23 membres et détermine s'il existe un motif sérieux de croire qu'une infraction grave a été commise. Pour parvenir à cette conclusion, les grands jurys sont investis de pouvoirs d'enquête qui leur permettent d'émettre des citations à comparaître.

([158]) Voir annexe VI.

([159]) Code fédéral de procédure pénale, 17.

([160]) *United States v. Powell*, 379 U.S. 48 (1964).

([161]) *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

([162]) La Cour suprême a précisé qu'en cas de contestation d'une injonction administrative, une juridiction doit considérer si 1) l'enquête sert une finalité autorisée par la loi, 2) le pouvoir d'injonction en cause relève du pouvoir du Congrès, et 3) les documents demandés sont pertinents pour l'enquête. La Cour a également fait observer qu'une demande d'injonction administrative devait être «raisonnable», à savoir qu'elle nécessitait une « description adéquate, mais pas excessive, des documents à fournir pour les besoins de l'enquête en cause», incluant des «précisions» dans la «description du lieu à perquisitionner et des personnes à appréhender ou des biens à saisir».

([163]) Par exemple, le Right to Financial Privacy Act (loi sur le droit à la protection des données personnelles à caractère financier) ne confère à une autorité publique le pouvoir d'obtenir des états financiers détenus par un établissement financier en vertu d'une injonction administrative que 1) s'il existe des raisons de croire que les documents demandés sont pertinents pour une enquête légitime en matière répressive et 2) si une copie de l'injonction ou de la citation à comparaître a été transmise au client, accompagnée d'un avis décrivant de manière raisonnablement précise la nature de l'enquête (12 U.S.C., § 3405). Le Fair Credit Reporting Act, qui interdit aux agences de renseignement sur la consommation de divulguer des informations relatives aux consommateurs en réponse à des demandes d'injonction administrative (et leur permet de donner suite uniquement aux demandes de comparution devant le grand jury ou aux décisions de justice, 15 U.S.C., § 1681 et suivants) constitue un autre exemple. En ce qui concerne l'accès à des donnés de communication, les exigences spécifiques du Stored Communications Act s'appliquent, y compris pour la possibilité de recourir à des injonctions administratives (voir les considérants 96 à 97 pour un aperçu détaillé).

(95) Troisièmement, plusieurs bases juridiques permettent aux autorités répressives d'obtenir l'accès à des données de communication. Un tribunal peut rendre une ordonnance judiciaire autorisant la collecte d'informations génériques de composition de numéro de téléphone, de routage, d'adressage et de signalisation, ne portant pas sur le contenu et en temps réel, sur un numéro de téléphone ou une adresse de courrier électronique (en utilisant un enregistreur graphique ou un dispositif de traçage), s'il constate que l'autorité a certifié que les informations susceptibles d'être obtenues sont en rapport avec une enquête pénale en cours ([164]). L'ordonnance doit notamment préciser l'identité du suspect, si elle est connue; les caractéristiques des communications auxquelles elle s'applique et l'infraction à laquelle se rapportent les informations à collecter. L'utilisation d'un enregistreur graphique ou d'un dispositif de traçage peut être autorisée pour une période maximale de 60 jours, qui ne peut être prolongée que par une nouvelle ordonnance judiciaire.

(96) En outre, l'accès, à des fins répressives, aux informations d'abonnement, données de trafic et contenus de communications enregistrés par des fournisseurs de service internet, des compagnies de téléphone et d'autres fournisseurs de services tiers peut être obtenu sur la base du Stored Communications Act ([165]). Afin d'accéder au contenu enregistré de communications électroniques, les autorités répressives doivent, en principe, obtenir auprès d'un juge un mandat fondé sur un motif sérieux de croire que le compte en question contient des preuves d'une infraction grave ([166]). Pour les informations relatives à l'enregistrement des abonnés, les adresses IP et les données temporelles y afférentes, ainsi que les informations de facturation, les autorités répressives peuvent obtenir une injonction. Pour la plupart des autres informations enregistrées ne portant pas sur le contenu, telles que les intitulés de courriers électroniques sans indication d'objet, les autorités répressives doivent obtenir une ordonnance judiciaire, qui sera délivrée si le juge estime qu'il existe des motifs raisonnables de croire que les informations demandées sont pertinentes et nécessaires pour une enquête pénale en cours.

(97) Les fournisseurs qui reçoivent des demandes au titre du Stored Communications Act peuvent adresser volontairement une notification au client ou à l'abonné au sujet duquel des informations sont demandées, sauf si l'autorité répressive compétente obtient une ordonnance conservatoire interdisant une telle notification ([167]). Il s'agit d'une ordonnance judiciaire exigeant qu'un fournisseur de services de communications électroniques ou de services informatiques à distance à qui un mandat, une assignation ou une ordonnance judiciaire est adressé, ne notifie à aucune autre personne l'existence du mandat, de l'assignation ou de l'ordonnance judiciaire, aussi longtemps que le tribunal le juge approprié. Une ordonnance conservatoire est accordée si un tribunal estime qu'il y a des motifs de considérer que la notification compromettrait gravement une enquête ou retarderait indûment un procès, par exemple parce qu'elle mettrait en danger la vie ou la sécurité physique d'une personne, lui permettrait d'échapper à des poursuites, intimiderait des témoins potentiels, etc. Un mémorandum du procureur général adjoint (qui s'impose à tous les avocats et agents du ministère de la justice) exige des procureurs qu'ils établissent de manière détaillée la nécessité d'une ordonnance conservatoire et qu'ils justifient auprès du tribunal la manière dont les critères prévus pour l'obtention d'une telle ordonnance sont remplis dans le cas d'espèce ([168]). Le mémorandum prévoit également que les demandes d'ordonnances conservatoires ne doivent généralement pas viser à retarder la notification de plus d'un an. Lorsque, dans des circonstances exceptionnelles, des ordonnances de plus longue durée peuvent s'avérer nécessaires, elles ne peuvent être sollicitées qu'avec l'accord écrit d'un superviseur désigné par le procureur général ou l'assistant du procureur général compétent. En outre, lors de la clôture d'une enquête, le procureur doit immédiatement évaluer s'il y a lieu de maintenir les ordonnances conservatoires en vigueur et, si ce n'est pas le cas, mettre fin à l'ordonnance et veiller à ce que le fournisseur de services en soit informé ([169]).

([164]) 18 U.S.C. § 3123.

([165]) 18 U.S.C. § 2701 à 2713.

([166]) 18 U.S.C. §§ 2701(a)-(b)(1)(A). Si l'abonné ou le client concerné est informé (soit à l'avance, soit, dans certains cas, par une notification différée), les informations de contenu conservées pendant plus de 180 jours peuvent également être obtenues sur la base d'une injonction administrative ou d'une citation à comparaître devant un grand jury [18 U.S.C. §§ 2701(b)(1)(B)] ou une ordonnance judiciaire [s'il existe des motifs raisonnables de croire que les informations demandées sont pertinentes et nécessaires pour une enquête pénale en cours (18 U.S.C. §§ 2701(d)]. Toutefois, conformément à un arrêt de la cour d'appel fédérale, les enquêteurs du gouvernement obtiennent généralement des mandats de perquisition auprès de juges afin de collecter le contenu de communications privées ou de données enregistrées auprès d'un fournisseur de services de communication commerciale. United States/Warshak, 631 F.3d 266 (6th Cir. 2010).

([167]) 18 U.S.C. § 2705(b).

([168]) Voir mémorandum publié par le procureur général adjoint Rod Rosenstein le 19 octobre 2017 sur une politique plus restrictive concernant les demandes d'ordonnances conservatoires (ou de non-divulgation), disponible à l'adresse suivante: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Mémorandum publié par le procureur général adjoint Lisa Moncao le 27 mai 2022 sur une politique supplémentaire concernant les demandes d'ordonnances conservatoires en vertu du 18 U.S.C. § 2705(b).

(98) Les autorités répressives peuvent également intercepter en temps réel les communications filaires, orales ou électroniques sur la base d'une ordonnance judiciaire par un juge estimant notamment qu'il existe un motif sérieux de croire que la mise sur écoute ou l'interception électronique permettra d'obtenir des preuves d'une infraction grave au droit fédéral ou des renseignements sur la localisation d'un fugitif cherchant à échapper à des poursuites ([170]).

(99) D'autres protections sont prévues par diverses politiques et lignes directrices du ministère de la justice, par exemple les lignes directrices du procureur général destinées aux activités intérieures du Federal Bureau of Investigation (FBI) (AGG-DOM), qui exigent notamment que le FBI utilise les méthodes d'enquête les moins intrusives possible, en tenant compte de leur impact sur la vie privée et les libertés civiles ([171]).

(100) Selon les observations du gouvernement américain, les protections identiques ou plus élevées décrites plus haut s'appliquent aux enquêtes menées au niveau des États aux fins de garantir le respect de la loi (pour les enquêtes menées en vertu des législations des États) ([172]). En particulier, les dispositions constitutionnelles, ainsi que les lois et la jurisprudence au niveau de l'État réaffirment les protections susmentionnées contre les perquisitions et saisies abusives en exigeant la délivrance d'un mandat de perquisition ([173]). À l'instar des protections accordées au niveau fédéral, les mandats de perquisition ne peuvent être délivrés que sur la base d'une présomption sérieuse et doivent décrire le lieu à perquisitionner et la personne à appréhender ou le bien à saisir ([174]).

([170]) 18 U.S.C. §§ 2510 à 2522.

([171]) Lignes directrices du procureur général destinées aux activités intérieures du Federal Bureau of Investigation (FBI) (septembre 2008), disponibles à l'adresse suivante: http://www.justice.gov/archive/opa/docs/guidelines.pdf. D'autres règles et politiques limitant les activités d'enquête des procureurs fédéraux sont incluses dans le manuel des procureurs des États-Unis (United States Attorneys'Manual, USAM), également disponible en ligne à l'adresse http://www.justice.gov/usam/united-states-attorneys-manual. Pour déroger à ces lignes directrices, il faut obtenir l'accord préalable du directeur du FBI, du directeur adjoint ou du directeur adjoint exécutif désigné par le directeur, sauf si cet accord ne peut être obtenu en raison de l'immédiateté ou de la gravité d'une menace pour la sécurité des personnes ou des biens ou pour la sécurité nationale (auquel cas le directeur ou une autre personne habilitée doit en être informé dès que possible). En cas de non-respect des lignes directrices, le FBI doit en informer le ministère de la justice, qui informe à son tour le procureur général et le procureur général adjoint.

([172]) Annexe VI, note de bas de page n° 2. Voir également, par exemple, Arnold c. City of Cleveland, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) («Dans les domaines des droits individuels et des libertés civiles, la Constitution des États-Unis, lorsqu'elle s'applique aux États, prévoit un seuil sous lequel les décisions des juridictions d'État ne peuvent s'appliquer»); Cooper c. Californie, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) («Notre position, bien entendu, n'affecte pas le pouvoir de l'État d'imposer, s'il le souhaite, des normes plus élevées en matière de perquisitions et de saisies que ne l'exige la Constitution fédérale.»); *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) («Bien que la Constitution de l'Arizona puisse imposer des normes plus strictes en matière de perquisitions et de saisies que celles de la Constitution fédérale, les juridictions de l'Arizona ne peuvent offrir une protection moindre que celle du quatrième amendement.»).

([173]) La majorité des États ont reproduit les protections du quatrième amendement dans leurs constitutions. Voir Alabama Const. art. I, § 5); Alaska Const., art. I, § 14; 1. Arkansas Const. art. II, § 15; California Const. art. I, § 13; Colorado Const. art. II, § 7; Conneticut Const. art. I, § 7; Delaware Const. art. I, § 6; Florida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawai Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusets Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevad Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. D'autres (par exemple, Maryland, Caroline du Nord et Virginie) ont inscrit dans leurs constitutions des termes spécifiques concernant les mandats qui ont été interprétées au niveau juridictionnel comme fournissant des protections similaires ou supérieures à celles du quatrième amendement (voir Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, et jurisprudence liée, p. ex. *Hamel v. State*, 943 A.2d 686, 701 [Md. Ct. Spec. App. 2008; *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) et *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)]). Enfin, l'Arizona et Washington appliquent des dispositions constitutionnelles protégeant la vie privée de manière plus générale (Arizona Const. art. 2, § 8; Washington Const. art. I, § 7), que des juridictions ont interprétées comme fournissant davantage de protections que le quatrième amendement [voir par exemple *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984), *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)].

([174]) Voir, par exemple, l'article 1524,3, point b), du code pénal de Californie; article 3.6-3.13 du règlement de procédure pénale de l'Alabama; article 10.79.035; code révisé de Washington; article 19.2-59 du chapitre 5, Titre 19.2 Procédure pénale, code de Virginie.

3.1.1.2. *Utilisation ultérieure des informations recueillies*

(101) En ce qui concerne l'utilisation ultérieure des données collectées par les autorités répressives fédérales, différentes lois, lignes directrices et normes imposent des garanties spécifiques. À l'exception des instruments spécifiques applicables aux activités du FBI (AGG-DOM et Domestic Investigations and Operations Guide du FBI), les exigences décrites dans la présente section s'appliquent généralement à l'utilisation ultérieure des données par toute autorité fédérale, y compris aux données consultées à des fins civiles ou réglementaires. Il s'agit notamment des exigences découlant des mémos/règlements de l'Office of Management and Budget, du Federal Information Security Management Modernization Act, du E-Government Act and du Federal Records Act.

(102) Conformément à l'autorité conférée par le Clinger-Cohen Act (P.L. 104-106, Division E) et le Computer Security Act de 1987 (P.L. 100-235), l'Office of Management and Budget (OMB) a publié la circulaire A-130 afin d'établir des orientations générales contraignantes qui s'appliquent à toutes les agences fédérales (y compris les autorités répressives) lorsqu'elles traitent des données d'identification ([175]). En particulier, la circulaire demande à toutes les agences fédérales de «limiter la création, la collecte, l'utilisation, le traitement, le stockage, la conservation, la diffusion et la divulgation de données d'identification à ce qui est légalement autorisé, pertinent et raisonnablement considéré comme nécessaire à la bonne exécution des fonctions autorisées de l'agence» ([176]). En outre, dans la mesure du possible, les agences fédérales doivent veiller à ce que les données d'identification soient exactes, pertinentes, disponibles en temps utile et complètes, et réduites au minimum nécessaire à la bonne exécution des fonctions de l'agence. Plus généralement, les agences fédérales doivent mettre en place un programme complet de protection de la vie privée afin de garantir le respect des exigences applicables en la matière, d'élaborer et d'évaluer les politiques de protection de la vie privée et de gérer les risques liés à la protection de la vie privée; mettre en place des procédures pour détecter, documenter et signaler les incidents liés au respect de la vie privée; élaborer des programmes de sensibilisation et de formation à la protection de la vie privée à l'intention des employés et des sous-traitants; et mettre en place des politiques et des procédures pour s'assurer que le personnel est tenu responsable du respect des exigences et des politiques en matière de protection de la vie privée ([177]).

(103) En outre, la loi sur l'administration en ligne (E-Government Act) ([178]) exige que toutes les agences fédérales (y compris les autorités répressives) mettent en place des mesures de protection de la sécurité des informations proportionnées au risque et à l'ampleur du préjudice qui résulterait de tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés; qu'elles disposent d'un responsable de l'information chargé de veiller au respect des exigences en matière de sécurité de l'information et qu'elles procèdent à une évaluation annuelle indépendante (par exemple par un inspecteur général, voir considérant 109) de leur programme et de leurs pratiques en matière de sécurité de l'information ([179]). De même, le Federal Records Act (FRA) ([180]) et les règlements complémentaires ([181]) exigent que les informations détenues par les agences fédérales soient soumises à des mesures de sauvegarde garantissant l'intégrité physique des informations et les protégeant contre tout accès non autorisé.

(104) En vertu des pouvoirs conférés par une loi fédérale, notamment le Federal Information Security Modernisation Act de 2014, l'OMB et le National Institute of Standards and Technology (NIST) ont élaboré des normes qui sont contraignantes pour les agences fédérales (y compris les autorités répressives) et qui précisent les exigences minimales en matière de sécurité de l'information qui doivent être mises en place, notamment les contrôles d'accès, la sensibilisation et la formation, les plans d'urgence, la réponse aux incidents, les outils d'audit et de responsabilité, la garantie de l'intégrité des systèmes et des informations, la réalisation d'évaluations des risques en matière de sécurité et de protection de la vie privée, etc. ([182]). En outre, toutes les agences fédérales (y compris les autorités

([175]) C'est-à-dire «des informations qui peuvent être utilisées pour distinguer ou retracer l'identité d'une personne, seules ou combinées à d'autres informations liées ou pouvant être liées à une personne donnée», voir circulaire A-130 de l'OMB, p. 33 (définition des «informations d'identification»).

([176]) Circulaire A-130 de l'OMB, «Managing Information as a Strategic Resource», Annexe II, «Responsibilities for Managing Personally Identifiable Information», 81 Fed. Reg. 49,689 (28 juillet 2016), p. 17.

([177]) Annexe II, § 5(a) à (h).

([178]) 44 U.S.C. chapitre 36.

([179]) 44 U.S.C. § 3544 à 3545.

([180]) FAC, 44 U.S.C. § 3105.

([181]) 36 C.F.R. § 1228,150 et suivants, § 1228,228, et annexe A.

([182]) Voir, par exemple, circulaire A-130 de l'OMB; NIST SP 800-53, révision 5, «Security and Privacy Controls for Information Systems and Organizations» (10 décembre 2020); et «Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems» du NIST.

répressives) doivent, conformément aux lignes directrices de l'OMB, établir et mettre en œuvre un plan de gestion des violations de données, notamment lorsqu'il s'agit de répondre à de telles violations et d'évaluer les risques de préjudice ([183]).

(105) En ce qui concerne la conservation des données, le FRA ([184]) exige que les agences fédérales américaines (y compris les autorités répressives) établissent des périodes de conservation pour leurs archives (après quoi ces archives doivent être éliminées), qui doivent être approuvées par la National Archives and Record Administration ([185]). La durée de ces périodes de conservation est fixée en fonction de différents facteurs, tels que le type d'enquête, la question de savoir si les éléments de preuve sont toujours pertinents pour l'enquête, etc. En ce qui concerne le FBI, l'AGG-DOM prévoit que celui-ci doit mettre en place un tel plan de conservation des archives et gérer un système permettant de consulter rapidement l'état d'avancement et le fondement des enquêtes.

(106) Enfin, la circulaire A-130 de l'OMB contient également certaines exigences relatives à la diffusion de données d'identification. En principe, la diffusion et la divulgation de données d'identification doivent être limitées à ce qui est légalement autorisé, pertinent et raisonnablement considéré comme nécessaire à la bonne exécution des fonctions d'une agence ([186]). Lorsqu'elles partagent des données d'identification avec d'autres entités publiques, les agences fédérales américaines doivent imposer, le cas échéant, des conditions (notamment la mise en œuvre de contrôles spécifiques en matière de sécurité et de respect de la vie privée) qui régissent le traitement des informations dans le cadre d'accords écrits (notamment des contrats, des accords d'utilisation des données, des accords d'échange d'informations et des protocoles d'accord) ([187]). En ce qui concerne les motifs sur la base desquels les informations peuvent être diffusées, l'AGG-DOM et le Domestic Investigations and Operations Guide du FBI ([188]) prévoient, par exemple, que le FBI peut être soumis à une obligation légale d'agir de la sorte (par exemple en vertu d'un accord international) ou être autorisé à diffuser des informations dans certaines circonstances, par exemple à d'autres agences américaines si la divulgation est compatible avec l'objectif pour lequel les informations ont été collectées et si elle est liée à leurs responsabilités; à des commissions du Congrès; à des agences étrangères si les informations sont liées à leurs responsabilités et si leur diffusion est compatible avec les intérêts des États-Unis, si la diffusion est notamment nécessaire pour protéger la sûreté ou la sécurité des personnes ou des biens, ou pour prévenir une atteinte ou une menace pour la sécurité nationale et offrir une protection contre ces dernières, et si la divulgation est compatible avec la finalité pour laquelle les informations ont été collectées ([189]).

3.1.2. ***Surveillance***

(107) Les activités des autorités répressives fédérales font l'objet d'une surveillance de la part de divers organes ([190]). Comme expliqué aux considérants 92 à 99, dans la plupart des cas, cela inclut une surveillance préalable par le pouvoir judiciaire, qui doit autoriser des mesures de collecte individuelles avant qu'elles puissent être appliquées. En outre, d'autres organismes surveillent les différentes étapes des activités des autorités répressives, y compris la collecte et le traitement de données à caractère personnel. Ensemble, ces organes judiciaires et non judiciaires veillent à ce que les autorités répressives soient soumises à une surveillance indépendante.

([183]) Mémorandum 17-12, «Preparing for and Responding to a Breach of Personally Identifiable Information», disponible à l'adresse https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf et circulaire de l'OMB n° A-130. Par exemple, les procédures de réponse aux violations de données du ministère de la justice, voir https://www.justice.gov/file/4336/download.

([184]) FRA, 44 U.S.C. §§ 3101 et suivants.

([185]) La National Archives and Record Administration est habilitée à évaluer les pratiques de gestion des archives des agences et peut déterminer si la conservation prolongée de certaines archives est justifiée [44 U.S.C. §§ 2904(c), 2906].

([186]) Circulaire A-130 de l'OMB, section 5.f.1.(d).

([187]) Circulaire A-130 de l'OMB, annexe I, § 3(d).

([188]) Voir également le Domestic Investigations and Operations Guide (DIOG) du FBI, section 14.

([189]) AGG-DOM, section VI, B et C; Domestic Investigations and Operations Guide (DIOG) du FBI, section 14.

([190]) Les mécanismes mentionnés dans la présente section s'appliquent également à la collecte et à l'utilisation de données par les autorités fédérales à des fins civiles et réglementaires. Les agences civiles et réglementaires fédérales sont soumises au contrôle de leurs inspecteurs généraux respectifs et au contrôle du Congrès, notamment du Government Accountability Office, l'organe d'audit et d'enquête du Congrès. À moins que l'agence ne dispose d'un responsable de la protection de la vie privée et des libertés civiles désigné - un poste que l'on retrouve généralement au sein d'organismes tels que le ministère de la justice et le ministère de la sécurité intérieure du fait de leurs compétences en matière répressive et de sécurité nationale - ces tâches incombent au haut fonctionnaire de l'organisme chargé de la protection de la vie privée. Toutes les agences fédérales sont légalement tenues de désigner un haut fonctionnaire chargé de la protection de la vie privée, qui a pour tâche de veiller au respect de la législation sur la protection de la vie privée par l'agence et de superviser les questions connexes. Voir, par exemple, OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

(108) Premièrement, des délégués à la protection des libertés civiles ou de la vie privée investis de responsabilités en matière pénale sont en place dans différents services ([191]). Si les pouvoirs spécifiques de ces délégués peuvent varier quelque peu en fonction de leur mandat, ils englobent généralement la surveillance des procédures permettant de veiller à ce que le service concerné/l'agence concernée prenne en compte de façon adéquate les problèmes touchant à la vie privée et aux libertés civiles et ait mis en place des procédures appropriées pour traiter les réclamations émanant de personnes qui estiment que leur vie privée ou les libertés civiles ont été violées. Les chefs de service ou de l'agence doivent veiller à ce que les délégués à la protection des libertés civiles et de la vie privée disposent des documents et des ressources nécessaires à l'accomplissement de leur mandat, se voient accorder l'accès à tous les documents et au personnel nécessaires pour pouvoir s'acquitter de leurs fonctions et soient informés et consultés sur les changements de politique proposés ([192]). Les délégués à la protection des libertés civiles et de la vie privée font régulièrement rapport au Congrès, notamment sur le nombre et la nature des réclamations reçues par le service/l'agence, les informent succinctement du sort réservé à ces réclamations, et les renseignent sur les examens et les enquêtes effectués ainsi que sur l'impact des activités menées par le délégué ([193]).

(109) Deuxièmement, un inspecteur général indépendant contrôle les activités du ministère de la justice, y compris du FBI ([194]). Les inspecteurs généraux sont des entités dont l'indépendance est inscrite dans la loi ([195]) et sont chargés de mener des enquêtes, des audits et des inspections indépendants sur les programmes et activités menés par le ministère. Ils ont accès à l'ensemble des archives, rapports, audits, réexamens, documents, recommandations ou à tout autre matériel pertinent, si nécessaire au moyen d'une ordonnance, et ils peuvent recueillir des témoignages ([196]). Si les inspecteurs généraux formulent des recommandations non contraignantes sur l'adoption de mesures correctives, leurs rapports, notamment sur les mesures de suivi (ou leur absence) ([197]) sont généralement rendus publics et transmis au Congrès qui peut, sur cette base, exercer sa fonction de contrôle (voir considérant 111) ([198]).

([191]) Voir 42 U.S.C. § 2000ee-1. Il s'agit par exemple du ministère de la justice, du ministère de la sécurité intérieure et du FBI. Au sein du ministère de la sécurité intérieure, un responsable de la protection de la vie privée est chargé de préserver et d'améliorer la protection de la vie privée et de promouvoir la transparence au sein du ministère (6 U.S.C. 142, section 222). Tous les systèmes, technologies, formulaires et programmes du ministère de la sécurité intérieure qui collectent des données à caractère personnel ou qui ont une incidence sur la vie privée sont soumis à la surveillance du responsable de la protection de la vie privée, qui a accès à l'ensemble des archives, rapports, audits, réexamens, documents, notes, recommandations et autre matériel dont dispose le ministère, et le cas échéant au moyen d'une ordonnance. Le responsable de la protection de la vie privée doit faire rapport au Congrès tous les ans sur les activités du ministère qui ont trait au respect de la vie privée, notamment les réclamations pour violation de la vie privée.

([192]) 42 U.S.C. § 2000ee-1(d).

([193]) Voir 42 U.S.C. § 2000ee-1.(f)(1) et (2). Par exemple, le rapport du délégué à la protection des libertés civiles et de la vie privée du ministère de la justice et du bureau des libertés civiles et de la vie privée couvrant la période d'octobre 2020 à mars 2021 indique que 389 examens de la protection de la vie privée ont été effectués, notamment des systèmes d'information et d'autres programmes (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) De même, le Homeland Security Act de 2002 a créé un bureau de l'inspecteur général au sein du ministère de la sécurité intérieure.

([195]) Les inspecteurs généraux sont inamovibles; ils ne peuvent être révoqués que par le président qui doit informer par écrit le Congrès des motifs de cette révocation.

([196]) Voir la loi sur l'inspecteur général de 1978 (Inspector General Act), § 6.

([197]) Voir à cet égard, par exemple, la vue d'ensemble préparée par le bureau de l'inspecteur général du ministère de la justice sur ses recommandations et la mesure dans laquelle elles ont été mises en œuvre dans le cadre des actions de suivi du ministère et de l'agence, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Voir la loi sur l'inspecteur général de 1978 (Inspector General Act), §§ 4(5), 5. Par exemple, le bureau de l'inspecteur général du ministère de la justice a récemment publié son rapport semestriel au Congrès (1er octobre 2021-31 mars 2022, https://oig.justice.gov/node/23596), qui donne un aperçu de ses audits, évaluations, inspections, examens spéciaux et enquêtes sur les programmes et activités du ministère de la justice. Ces activités comprenaient une enquête sur un ancien contractant concernant la divulgation illicite d'une surveillance électronique (mise sur écoute d'une personne) dans le cadre d'une enquête en cours, qui a entraîné la condamnation du contractant. Le bureau de l'inspecteur général a également mené une enquête sur les programmes et pratiques de sécurité de l'information des agences du ministère de la justice, qui consiste notamment à tester l'efficacité des politiques, procédures et pratiques de sécurité de l'information d'un sous-ensemble représentatif des systèmes de l'agence.

(110) Troisièmement, dans la mesure où ils mènent des activités de lutte contre le terrorisme, les services investis de responsabilités en matière pénale sont soumis au contrôle du conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, PCLOB), une agence indépendante au sein du pouvoir exécutif composée d'un conseil bipartisan constitué de cinq membres nommés par le président pour un mandat fixe de six ans avec l'approbation du Sénat ([199]). Selon son statut fondateur, le PCLOB est investi de responsabilités dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre, en vue de protéger la vie privée et les libertés civiles. Dans le cadre de son examen, il peut avoir accès à l'ensemble des archives, rapports, audits, analyses, documents, pièces et recommandations pertinents, notamment aux informations classifiées, mener des entretiens et recueillir des témoignages ([200]). Il reçoit des rapports des délégués à la protection des libertés civiles et de la vie privée de plusieurs agences/organes fédéraux ([201]); il peut adresser des recommandations aux autorités gouvernementales et répressives et fait régulièrement rapport aux commissions du Congrès et au président ([202]). Les rapports du PCLOB, y compris ceux destinés au Congrès, doivent être rendus publics dans la mesure la plus large possible ([203]).

(111) Enfin, les activités de répression pénale sont soumises à la surveillance de commissions spécifiques du Congrès américain (les commissions judiciaires de la Chambre des représentants et du Sénat). Les commissions judiciaires exercent une surveillance régulière de différentes manières, notamment au moyen d'auditions, d'enquêtes, d'examens et de rapports ([204]).

3.1.3. ***Recours***

(112) Comme indiqué, les autorités répressives doivent, dans la plupart des cas, obtenir une autorisation judiciaire préalable pour collecter des données à caractère personnel. Bien qu'une telle autorisation ne soit pas nécessaire pour les injonctions administratives, le recours à celles-ci est limité à des cas spécifiques et sera soumis à un contrôle juridictionnel indépendant, tout du moins lorsque le gouvernement cherche à faire exécuter ces injonctions par la voie judiciaire. En particulier, les destinataires des injonctions administratives peuvent contester celles-ci en justice au motif qu'elles ne sont pas raisonnables, c'est-à-dire qu'elles sont excessives, abusives ou accablantes ([205]).

(113) Les personnes peuvent tout d'abord introduire des demandes ou des réclamations auprès des autorités répressives concernant le traitement des données à caractère personnel les concernant. Dans ce contexte, elles ont notamment la possibilité de demander l'accès à des données à caractère personnel et leur rectification ([206]). En ce qui concerne les activités liées à la lutte contre le terrorisme, les personnes peuvent également introduire une réclamation auprès des délégués à la protection des libertés civiles et de la vie privée (ou d'autres agents chargés de la protection de la vie privée) au sein des services répressifs ([207]).

(114) De plus, le droit américain offre aux personnes physiques plusieurs voies de recours contre les autorités publiques, ou un de leurs fonctionnaires, lorsque ces autorités traitent des données à caractère personnel ([208]). Ces voies de recours, parmi lesquelles figurent notamment l'APA, le Freedom of Information Act (loi sur la liberté d'information, FOIA) et l'Electronic Communications Privacy Act (loi sur la confidentialité des communications électroniques, ECPA), sont ouvertes à toutes les personnes, quelle que soit leur nationalité, sous réserve des conditions applicables.

([199]) Les membres du PCLOB doivent être sélectionnés uniquement sur la base de leurs qualifications professionnelles, de leurs réalisations, de leur stature publique, de leur expertise en matière de protection de la vie privée et des libertés civiles et de leur expérience pertinente, sans tenir compte de leur affiliation politique. Le PCLOB ne peut en aucun cas compter plus de trois membres appartenant au même parti politique. Une personne nommée au PCLOB ne peut, pendant son mandat, être un représentant élu, un fonctionnaire ou un employé du gouvernement fédéral, autrement qu'en sa qualité de membre du PCLOB. Voir 42 U.S.C. § 2000ee (h).

([200]) 42 U.S.C. § 2000ee (g).

([201]) Voir 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Ceux-ci englobent au moins le ministère de la justice, le ministère de la défense, le ministère de la sécurité intérieure, ainsi que tout autre service, agence ou entité du pouvoir exécutif désigné par le PCLOB comme adéquats pour les examens considérés.

([202]) 42 U.S.C. § 2000ee (e).

([203]) 42 U.S.C. § 2000ee (f).

([204]) Par exemple, les commissions organisent des auditions thématiques (voir, par exemple, une récente audition de la commission judiciaire de la Chambre des représentants sur les «filets numériques», https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), ainsi que des auditions de contrôle régulières, par exemple du FBI et du ministère de la justice, voir https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 et https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

([205]) Voir annexe VI.

([206]) Circulaire OMB n° A-130, appendice II, section 3, points a) et f), qui impose aux agences fédérales de garantir aux personnes concernées un accès et une rectification appropriés lorsqu'elles en font la demande, et de mettre en place des procédures de réception et de traitement des réclamations et requêtes en matière de protection de la vie privée.

([207]) Voir 42 U.S.C., § 2000ee-1, en ce qui concerne, par exemple, le ministère de la justice et le ministère de la sécurité intérieure. Voir également le mémorandum M-16-24 de l'OMB, Role and Designation of Senior Agency Officials for Privacy.

([208]) Les mécanismes de recours mentionnés dans la présente section s'appliquent également à la collecte et à l'utilisation de données par les autorités fédérales à des fins civiles et réglementaires.

(115) De manière générale, en vertu des dispositions relatives au contrôle juridictionnel de l'APA ([209]), «toute personne subissant un dommage du fait d'une décision d'une agence, ou qui est affectée ou lésée par une telle décision», peut former un recours juridictionnel ([210]). Cela inclut la possibilité de demander au tribunal de «déclarer illégales et d'annuler la décision, les constatations et les conclusions de l'agence jugées […] arbitraires, capricieuses, constitutives d'un abus du pouvoir d'appréciation ou non conformes à la loi pour une autre raison» ([211]).

(116) Plus spécifiquement, le titre II de l'ECPA ([212]) définit un système de droits légaux en matière de protection de la vie privée et régit l'accès des autorités chargées de faire respecter la loi aux contenus des communications téléphoniques, orales ou électroniques stockées par des prestataires de services tiers ([213]). Il rend punissable l'accès illicite (c'est-à-dire non autorisé par les juridictions ou autrement permis) à ces communications et permet aux personnes concernées d'engager une action au civil devant un tribunal fédéral américain pour demander des dommages et intérêts, y compris punitifs, ainsi qu'une réparation en equity ou une décision déclaratoire contre un fonctionnaire de l'État qui a délibérément commis ces actes illicites ou contre les États-Unis.

(117) En outre, plusieurs autres lois garantissent aux personnes le droit d'intenter un procès contre une autorité publique ou un fonctionnaire américain(e) en ce qui concerne le traitement de leurs données à caractère personnel, telles que le Wiretap Act (loi sur les écoutes téléphoniques) ([214]), le Computer Fraud and Abuse Act (loi relative à la fraude et aux abus informatiques) ([215]), le Federal Torts Claim Act (loi fédérale sur les actions pour cause d'infraction) ([216]), le Right to Financial Privacy Act (loi sur le droit à la protection des données personnelles à caractère financier) ([217]), et le Fair Credit Reporting Act ([218]).

([209]) 5 U.S.C. § 702.

([210]) Généralement, seules les décisions «finales» d'une agence — par opposition aux décisions préliminaires, procédurales ou intermédiaires — sont soumises au contrôle juridictionnel. Voir 5 U.S.C. § 704.

([211]) 5 U.S.C. § 706(2)(A).

([212]) 18 U.S.C. §§ 2701 à 2712.

([213]) L'ECPA protège les communications détenues par deux catégories définies de prestataires de service réseau, à savoir les prestataires de: i) services de communication électronique, tels que les services de téléphonie ou de messagerie électronique; ii) de services informatiques à distance, tels que des services de stockage et de traitement de données.

([214]) 18 U.S.C. §§ 2510 et suivants. Conformément au Wiretap Act (18 U.S.C. § 2520), une personne dont une communication téléphonique, verbale ou électronique est interceptée, divulguée ou délibérément utilisée peut intenter une action civile pour violation du Wiretap Act, y compris, dans certaines circonstances, contre un agent d'État particulier ou contre les États-Unis. Pour la collecte d'informations d'adressage et d'autres informations sans contenu (adresse IP, adresse électronique destinataire/émetteur, par exemple), voir également chapitre «Pen Registers and Trap and Trace Devices» du titre 18 (18 U.S.C. §§ 3121 à 3127 et, en ce qui concerne l'action civile, § 2707).

([215]) 18 U.S.C. § 1030. Conformément au Computer Fraud and Abuse Act, toute personne peut intenter un procès contre toute autre personne pour accès non autorisé intentionnel (ou pour accès autorisé excessif) dans le but de recueillir des informations auprès d'un établissement financier, d'un système informatique des autorités américaines ou d'un autre système déterminé, y compris, dans certaines circonstances, contre un agent d'État particulier.

([216]) 28 U.S.C. §§ 2671 et suivants. Conformément au Federal Tort Claims Act, une personne peut intenter un procès, dans certaines circonstances, contre les États-Unis pour actes ou omissions négligents ou illégitimes que commet tout agent de l'État agissant dans le cadre de ses fonctions ou de son emploi.

([217]) 12 U.S.C. §§ 3401 et suivants. Conformément au Right to Financial Privacy Act, une personne peut intenter un procès, dans certaines circonstances, contre les États-Unis pour obtention ou divulgation de documents financiers protégés en violation de la loi. L'accès du gouvernement aux documents financiers protégés est en général interdit, sauf si le gouvernement effectue la demande sous réserve d'une assignation ou d'un mandat de perquisition légal ou, sous réserve de limitations, d'une demande écrite officielle, et que la personne au sujet de laquelle des informations sont demandées reçoit notification d'une telle demande.

([218]) 15 U.S.C. §§ 1681-1681x. Conformément au Fair Credit Reporting Act, une personne peut intenter un procès contre toute personne qui ne se conforme pas aux exigences (notamment la nécessité d'une autorisation légale) concernant la collecte, la diffusion et l'utilisation d'informations sur les crédits à la consommation, ou, dans certaines circonstances, contre une agence gouvernementale.

(118) En outre, en vertu du FOIA ([219]), 5 U.S.C. § 552, toute personne a le droit d'obtenir l'accès à des informations d'agences fédérales, y compris lorsque celles-ci contiennent les données à caractère personnel de la personne concernée. Après avoir épuisé les voies de recours administratives, une personne concernée peut invoquer ce droit d'accès en justice, à moins que ces informations ne soient protégées contre toute divulgation publique par une dérogation ou par une exclusion spéciale à des fins répressives ([220]). Dans ce cas, la juridiction appréciera si une dérogation s'applique ou a été légalement invoquée par l'autorité publique compétente.

3.2. **Accès aux données et utilisation de celles-ci par les autorités publiques américaines à des fins de sécurité nationale**

(119) Le droit des États-Unis impose diverses limitations et garanties en ce qui concerne l'accès aux données à caractère personnel et l'utilisation de celles-ci à des fins de sécurité nationale. Il prévoit également des mécanismes de surveillance et de recours qui sont conformes aux exigences visées au considérant 89 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

3.2.1. ***Bases juridiques, limitations et garanties***

3.2.1.1. *Cadre juridique applicable*

(120) Les données à caractère personnel transférées de l'Union vers des organisations participant au CPD UE - États-Unis peuvent être collectées par les autorités américaines à des fins de sécurité nationale sur la base de différents instruments juridiques, sous réserve de conditions et de garanties spécifiques.

(121) Une fois que des organisations situées aux États-Unis ont reçu des données à caractère personnel, les services de renseignement américains ne peuvent demander l'accès à ces données à des fins de sécurité nationale que s'ils y sont autorisés par la loi, en particulier en vertu de la loi sur la surveillance des renseignements étrangers (FISA) ou des dispositions légales autorisant l'accès au moyen de lettres de sécurité nationale (National Security Letters, NSL) ([221]). Le FISA contient plusieurs bases juridiques qui peuvent être utilisées pour collecter (et par la suite traiter) les données à caractère personnel de personnes concernées de l'Union transférées en vertu du CPD UE - États-Unis [article 105 du FISA ([222]), article 302 du FISA ([223]), article 402 du FISA ([224]), article 501 du FISA ([225]) et article 702 du FISA ([226])], comme décrit plus en détail aux considérants 142 à 152.

([219]) 5 U.S.C. § 552.

([220]) Ces exclusions sont toutefois encadrées. À titre d'exemple, conformément au 5 U.S.C. § 552 (b)(7), les droits accordés en vertu du FOIA sont exclus pour «les documents ou informations collectés à des fins répressives, mais uniquement si la production de tels documents ou informations en matière répressive A) pourrait raisonnablement être présumée entraver une action répressive, B) priverait une personne d'un droit à un procès équitable ou à un jugement impartial, C) pourrait raisonnablement être présumée constituer une atteinte injustifiée à la vie privée, D) pourrait raisonnablement être présumée révéler l'identité d'une source confidentielle, notamment d'une agence ou autorité nationale, locale ou étrangère ou de toute institution privée ayant fourni des informations à titre confidentiel, et, dans le cas d'un document ou d'informations collectés par des services répressifs dans le cadre d'une enquête pénale ou par une agence menant une enquête nationale légale en matière de renseignement de sécurité, des informations fournies par une source confidentielle, E) aurait pour effet de révéler au grand jour des techniques et procédures propres aux enquêtes ou poursuites menées par les services répressifs ou de divulguer les lignes directrices appliquées aux enquêtes ou poursuites menées par les services répressifs, au risque probable de permettre le contournement de la loi, ou F) pourrait raisonnablement être présumée mettre en péril la vie ou la sécurité de toute personne. De plus, lors de toute demande impliquant l'accès à des documents (dont la production pourrait raisonnablement être présumée entraver une action répressive) et chaque fois A) que l'enquête ou la procédure implique une possible violation du droit pénal; et B) qu'il existe des raisons de croire i) que la personne faisant l'objet de l'enquête ou de la procédure n'est pas consciente de la litispendance de cette dernière, et ii) que la divulgation de l'existence des documents pourrait raisonnablement être présumée entraver une action répressive, l'agence peut, durant une période limitée à la période pendant laquelle cette circonstance continue de prévaloir, traiter les documents comme n'étant pas soumis aux dispositions de la présente section» [5 U.S.C. § 552 (c)(1)].

([221]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u et 1681v; et 18 U.S.C. § 2709. Voir considérant 153.

([222]) 50 U.S.C. § 1804, qui porte sur la surveillance électronique classique des individus.

([223]) 50 U.S.C. § 1822, qui porte sur les fouilles corporelles à des fins de renseignement extérieur.

([224]) 50 U.S.C. § 1842 lu en combinaison avec § 1841(2) et titre 18, article 3127, relatif à l'installation de dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications.

([225]) 50 U.S.C. § 1861, qui permet au FBI de soumettre «une demande d'ordonnance autorisant un transporteur public, un établissement d'hébergement public, un établissement de stockage physique ou un établissement de location de véhicules à divulguer des documents en sa possession dans le cadre d'une enquête visant à recueillir des informations de renseignement extérieur ou d'une enquête concernant le terrorisme international».

([226]) 50 U.S.C. § 1881a, qui permet aux composantes de la communauté du renseignement des États-Unis de demander l'accès à des informations, y compris le contenu des communications internet, auprès de sociétés américaines, en ciblant certaines personnes qui ne sont pas américaines en dehors des États-Unis, avec l'aide légalement obligatoire des fournisseurs de communications électroniques.

(122) 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. La collecte en dehors des États-Unis est fondée sur le décret présidentiel n° 12333 (Executive Order 12333, ci-après l'«EO 12333») ([227]), émis par le président ([228]).

(123) La collecte de renseignements d'origine électromagnétique est la forme de collecte de renseignements la plus pertinente pour la présente décision relative à l'adéquation du niveau de protection, car elle concerne la collecte de communications électroniques et de données provenant de systèmes d'information. Cette collecte peut être effectuée par les agences de renseignement américaines à la fois sur le territoire des États-Unis (sur la base du FISA) et pendant que les données sont en transit vers les États-Unis (sur la base de l'EO 12333).

(124) Le 7 octobre 2022, le président des États-Unis a publié l'EO 14086 sur le renforcement des garanties pour les activités de renseignement d'origine électromagnétique menées par les États-Unis, qui fixe des limites et des garanties pour toutes les activités de renseignement d'origine électromagnétique menées par les États-Unis. Ce décret remplace, dans une large mesure ([229]), la directive présidentielle n° 28 (Presidential Policy Directive 28, ci-après la «PPD-28»), renforce les conditions, les limitations et les garanties qui s'appliquent à toutes les activités de renseignement d'origine électromagnétique (c'est-à-dire sur la base du FISA et de l'EO 12333), quel que soit le lieu où elles se déroulent ([230]), et établit un nouveau mécanisme de recours par lequel ces garanties peuvent être invoquées et appliquées par les personnes concernées ([231]) (voir plus en détail les considérants 176 à 194). Ce faisant, il transpose en droit américain le résultat des pourparlers qui ont eu lieu entre l'UE et les États-Unis à la suite de l'invalidation par la Cour de justice de la décision de la Commission relative à l'adéquation du niveau de protection assuré par le bouclier de protection des données (voir considérant 6). Il s'agit donc d'un élément particulièrement important du cadre juridique évalué dans la présente décision.

(125) Les limitations et garanties introduites par l'EO 14086 complètent celles prévues à l'article 702 du FISA et à l'EO 12333. Les exigences décrites ci-dessous (aux sections 3.2.1.2 et 3.2.1.3) doivent être appliquées par les agences de renseignement lorsqu'elles se livrent à des activités de renseignement d'origine électromagnétique en vertu de l'article 702 du FISA et de l'EO 12333, par exemple lorsqu'elles sélectionnent/identifient des catégories de renseignements étrangers à acquérir en vertu de l'article 702 du FISA; collectent des renseignements étrangers ou des contre-renseignements conformément à l'EO 12333; et prennent des décisions de ciblage individuel au titre de l'article 702 du FISA et de l'EO 12333.

(126) Les exigences énoncées dans ce décret présidentiel sont contraignantes pour l'ensemble de la communauté du renseignement. Elles 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 consultation avec le procureur général, le responsable de la protection des libertés civiles du bureau du directeur du renseignement national (ODNI CLPO) et le conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, PCLOB) — un organe de surveillance indépendant habilité à examiner les politiques relevant du pouvoir exécutif et leur mise en œuvre, en vue de protéger la vie privée et les libertés civiles (voir considérant 110 en ce qui concerne le rôle et le statut du PCLOB) — et être rendues publiques ([232]). En outre, une fois que les

([227]) EO 12333: United States Intelligence Activities, Federal Register vol. 40, n° 235 (8 décembre 1981, tel que modifié le 30 juillet 2008). Le décret EO 12333 définit plus généralement les objectifs, les orientations principales, les missions et les responsabilités des activités de renseignement des États-Unis (y compris le rôle des diverses composantes de la communauté du renseignement) et établit le cadre général de la conduite des activités de renseignement.

([228]) En vertu de l'article II de la Constitution des États-Unis, la responsabilité de garantir la sécurité nationale, et notamment de recueillir des renseignements étrangers, relève de l'autorité du président en tant que commandant en chef des forces armées.

([229]) L'EO 14086 remplace une directive présidentielle antérieure, la directive 28 (PPD-28), à l'exception de son article 3 et d'une annexe complémentaire (qui demande aux agences de renseignement de réexaminer chaque année leurs priorités et leurs besoins en matière de renseignement d'origine électromagnétique, en tenant compte des avantages des activités de renseignement d'origine électromagnétique pour les intérêts nationaux des États-Unis, ainsi que des risques posés par ces activités) et de son article 6 (qui contient des dispositions générales), voir mémorandum de sécurité nationale sur la révocation partielle de la directive 28 (PPD-28), disponible en anglais à l'adresse suivante: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Voir article 5(f) de l'EO 14086, qui explique que le décret a le même champ d'application que la PPD-28, qui, selon sa note de bas de page 3, s'applique aux activités de renseignement d'origine électromagnétique menées dans le but de collecter des communications ou des informations sur les communications, à l'exception des activités de renseignement d'origine électromagnétique entreprises pour tester ou développer des capacités de renseignement d'origine électromagnétique.

([231]) Voir à cet égard, par exemple, article 5(h) de l'EO 14086, qui précise que les garanties prévues par le décret créent une obligation juridique et peuvent être appliquées par les personnes concernées dans le cadre du mécanisme de recours.

([232]) Voir article 2(c)(iv)(C) de l'EO 14086.

politiques et procédures actualisées seront en place, le PCLOB procédera à un examen afin de s'assurer qu'elles sont conformes au décret. Dans les 180 jours suivant l'achèvement de cet examen par le PCLOB, chaque agence de renseignement doit examiner attentivement et mettre en œuvre toutes les recommandations du PCLOB ou y donner suite d'une autre manière. Le 3 juillet 2023, le gouvernement américain a publié ces politiques et procédures actualisées ([233]).

3.2.1.2. *Limitations et garanties concernant la collecte de données à caractère personnel à des fins de sécurité nationale*

(127) L'EO 14086 fixe un certain nombre d'exigences fondamentales qui s'appliquent à toutes les activités de renseignement d'origine électromagnétique (collecte, utilisation, diffusion, etc. de données à caractère personnel).

(128) Premièrement, ces activités doivent être fondées sur une loi ou une autorisation présidentielle et doivent être effectuées conformément au droit des États-Unis, notamment la Constitution ([234]).

(129) Deuxièmement, des garanties appropriées doivent être mises en place pour s'assurer qu'il est pleinement tenu compte de la protection de la vie privée et des libertés fondamentales dans la planification de ces activités ([235]).

(130) En particulier, toute activité de renseignement d'origine électromagnétique ne peut être menée qu'«après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, que les activités sont nécessaires pour faire progresser une priorité validée en matière de renseignement» (en ce qui concerne la notion de «priorité validée en matière de renseignement», voir considérant 135) ([236]).

(131) En outre, ces activités ne peuvent être menées que «dans la mesure et d'une manière proportionnées à la priorité validée en matière de renseignement pour laquelle elles ont été autorisées» ([237]). En d'autres termes, il convient de trouver un juste équilibre «entre l'importance de la priorité poursuivie en matière de renseignement et l'incidence sur la vie privée et les libertés civiles de la personne concernée, quels que soient sa nationalité et son lieu de résidence» ([238]).

(132) Enfin, pour garantir le respect de ces exigences générales — qui tiennent compte des principes de légalité, de nécessité et de proportionnalité —, les activités de renseignement d'origine électromagnétique font l'objet d'une surveillance (voir plus en détail la section 3.2.2) ([239]).

(133) Ces exigences fondamentales sont renforcées, en ce qui concerne la collecte de renseignements d'origine électromagnétique, par un certain nombre de conditions et de limitations garantissant que l'ingérence dans les droits des personnes est limitée à ce qui est nécessaire et proportionné pour atteindre un objectif légitime.

(134) Premièrement, le décret limite de deux manières les motifs pour lesquels des données peuvent être collectées dans le cadre d'activités de renseignement d'origine électromagnétique. D'une part, le décret définit les objectifs légitimes qui peuvent être poursuivis par la collecte de renseignements d'origine électromagnétique, par exemple comprendre ou évaluer les capacités, les intentions ou les activités d'organisations étrangères, notamment d'organisations terroristes internationales, qui constituent une menace actuelle ou potentielle pour la sécurité nationale des États-Unis; se protéger contre les capacités et les activités militaires étrangères; comprendre ou évaluer les menaces transnationales qui ont une incidence sur la sécurité mondiale, telles que les changements climatiques et autres changements écologiques, les risques pour la santé publique et les menaces humanitaires ([240]). D'autre part, le décret énumère

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Article 2(a)(i) de l'EO 14086.

([235]) Article 2(a)(ii) de l'EO 14086.

([236]) Article 2(a)(ii)(A) de l'EO 14086. Cela n'implique pas nécessairement que le renseignement d'origine électromagnétique soit le seul moyen de faire progresser certains aspects d'une priorité validée en matière de renseignement. Par exemple, la collecte de renseignements d'origine électromagnétique peut être utilisée pour garantir d'autres voies de validation (par exemple, pour corroborer les informations reçues d'autres sources de renseignements) ou pour maintenir un accès fiable aux mêmes informations [article 2(c)(i)(A) de l'EO 14086].

([237]) Article 2(a)(ii)(B) de l'EO 14086.

([238]) Article 2(a)(ii)(B) de l'EO 14086.

([239]) Article 2(a)(iii), en liaison avec l'article 2(d) de l'EO 14086.

([240]) Article 2(b)(i) de l'EO 14086. En raison de la liste circonscrite d'objectifs légitimes dans l'EO, qui ne couvre pas d'éventuelles menaces futures, l'EO prévoit la possibilité pour le président de mettre à jour cette liste si de nouveaux impératifs de sécurité nationale apparaissent, tels que de nouvelles menaces pour la sécurité nationale. Ces mises à jour doivent en principe être rendues publiques, sauf si le président considère que cela constituerait en soi un risque pour la sécurité nationale des États-Unis [article 2(b)(i)(B) de l'EO 14086].

certains objectifs qui ne doivent jamais être poursuivis par des activités de renseignement d'origine électromagnétique, par exemple dans le but d'entraver les critiques, les désaccords ou la libre expression d'idées ou d'opinions politiques par des personnes ou par la presse; de défavoriser des personnes au motif de leur appartenance ethnique, de leur race, de leur genre, de leur identité sexuelle, de leur orientation sexuelle ou de leur religion; ou de conférer un avantage concurrentiel aux entreprises américaines ([241]).

(135) En outre, les objectifs légitimes définis dans l'EO 14086 ne peuvent pas, à eux seuls, être invoqués par les agences 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. En d'autres termes, la collecte effective ne peut avoir lieu que pour faire progresser une priorité plus spécifique. Ces priorités sont établies dans le cadre d'une procédure spéciale visant à garantir le respect des exigences légales applicables, notamment celles relatives à la vie privée et aux libertés civiles. Plus précisément, les priorités en matière de renseignement sont d'abord définies par le directeur du renseignement national (dans le cadre des priorités nationales en matière de renseignement) et soumises à l'approbation du président ([242]). Avant de proposer au président des priorités en matière de renseignement, le directeur doit, conformément à l'EO 14086, obtenir une évaluation de l'ODNI CLPO pour chaque priorité afin de déterminer si elle 1) fait progresser un ou plusieurs objectifs légitimes énumérés dans le décret; 2) n'a pas été conçue pour la collecte de renseignements d'origine électromagnétique à des fins interdites énumérées dans le décret ni ne devrait donner lieu à une telle collecte; et 3) a été établie après avoir dûment pris en compte les aspects relatifs à la vie privée et aux libertés civiles de toutes les personnes, quels que soient leur nationalité et leur lieu de résidence ([243]). Si le directeur est en désaccord avec l'évaluation du CLPO, les deux avis doivent être présentés au président ([244]).

(136) Par conséquent, cette procédure garantit notamment que les questions de protection de la vie privée sont prises en compte dès le stade initial de l'élaboration des priorités en matière de renseignement.

(137) Deuxièmement, une fois qu'une priorité en matière de renseignement a été établie, un certain nombre d'exigences régissent la décision de savoir si et dans quelle mesure des renseignements d'origine électromagnétique peuvent être collectés pour faire avancer cette priorité. Ces exigences concrétisent les normes générales de nécessité et de proportionnalité énoncées à l'article 2(a) du décret.

(138) En particulier, les renseignements d'origine électromagnétique ne peuvent être collectés qu'«après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, que la collecte est nécessaire pour faire progresser une priorité spécifique en matière de renseignement» ([245]). Afin de déterminer si la collecte de renseignements d'origine électromagnétique est nécessaire pour faire progresser une priorité validée en matière de renseignement, les agences de renseignement américaines doivent examiner la disponibilité, la faisabilité et la validité d'autres sources et méthodes moins intrusives, notamment de sources diplomatiques et publiques ([246]). Lorsqu'elles sont disponibles, la priorité doit être donnée à ces autres sources et méthodes moins intrusives ([247]).

(139) Lorsque, en application de ces critères, la collecte de renseignements d'origine électromagnétique est jugée nécessaire, elle doit être aussi «ciblée que possible» et ne doit pas «avoir un effet disproportionné sur la vie privée et les libertés civiles» ([248]). Afin de prévenir un effet disproportionné sur la vie privée et les libertés civiles, c'est-à-dire de trouver un juste équilibre entre les besoins de sécurité nationale et la protection de la vie privée et des libertés civiles, tous les facteurs pertinents doivent être dûment pris en compte, tels que la nature de l'objectif poursuivi; le caractère intrusif de la collecte, notamment sa durée; la contribution probable de la collecte à l'objectif poursuivi; les conséquences raisonnablement prévisibles pour les personnes concernées; et la nature et le caractère sensible des données à collecter ([249]).

([241]) Article 2(b)(ii) de l'EO 14086.
([242]) Article 102A de la loi sur la sécurité nationale et article 2(b)(iii) de l'EO 14086.
([243]) Dans des cas exceptionnels (notamment lorsqu'une telle procédure ne peut être mise en œuvre en raison de la nécessité de répondre à un besoin en matière de renseignement nouveau ou en évolution), ces priorités peuvent être fixées directement par le président ou le responsable d'une composante de la communauté du renseignement, qui doivent en principe appliquer les mêmes critères que ceux décrits à l'article 2(b)(iii)(A)(1) à (3), voir article 4(n) de l'EO 14086.
([244]) Article 2(b)(iii)(C) de l'EO 14086.
([245]) Article 2(b) et (c)(i)(A) de l'EO 14086.
([246]) Article 2(c)(i)(A) de l'EO 14086.
([247]) Article 2(c)(i)(A) de l'EO 14086.
([248]) Article 2(c)(i)(B) de l'EO 14086.
([249]) Article 2(c)(i)(B) de l'EO 14086.

(140) En ce qui concerne le type de collecte de renseignements d'origine électromagnétique, la collecte de données aux États-Unis, qui est la plus pertinente pour la présente décision puisqu'elle concerne des données qui ont été transférées vers des organisations aux États-Unis, doit toujours être ciblée, comme expliqué plus en détail aux considérants 142 à 153.

(141) La «collecte en vrac» ([250]) ne peut avoir lieu qu'en dehors des États-Unis, sur la base de l'EO 12333. Également dans ce cas, conformément à l'EO 14086, la priorité doit être donnée à une collecte ciblée ([251]). Inversement, la collecte en vrac n'est autorisée que lorsque les informations nécessaires pour faire progresser une priorité validée en matière de renseignement ne peuvent raisonnablement pas être obtenues par une collecte ciblée ([252]). Lorsqu'il est nécessaire de procéder à une collecte en vrac en dehors des États-Unis, des garanties spécifiques s'appliquent en vertu de l'EO 14086 ([253]). Premièrement, des méthodes et des mesures techniques doivent être appliquées afin de limiter les données collectées à ce qui est nécessaire pour faire progresser une priorité validée en matière de renseignement, tout en réduisant autant que possible la collecte d'informations non pertinentes ([254]). Deuxièmement, le décret limite l'utilisation des informations collectées en vrac (y compris les interrogations de données) à six objectifs spécifiques, notamment la protection contre le terrorisme, la prise d'otages et la détention de personnes en captivité par un gouvernement, une organisation ou une personne étrangère ou pour son compte; la protection contre l'espionnage étranger, le sabotage ou l'assassinat; la protection contre les menaces liées au développement, à la possession ou à la prolifération d'armes de destruction massive ou de technologies et menaces connexes, etc. ([255]). Enfin, toute interrogation de données de renseignement d'origine électromagnétique obtenues en vrac ne peut avoir lieu que si elle est nécessaire pour faire progresser une priorité validée en matière de renseignement, dans le cadre de la poursuite de ces six objectifs et conformément à des politiques et procédures qui tiennent dûment compte de l'incidence des interrogations de données sur la vie privée et les libertés civiles de toutes les personnes, quels que soient leur nationalité ou leur lieu de résidence ([256]).

(142) Outre les exigences de l'EO 14086, la collecte de données de renseignement d'origine électromagnétique transférées vers une organisation aux États-Unis est soumise à des limitations et garanties spécifiques régies par l'article 702 du FISA ([257]). Ce dernier autorise la collecte de renseignements étrangers via le ciblage de personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis, avec l'assistance obligatoire des fournisseurs de services de communications électroniques américains ([258]). Afin de collecter des renseignements étrangers conformément à l'article 702 du FISA, le procureur général et le directeur du renseignement national

([250]) C'est-à-dire la collecte de grandes quantités de renseignements d'origine électromagnétique qui, pour des raisons techniques ou opérationnelles, est effectuée sans utiliser de discriminants (par exemple des identifiants ou des critères de sélection spécifiques), voir article 4(b) de l'EO 14086. Conformément à l'EO 14086 et comme expliqué plus en détail au considérant 141, la collecte en vrac prévue par l'EO 12333 n'a lieu que si elle est nécessaire pour faire progresser certaines priorités validées en matière de renseignement et est soumise à un certain nombre de restrictions et de garanties destinées à s'assurer que les données ne sont pas consultées à l'aveugle. Il convient donc de distinguer la collecte en vrac de la collecte généralisée et indifférenciée («surveillance de masse») sans restrictions ni garanties.

([251]) Article 2(c)(ii)(A) de l'EO 14086.

([252]) Article 2(c)(ii)(A) de l'EO 14086.

([253]) Les règles spécifiques de l'EO 14086 relatives à la collecte en vrac s'appliquent également à une activité ciblée de collecte de renseignements d'origine électromagnétique qui utilise temporairement des données acquises sans discrimants (par exemple des critères de sélection ou des identifiants spécifiques), c'est-à-dire en vrac (ce qui n'est possible qu'en dehors du territoire des États-Unis). Ce n'est pas le cas lorsque ces données ne sont utilisées que pour soutenir la phase technique initiale de l'activité ciblée de collecte de renseignements d'origine électromagnétique, qu'elles ne sont conservées que pendant une courte période nécessaire pour mener à bien cette phase et qu'elles sont supprimées immédiatement après [article 2, point c) ii), point D) de l'EO 14086]. Dans ce cas, le seul objectif de la collecte initiale sans discriminants est de permettre une collecte ciblée d'informations en appliquant un identifiant ou un critère de sélection spécifique. Dans un tel scénario, seules les données qui répondent à l'application d'un certain discriminant sont insérées dans les bases de données gouvernementales, tandis que les autres données sont détruites. Cette collecte ciblée reste donc régie par les règles générales applicables à la collecte de renseignements d'origine électromagnétique, y compris l'article 2(a)-(b) et (c)(i) de l'EO 14086.

([254]) Article 2(c)(ii)(A) de l'EO 14086.

([255]) Article 2(c)(ii)(B) de l'EO 14086. Si de nouveaux impératifs de sécurité nationale apparaissent, tels que de nouvelles menaces pour la sécurité nationale, le président peut mettre à jour cette liste. Ces mises à jour doivent en principe être rendues publiques, sauf si le président considère que cela constituerait en soi un risque pour la sécurité nationale des États-Unis [article 2(c)(ii)(C) de l'EO 14086]. En ce qui concerne les demandes de données collectées en vrac, voir article 2(c)(iii)(D) de l'EO 14086.

([256]) Article 2(a)(ii)(A), en liaison avec l'article 2(c)(iii)(D) de l'EO 14086. Voir également annexe VII.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). En particulier, comme l'a noté le Conseil de surveillance de la vie privée et des libertés civiles, la surveillance au titre de l'article 702 «consiste exclusivement dans le fait de cibler des personnes (non américaines) spécifiques faisant l'objet d'une décision spécifique» (Conseil de surveillance de la vie privée et des libertés civiles, rapport sur le programme de surveillance mis en œuvre conformément à l'article 702 de la loi sur la surveillance et le renseignement étranger, 2 juillet 2014, rapport sur l'article 702, p. 111). Voir également CLPO/NSA (NSA's Implementation of Foreign Intelligence Act Section 702 du 16 avril 2014). La notion de «fournisseur de services de communications électroniques» est définie dans 50 U.S.C. § 1881 (a)(4).

soumettent des certifications annuelles au tribunal de la surveillance du renseignement étranger (Foreign Intelligence Surveillance Court, FISC), qui déterminent des catégories de renseignements étrangers à collecter ([259]). Les certifications doivent être accompagnées de procédures de ciblage, de minimisation et d'interrogation, qui sont également approuvées par le tribunal et sont juridiquement contraignantes pour les agences de renseignement américaines.

(143) Le FISC est un tribunal indépendant ([260]) institué par une loi fédérale dont les décisions peuvent être contestées devant la cour révisant les décisions en matière de surveillance du renseignement extérieur (FISCR) ([261]) et, en dernier recours, devant la Cour suprême des États-Unis ([262]). Le FISC (de même que la FISCR) reçoit l'appui d'un panel permanent de cinq avocats et cinq experts techniques qui ont une expertise en matière de sécurité nationale et de libertés civiles ([263]). Le tribunal désigne une personne de ce groupe qui agira en tant qu'amicus curiae pour contribuer à l'examen de toute demande d'ordonnance ou de révision qui, selon le tribunal, contiendrait une interprétation nouvelle ou notable de la loi, sauf si le tribunal estime cette désignation inutile ([264]). Cette possibilité garantit notamment que les questions de protection de la vie privée sont dûment prises en compte dans les évaluations du tribunal. Celui-ci peut également désigner une personne ou une organisation qui agira en tant qu'amicus curiae, notamment en fournissant une expertise technique, chaque fois qu'il l'estime approprié ou, sur demande, autorisera une personne ou une organisation à déposer un dossier d'amicus curiae ([265]).

(144) Le FISC examine les certifications et les procédures connexes (en particulier les procédures de ciblage et de minimisation) pour veiller à leur conformité avec les exigences du FISA. S'il constate que les exigences ne sont pas satisfaites, il peut refuser la certification en tout ou en partie et demander que les procédures soient modifiées ([266]). À cet égard, le FISC a confirmé à plusieurs reprises que son examen des procédures de ciblage et de minimisation au titre de l'article 702 ne se limite pas aux procédures telles qu'elles sont rédigées, mais qu'il porte également sur la manière dont les procédures sont mises en œuvre par le gouvernement ([267]).

(145) Les décisions de ciblage individuel sont prises par la NSA (l'agence de renseignement responsable du ciblage en vertu de l'article 702 du FISA) conformément aux procédures de ciblage approuvées par le FISC, qui exigent que la NSA évalue, sur la base de l'ensemble des circonstances, que le ciblage d'une personne donnée est susceptible de permettre l'obtention d'une catégorie de renseignements étrangers indiquée dans une certification ([268]). Cette évaluation doit être détaillée et factuelle, et s'appuyer sur le jugement analytique, la formation spécialisée et

([259]) 50 U.S.C. § 1881a (g).

([260]) Le FISC se compose de juges nommés par le juge en chef parmi les juges de district américains qui siègent et ont été nommés au préalable par le président et confirmés par le Sénat. Les juges, qui ont un statut permanent et ne peuvent être révoqués que pour un motif sérieux, exercent auprès du FISC pour des mandats de sept ans échelonnés. Le FISA exige que les juges soient recrutés dans au moins sept circuits judiciaires américains différents. Voir 50 U.S.C. § 1803 (a). Les juges sont assistés de référendaires expérimentés qui constituent le personnel juridique du tribunal et préparent les analyses juridiques des demandes de collecte. Voir lettre de l'honorable Reggie B. Walton, juge-président, U.S. Foreign Intelligence Surveillance Court, adressée à l'honorable Patrick J. Leahy, Président, Commission judiciaire, Sénat américain (29 juillet 2013) («lettre Walton»), p. 2, consultable à l'adresse suivante: https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) La FISCR est composée de juges nommés par le juge en chef des États-Unis et recrutés dans les tribunaux de district ou cours d'appel américains, en service pour un mandat de sept ans échelonné. Voir 50 U.S.C. § 1803 (b).

([262]) Voir 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([263]) 50 U.S.C. § 1803 (i)(1), (3)(A).

([264]) 50 U.S.C. § 1803 (i)(2)(A).

([265]) 50 U.S.C. § 1803 (i)(2)(B).

([266]) Voir, par exemple, avis du FISC du 18 octobre 2018, disponible à l'adresse suivante: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct1, tel qu'il a été confirmé par la cour révisant les décisions en matière de surveillance du renseignement extérieur dans son avis du 12 juillet 2019, disponible à l'adresse suivante: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Voir par exemple FISC, Memorandum Opinion and Order at 35 (18 novembre 2020) (publication autorisée le 26 avril 2021) (annexe D).

([268]) 50 U.S.C. § 1881a(a), procédures utilisées par l'Agence de sécurité nationale pour cibler des personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis afin d'obtenir des renseignements étrangers conformément à l'article 702 de la loi sur la surveillance du renseignement étranger de 1978, tel que modifié, de mars 2018 (procédures de ciblage de la NSA), disponible à l'adresse suivante: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27, p. 1 à 4, expliqué plus en détail dans le rapport du PCLOB, p. 41 et 42.

l'expérience de l'analyste, ainsi que sur la nature des renseignements étrangers à obtenir ([269]). Le ciblage est effectué en choisissant des «sélecteurs» qui recensent des moyens de communication spécifiques, comme l'adresse électronique ou le numéro de téléphone d'une cible, mais jamais des mots clés ni même les noms des personnes ciblées ([270]).

(146) Les analystes de la NSA recenseront dans un premier temps des personnes non américaines se trouvant à l'étranger et dont la surveillance conduira, selon l'évaluation des analystes, à l'action de renseignement extérieur pertinente précisée dans la certification ([271]). Comme le prévoient les procédures de ciblage de la NSA, celle-ci ne peut diriger la surveillance vers une cible que si elle dispose déjà de certaines informations à son sujet ([272]). Il peut s'agir d'informations provenant de différentes sources, par exemple le renseignement humain. Grâce à ces autres sources, l'analyste doit également se renseigner sur un sélecteur spécifique (c'est-à-dire un compte de communication) utilisé par la cible potentielle. Une fois que ces personnes désignées individuellement auront été recensées et que leur ciblage aura été approuvé au moyen d'un mécanisme de révision élargi au sein de la NSA ([273]), des sélecteurs qui recensent les moyens de communication utilisés par les cibles (comme les adresses électroniques) seront mis en œuvre (c'est-à-dire développés et appliqués) ([274]).

(147) La NSA doit documenter la base factuelle de la sélection de la cible ([275]) et, à intervalles réguliers après le ciblage initial, affirmer que la norme de ciblage continue d'être respectée ([276]). Lorsque la norme de ciblage n'est plus respectée, la collecte doit cesser ([277]). La sélection de chaque cible par la NSA et l'enregistrement de chaque évaluation et justification de ciblage sont vérifiés tous les deux mois par les fonctionnaires des bureaux de surveillance du renseignement du ministère de la justice, qui sont tenus de signaler toute violation au FISC et au Congrès, afin de s'assurer qu'ils respectent les procédures de ciblage ([278]). La documentation écrite de la NSA permet au FISC de vérifier si certaines personnes sont correctement ciblées en vertu de l'article 702 du FISA, conformément à ses pouvoirs de surveillance décrits aux considérants 173 et 174 ([279]). Enfin, le directeur du renseignement national est également tenu de communiquer chaque année le nombre total de cibles au titre de l'article 702 du FISA dans des rapports annuels publics sur la transparence en matière statistique. Les entreprises qui reçoivent des directives au titre de l'article 702 du FISA peuvent publier des données agrégées (via des rapports de transparence) sur les demandes qu'elles reçoivent ([280]).

([269]) Procédures de ciblage de la NSA, p. 4. Voir PCLOB;

([270]) Voir PCLOB; rapport sur l'article 702, p. 32, 33 et 45 et autres références. Voir également l'évaluation semestrielle du respect des procédures et lignes directrices conformément à l'article 702 de la loi sur la surveillance du renseignement étranger, publiée par le procureur général et le directeur du renseignement national, période de référence: 1er décembre 2016-31 mai 2017, p. 41 (octobre 2018), disponible à l'adresse suivante: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, rapport sur l'article 702, p. 42 et 43.

([272]) Procédures de ciblage de la NSA, p. 2.

([273]) PCLOB, rapport sur l'article 702, p. 46. Par exemple, la NSA doit vérifier qu'il existe un lien entre la cible et le sélecteur et rendre compte des renseignements extérieurs susceptibles d'être recueillis; ces renseignements doivent être examinés et avalisés par deux analystes confirmés de la NSA; enfin le processus général fera l'objet d'un suivi et d'un examen ultérieur de l'ODNI et du ministère de la justice qui évalueront sa conformité. Voir CLPO/NSA (NSA's Implementation of Foreign Intelligence Act Section 702 du 16 avril 2014).

([274]) 50 U.S.C. § 1881a (h).

([275]) Procédures de ciblage de la NSA, p. 8. Voir également PCLOB, rapport sur l'article 702, p. 46. L'absence de justification écrite constitue un incident de conformité de la documentation qui doit être signalé au FISC et au Congrès. Voir l'évaluation semestrielle du respect des procédures et lignes directrices conformément à l'article 702 de la loi sur la surveillance du renseignement étranger, publiée par le procureur général et le directeur du renseignement national, période de référence: 1er décembre 2016-31 mai 2017, p. 41 (octobre 2018), rapport sur le respect de la conformité au FISC de l'ODNI du ministère de la justice pour la période décembre 2016-mai 2017, p. A-6, disponible à l'adresse suivante: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Voir les observations du gouvernement américain au tribunal de surveillance du renseignement extérieur, résumé 2015 des exigences notables de l'article 702, aux pages 2 et 3 (15 juillet 2015) et les informations fournies à l'annexe VII.

([277]) Voir les observations du gouvernement américain au tribunal de surveillance du renseignement extérieur, résumé 2015 des exigences notables de l'article 702, aux pages 2 et 3 (15 juillet 2015), qui indiquent que, «[s]i le gouvernement estime par la suite que le fait de continuer à utiliser le sélecteur d'une cible ne devrait pas permettre l'obtention de renseignements étrangers, le dessaisissement rapide est requis et tout retard peut donner lieu à un incident de conformité à signaler». Voir également les informations fournies à l'annexe VII.

([278]) PCLOB, rapport sur l'article 702, p. 70 et 72; article 13(b) du règlement intérieur du tribunal de la surveillance du renseignement extérieur, disponible à l'adresse suivante: https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Voir également le rapport sur le respect de la conformité avec le FISC de l'ODNI du ministère de la justice pour la période décembre 2016-mai 2017, p. A-6.

([280]) 50 U.S.C. § 1874.

(148) En ce qui concerne les autres bases juridiques permettant de collecter des données à caractère personnel transférées vers des organisations aux États-Unis, différentes restrictions et garanties s'appliquent. En général, la collecte de données en vrac est spécifiquement interdite en vertu de l'article 402 du FISA (dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications) et par le recours aux lettres de sécurité nationale, et demande à la place l'utilisation de «critères de sélection» spécifiques ([281]).

(149) Pour procéder à une surveillance électronique classique des individus (conformément à l'article 105 du FISA), les agences de renseignement doivent soumettre une demande au FISC, accompagnée d'un exposé des faits et circonstances invoqués à l'appui de la conviction qu'il existe un motif sérieux de croire que l'installation est utilisée ou sur le point d'être utilisée par une puissance étrangère ou un agent d'une puissance étrangère ([282]). Le FISC appréciera, entre autres, si sur la base des faits soumis, il existe une présomption sérieuse que c'est en effet le cas ([283]).

(150) Pour effectuer une perquisition dans des locaux ou sur des biens qui doit aboutir à une inspection, une saisie, etc., d'informations, de matériel ou de biens (par exemple, un dispositif informatique) sur la base de l'article 301 du FISA, une demande d'injonction du FISC est nécessaire ([284]). Cette demande doit notamment démontrer qu'il existe un motif sérieux de croire que la cible de la perquisition est une puissance étrangère ou un agent d'une puissance étrangère; que les locaux ou les biens à perquisitionner sont détenus, utilisés ou possédés par une puissance étrangère (ou par un agent d'une puissance étrangère) ou sont en transit vers ou depuis cette puissance étrangère ([285]).

(151) De même, l'installation de dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications (en vertu de l'article 402 du FISA) requiert une demande d'injonction du FISC (ou d'un juge magistrat américain) et l'utilisation d'un critère de sélection spécifique, à savoir un critère qui identifie spécifiquement une personne, un compte, etc., et qui sert à limiter, dans toute la mesure de ce qui est raisonnablement possible, l'étendue des informations recherchées ([286]). Cette base ne concerne pas le contenu des communications, mais a plutôt pour objet des informations sur le client ou l'abonné qui utilise un service (telles que le nom, l'adresse, le numéro de l'abonné, la longueur/le type de service reçu, la source/la modalité de paiement).

(152) L'article 501 du FISA ([287]), qui autorise la collecte de fichiers de sociétés d'un transporteur public (c'est-à-dire toute personne ou entité transportant des personnes ou des biens par voie terrestre, ferroviaire, maritime ou aérienne contre rémunération), d'un établissement d'hébergement public (par exemple un hôtel, un motel ou une auberge), d'un établissement de location de véhicules ou d'un établissement de stockage (c'est-à-dire qui fournit un espace ou des services liés au stockage de biens et de matériaux) ([288]), nécessite également une demande auprès du FISC ou d'un juge magistrat. Cette demande doit préciser les fichiers recherchés et les faits spécifiques et clairs donnant des raisons de croire que la personne à laquelle les fichiers se rapportent est une puissance étrangère ou un agent d'une puissance étrangère ([289]).

(153) Enfin, les lettres de sécurité nationale sont autorisées par différentes dispositions législatives et permettent aux services d'enquête d'obtenir des informations (n'incluant pas le contenu de communications) figurant dans des rapports de solvabilité, des états financiers et certains documents de transactions et d'abonnements électroniques de certaines entités (comme des institutions financières, des agences d'évaluation du crédit, des fournisseurs de services de communications électroniques) ([290]). La loi sur les lettres de sécurité nationale, qui autorise l'accès aux communications électroniques, ne peut être utilisée que par le FBI et exige que les demandes utilisent un terme qui identifie spécifiquement une personne, une entité, un numéro de téléphone ou un compte et qu'elles certifient que les informations présentent un intérêt pour une enquête de sécurité nationale autorisée afin de protéger le pays contre le terrorisme international ou des activités de renseignement clandestines ([291]). Les destinataires d'une lettre de sécurité nationale ont le droit de la contester devant un tribunal ([292]).

([281]) 50 U.S.C. § 1842(c)(3) et, en ce qui concerne les lettres de sécurité nationale, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); et 18 U.S.C. § 2709(a).

([282]) Un «agent d'une puissance étrangère» peut inclure des personnes non américaines qui se livrent à des activités de terrorisme international ou sont impliquées dans la prolifération d'armes de destruction massive (notamment des actes préparatoires) [50 U.S.C. § 1801(b)(1)].

([283]) 50 U.S.C. § 1804. Voir également § 1841(4) en ce qui concerne le choix des critères de sélection.

([284]) 50 U.S.C. § 1821(5).

([285]) 50 U.S.C. § 1823(a).

([286]) 50 U.S.C. § 1842 en liaison avec § 1841(2) et titre 18, article 3127.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861 à 1862.

([289]) 50 U.S.C. § 1862(b).

([290]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u et 1681v; et 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709(b).

([292]) Par exemple 18 U.S.C. § 2709(d).

3.2.1.3. *Utilisation ultérieure des informations recueillies*

(154) Le traitement des données à caractère personnel collectées par les agences de renseignement américaines au moyen de renseignements d'origine électromagnétique fait l'objet d'un certain nombre de garanties.

(155) Premièrement, chaque agence de renseignement doit garantir une sécurité appropriée des données et empêcher l'accès des personnes non autorisées aux données à caractère personnel collectées au moyen de renseignements d'origine électromagnétique. À cet égard, différents instruments, notamment des lois, des lignes directrices et des normes, précisent les exigences minimales en matière de sécurité de l'information qui doivent être mises en place (par exemple, l'authentification multifactorielle, le chiffrement, etc.) ([293]). L'accès aux données collectées doit être limité au personnel autorisé et formé qui a besoin de connaître ces informations pour mener à bien sa mission ([294]). Plus généralement, les agences de renseignement doivent proposer une formation appropriée à leurs employés, y compris sur les procédures de signalement et de traitement des violations de la loi (notamment l'EO 14086) ([295]).

(156) Deuxièmement, les agences de renseignement doivent se conformer aux normes de la communauté du renseignement en matière d'exactitude et d'objectivité, notamment en ce qui concerne la qualité et la fiabilité des données, la prise en compte d'autres sources d'information et l'objectivité dans la réalisation des analyses ([296]).

(157) Troisièmement, en ce qui concerne la conservation des données, l'EO 14086 précise que les données à caractère personnel des personnes non américaines sont soumises aux mêmes périodes de conservation que celles qui s'appliquent aux données des ressortissants américains ([297]). Les services de renseignement sont tenus de définir des durées de conservation précises et/ou les facteurs à prendre en compte pour déterminer la longueur des durées de conservation applicables (par exemple, si les informations constituent la preuve d'une infraction; si les informations constituent des renseignements étrangers; si les informations sont nécessaires pour protéger la sécurité des personnes ou des organisations, y compris les victimes ou les cibles du terrorisme international), qui sont prévues dans différents instruments juridiques ([298]).

(158) Quatrièmement, des règles spécifiques s'appliquent à la diffusion des données à caractère personnel collectées au moyen de renseignements d'origine électromagnétique. En règle générale, les données à caractère personnel concernant des personnes non américaines ne peuvent être diffusées que si elles concernent le même type d'informations que celles qui peuvent être diffusées au sujet de ressortissants américains, par exemple les informations nécessaires pour protéger la sécurité d'une personne ou d'une organisation (telles que les cibles, les victimes ou les otages d'organisations terroristes internationales) ([299]). En outre, les données à caractère personnel ne peuvent être diffusées uniquement en raison de la nationalité ou du pays de résidence d'une personne ou dans le but de contourner les exigences de l'EO 14086 ([300]). La diffusion au sein du gouvernement américain ne peut avoir lieu

([293]) Article 2(c)(iii)(B)(1) de l'EO 14086. Voir également titre VIII de la loi sur la sécurité nationale (qui détaille les conditions d'accès aux informations classifiées), article 1.5 de l'EO 12333 (qui oblige les chefs des agences de la communauté du renseignement à respecter les lignes directrices en matière de partage et de sécurité de l'information, de protection de la vie privée et d'autres exigences juridiques), la directive de sécurité nationale 42 intitulée «National Policy for the Security of National Security Telecommunications and Information Systems» (chargeant le comité des systèmes de sécurité nationale de fournir aux services et agences fédéraux des orientations en matière de sécurité des systèmes de sécurité nationale) et le mémorandum de sécurité nationale 8 intitulé «Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems» (établissant un calendrier et des orientations sur la manière dont les exigences en matière de cybersécurité seront mises en œuvre pour les systèmes de sécurité nationaux, notamment l'authentification multifactorielle, le chiffrement, les technologies en nuage et les services de détection des terminaux).

([294]) Article 2(c)(iii)(B)(2) de l'EO 14086. En outre, les données à caractère personnel pour lesquelles aucune décision finale de conservation n'a été prise ne peuvent être consultées que pour prendre ou étayer une telle décision ou pour exercer des fonctions autorisées d'administration, de contrôle, de développement, de sécurité ou de surveillance [article 2(c)(iii)(B)(3) de l'EO 14086].

([295]) Article 2(d)(ii) de l'EO 14086.

([296]) Article 2(c)(iii)(C) de l'EO 14086.

([297]) Article 2(c)(iii)(A)(2)(a) à (c) de l'EO 14086. Plus généralement, chaque agence doit mettre en place des politiques et des procédures visant à réduire autant que possible la diffusion et la conservation des données à caractère personnel collectées au moyen de renseignements d'origine électromagnétique [article 2(c)(iii)(A) de l'EO 14086].

([298]) Voir par exemple l'article 309 de la loi «Intelligence Authorization Act For Fiscal Year 2015»; les procédures de minimisation adoptées par les différentes agences de renseignement au titre de l'article 702 du FISA et autorisées par le FISC; les procédures approuvées par le procureur général et le FRA (obligeant les agences fédérales américaines, y compris les agences de sécurité nationale, à fixer des durées de conservation pour leurs archives qui doivent être approuvées par la National Archives and Record Administration).

([299]) Article 2(c)(iii)(A)(1)(a) et article 5(d) de l'EO 14086, en liaison avec l'article 2.3 de l'EO 12333.

([300]) Article 2(c)(iii)(A)(1)(b) et (e) de l'EO 14086.

que si une personne autorisée et formée a un motif sérieux de croire que le destinataire a besoin de connaître les informations ([301]) et qu'il les protégera de manière appropriée ([302]). Pour déterminer si des données à caractère personnel peuvent être diffusées à des destinataires extérieurs au gouvernement américain (notamment un gouvernement étranger ou une organisation internationale), il convient de tenir compte de l'objectif de la diffusion, de la nature et de l'étendue des données diffusées, ainsi que du préjudice potentiel pour la ou les personnes concernées ([303]).

(159) Enfin, afin de faciliter le contrôle du respect des exigences légales applicables et d'offrir des voies de recours efficaces, chaque agence de renseignement est tenue en vertu de l'EO 14086 de conserver une documentation appropriée sur la collecte de renseignements d'origine électromagnétique. Les exigences en matière de documentation couvrent des éléments tels que la base factuelle de l'évaluation selon laquelle une activité de collecte spécifique est nécessaire pour faire progresser une priorité validée en matière de renseignement ([304]).

(160) Outre les garanties susmentionnées de l'EO 14086 en ce qui concerne l'utilisation des informations collectées au moyen de renseignements d'origine électromagnétique, toutes les agences de renseignement américaines sont soumises à des exigences plus générales en matière de limitation des finalités, de minimisation des données, d'exactitude, de sécurité, de conservation et de diffusion, découlant notamment de la circulaire n° A-130 de l'OMB, de la loi sur l'administration en ligne (E-Government Act), du Federal Records Act (voir considérants 101 à 106) et des orientations du comité des systèmes de sécurité nationale (CNSS) ([305]).

3.2.2. ***Surveillance***

(161) Les activités des agences de renseignement américaines font l'objet d'une surveillance de la part de différents organismes.

(162) Tout d'abord, l'EO 14086 exige que chaque agence de renseignement dispose de responsables juridiques et de délégués chargés de la surveillance et du respect des règles de haut niveau afin de garantir le respect du droit américain applicable ([306]). En particulier, ils doivent surveiller régulièrement les activités de renseignement d'origine électromagnétique et veiller à ce que tout cas de non-respect soit corrigé. Les agences de renseignement doivent donner à ces responsables l'accès à toutes les informations pertinentes pour l'exercice de leurs fonctions et ne peuvent prendre aucune mesure pour entraver ou influencer indûment leurs activités de surveillance ([307]). En outre, tout cas de non-respect significatif ([308]) constaté par un délégué chargé de la surveillance ou toute autre personne doit être rapidement signalé au chef de l'agence de renseignement et au directeur du renseignement national, qui doivent veiller à ce que toutes les mesures nécessaires soient prises pour corriger ce cas et empêcher qu'il ne se reproduise ([309]).

(163) Cette fonction de surveillance est assurée par des délégués ayant un rôle désigné en matière de respect des règles, ainsi que par des délégués à la protection de la vie privée et des libertés civiles et des inspecteurs généraux ([310]).

([301]) Voir, par exemple, l'AGG-DOM, qui prévoit notamment que le FBI ne peut diffuser des informations que si le destinataire a besoin d'en connaître pour accomplir sa mission ou pour protéger le public.

([302]) Article 2(c)(iii)(A)(1)(c) de l'EO 14086. Les services de renseignement peuvent, par exemple, diffuser des informations dans des circonstances pertinentes pour une enquête pénale ou en lien avec une infraction, y compris, par exemple, en diffusant des avertissements concernant des menaces de meurtre, de blessure corporelle grave ou d'enlèvement; diffuser des informations sur la réponse à une cybermenace, à un incident ou à une intrusion; et informer des victimes ou avertir des victimes potentielles d'actes criminels.

([303]) Article 2(c)(iii)(A)(1)(d) de l'EO 14086.

([304]) Article 2(c)(iii)(E) de l'EO 14086.

([305]) Voir la politique du CNSS n° 22, Politique de gestion des risques de cybersécurité et instruction 1253 du CNSS, qui fournit des orientations détaillées sur les mesures de sécurité à mettre en place pour les systèmes de sécurité nationaux.

([306]) Article 2(d)(i)(A) et (B) de l'EO 14086.

([307]) Article 2(d)(i)(B) et (C) de l'EO 14086.

([308]) C'est-à-dire un manquement systémique ou intentionnel au droit américain applicable qui pourrait porter atteinte à la réputation ou à l'intégrité d'une composante de la communauté du renseignement ou remettre en question le bien-fondé d'une activité de la communauté du renseignement, notamment à la lumière de toute incidence significative sur la vie privée et les libertés civiles de la personne ou des personnes concernées, voir article 5(1) de l'EO 14086.

([309]) Article 2(d)(iii) de l'EO 14086.

([310]) Article 2(d)(i)(B) de l'EO 14086.

(164) Comme c'est le cas en ce qui concerne les autorités répressives, des délégués à la protection de la vie privée et des libertés civiles sont en place dans toutes les agences de renseignement ([311]). Les pouvoirs de ces délégués englobent généralement la surveillance des procédures permettant de veiller à ce que le service concerné/l'agence concernée prenne en compte de façon adéquate les problèmes touchant à la vie privée et aux libertés civiles et ait mis en place des procédures appropriées pour traiter les réclamations émanant de personnes qui estiment que leur vie privée ou les libertés civiles ont été violées (et, dans certains cas, à l'instar de l'ODNI, ces délégués peuvent eux-mêmes avoir le pouvoir d'enquêter sur des réclamations) ([312]). Les chefs de service ou de l'agence doivent veiller à ce que les délégués à la protection des libertés civiles et de la vie privée disposent des ressources nécessaires à l'accomplissement de leur mandat, se voient accorder l'accès à tous les documents et au personnel nécessaires pour pouvoir s'acquitter de leurs fonctions et soient informés et consultés sur les changements de politique proposés ([313]). Les délégués à la protection des libertés civiles et de la vie privée font régulièrement rapport au Congrès et au PCLOB, notamment sur le nombre et la nature des réclamations par le service/l'agence, les informent succinctement du sort réservé à ces réclamations, et les renseignent sur les examens et les enquêtes effectués ainsi que sur l'impact des activités menées par le délégué ([314]).

(165) Deuxièmement, chaque agence de renseignement compte un inspecteur général indépendant chargé, entre autres, de contrôler les activités de renseignement extérieur. Se trouve ainsi, au sein de l'ODNI, un bureau de l'inspecteur général de la communauté du renseignement doté de vastes attributions en ce qui concerne l'ensemble des services de renseignement qui est habilité à enquêter sur les réclamations ou les informations concernant des allégations de comportement infractionnel ou d'abus d'autorité, en relation avec des programmes et des activités de l'ODNI et/ou des programmes des services de renseignement ([315]). Comme c'est le cas pour les autorités répressives (voir considérant 109), ces inspecteurs généraux sont des entités dont l'indépendance est inscrite dans la loi ([316]); ils sont chargés d'effectuer des audits et des enquêtes sur les activités et programmes menés par l'agence concernée à des fins de renseignement national, y compris en ce qui concerne des abus ou une violation du droit ([317]). Ils ont accès à

([311]) Voir 42 U.S.C. § 2000ee-1. Il s'agit notamment du Département d'État, du ministère de la justice, du ministère de la sécurité intérieure, du ministère de la défense, de la NSA, de la CIA, du FBI et de l'ODNI.

([312]) Voir article 3(c) de l'EO 14086.

([313]) 42 U.S.C. § 2000ee-1(d).

([314]) Voir 42 U.S.C. § 2000ee-1.(f)(1) et (2). Par exemple, le rapport du bureau de la transparence, de la protection de la vie privée et des libertés civiles de la NSA couvrant la période allant de janvier à juin 2021 indique qu'il a effectué 591 examens des incidences sur les libertés civiles et la vie privée dans divers contextes, par exemple en ce qui concerne les activités de collecte, les accords et décisions de partage d'informations, les décisions de conservation des données, etc., en tenant compte de différents facteurs, tels que la quantité et le type d'informations liées à l'activité, les personnes concernées, l'objectif et l'utilisation prévue des données, les garanties en place pour atténuer les risques potentiels pour la vie privée, etc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). De même, les rapports du bureau des libertés civiles et de la vie privée de la CIA pour la période allant de janvier à juin 2019 fournissent des informations sur les activités de surveillance du bureau, par exemple un examen de la conformité avec les lignes directrices du procureur général au titre de l'EO 12333 en ce qui concerne la conservation et la diffusion des informations, les conseils fournis sur la mise en œuvre de la PPD-28 et les exigences visant à recenser et à traiter les cas de violation de données, ainsi que des examens de l'utilisation et du traitement des informations à caractère personnel (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Cet inspecteur général est nommé par le président, et sa nomination est entérinée par le Sénat; il ne peut être révoqué que par le président.

([316]) Les inspecteurs généraux sont inamovibles; ils ne peuvent être révoqués que par le président qui doit informer par écrit le Congrès des motifs de cette révocation. Cela ne signifie pas nécessairement qu'ils ne doivent recevoir aucune instruction. Dans certains cas, le responsable du service peut interdire à l'inspecteur général d'entamer et d'effectuer ou de mener à terme un audit ou une enquête lorsque cela est jugé nécessaire pour préserver d'importants intérêts nationaux (de sécurité). Le Congrès doit toutefois être informé de l'exercice de ce pouvoir et pourrait, sur cette base, tenir pour responsable le directeur respectif. Voir par ex. loi sur l'inspecteur général de 1978, § 8 (pour le ministère de la défense); § 8E (pour le ministère de la justice); § 8G (d)(2)(A),(B) (pour la NSA); 50. U.S.C. § 403q(b) (pour la CIA); et l'Intelligence Authorization Act For Fiscal Year 2010, article 405(f) (pour la communauté du renseignement).

([317]) Loi sur l'inspecteur général (Inspector General Act) de 1978, telle que modifiée, pub. L. 117-108 du 8 avril 2022. Par exemple, comme expliqué dans ses rapports semestriels au Congrès couvrant la période du 1er avril 2021 au 31 mars 2022, l'inspecteur général de la NSA a procédé à des évaluations du traitement des informations sur les ressortissants américains collectées au titre de l'EO 12333, de la procédure d'élimination des données de renseignement d'origine électromagnétique, d'un outil de ciblage automatisé utilisé par la NSA et du respect des règles de documentation et d'interrogation des données en ce qui concerne la collecte au titre de l'article 702 du FISA, et a formulé plusieurs recommandations dans ce contexte (voir https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, p. 5 à 8, et https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, p. 10 à 13). Voir également les récents audits et enquêtes menés par l'inspecteur général de la communauté du renseignement sur la sécurité de l'information et les divulgations non autorisées d'informations classifiées relatives à la sécurité nationale (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, p. 8, 11 et https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, p. 19 et 20).

l'ensemble des archives, rapports, audits, réexamens, documents, recommandations ou à tout autre matériel pertinent, si nécessaire au moyen d'une ordonnance, et ils peuvent recueillir des témoignages ([318]). Les inspecteurs généraux signalent les cas d'infractions pénales présumées à des fins de poursuites et formulent des recommandations sur l'adoption de mesures correctives à l'intention des chefs d'agence ([319]). Si leurs recommandations sont non contraignantes, leurs rapports, notamment sur les mesures de suivi (ou leur absence) ([320]) sont généralement rendus publics et transmis au Congrès qui peut, sur cette base, exercer sa propre fonction de contrôle (voir considérants 168 et 169) ([321]).

(166) Troisièmement, le conseil de surveillance du renseignement (Intelligence Oversight Board, IOB), qui est créé au sein du conseil consultatif en matière de renseignement relevant du président (President's Intelligence Advisory Board, PIAB), supervise le respect par les autorités américaines de renseignement de la Constitution et de toutes les règles applicables. Le PIAB est un organe consultatif au sein du bureau exécutif du président ([322]). Il est composé de 16 membres nommés par le président et ne faisant pas partie du gouvernement américain. L'IOB est composé d'un maximum de cinq membres désignés par le président parmi les membres du PIAB. En vertu de l'EO 12333 ([323]), les chefs de toutes les agences de renseignement sont tenus de signaler à l'IOB toute activité de renseignement dont ils ont des raisons de croire qu'elle pourrait être illégale ou contraire à un décret ou à une directive présidentielle. Afin de garantir que l'IOB a accès aux informations nécessaires à l'exercice de ses fonctions, le décret présidentiel n° 13462 (Executive Order 13462, ci-après l'«EO 13462») ordonne au directeur du renseignement national et aux chefs des agences de renseignement de fournir toutes les informations et l'assistance que l'IOB juge nécessaires à l'exercice de ses fonctions, dans la mesure où la loi l'autorise ([324]). L'IOB est à son tour tenu d'informer le président des activités de renseignement dont il estime qu'elles peuvent constituer une violation du droit américain (notamment des décrets) et qu'elles ne sont pas traitées de manière appropriée par le procureur général, le directeur du renseignement national ou le chef d'une agence de renseignement ([325]). En outre, l'IOB est tenu d'informer le procureur général d'éventuelles violations du droit pénal.

(167) Quatrièmement, les agences de renseignement sont soumises au contrôle du PCLOB. Selon son statut fondateur, le PCLOB est investi de responsabilités dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre, en vue de protéger la vie privée et les libertés civiles. Dans le cadre de son examen des activités des agences de renseignement, il peut avoir accès à l'ensemble des archives, rapports, audits, analyses, documents, pièces et recommandations pertinents, notamment aux informations classifiées, mener des entretiens et recueillir des témoignages ([326]). Il reçoit des rapports des délégués à la protection des libertés civiles et de la vie privée de plusieurs agences/organes fédéraux ([327]); il peut adresser des recommandations aux autorités gouvernementales et répressives et fait régulièrement rapport aux commissions du Congrès et au président ([328]). Les rapports du PCLOB, y compris ceux destinés au Congrès, doivent être rendus publics dans la mesure la plus large possible ([329]). Le PCLOB a publié plusieurs rapports de surveillance et de suivi, notamment une analyse des programmes menés sur la base de l'article 702 du FISA et de la protection de la vie privée dans ce contexte, de la mise en œuvre de la PPD-28 et de l'EO 12333 ([330]). Le PCLOB est également chargé d'exercer des fonctions de surveillance spécifiques en

([318]) Voir la loi sur l'inspecteur général de 1978 (Inspector General Act), § 6.

([319]) Voir ibidem, §§ 4, 6 et 5.

([320]) En ce qui concerne le suivi des rapports et des recommandations des inspecteurs généraux, voir par exemple la réponse à un rapport de l'inspecteur général du ministère de la justice qui a constaté que le FBI n'était pas suffisamment transparent avec le FISC dans les demandes de 2014 à 2019, ce qui a donné lieu à des réformes pour améliorer le respect des règles, la surveillance et la responsabilité au sein du FBI (par exemple, le directeur du FBI a ordonné plus de 40 mesures correctives, dont 12 spécifiques à la procédure du FISA concernant la documentation, la surveillance, la tenue des dossiers, la formation et les audits) (voir https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance et https://oig.justice.gov/reports/2019/o20012.pdf). Voir également, par exemple, l'audit de l'inspecteur général du ministère de la justice sur les rôles et les responsabilités du bureau du contentieux du FBI en matière de contrôle du respect des lois, des politiques et des procédures applicables aux activités du FBI en matière de sécurité nationale, ainsi que l'annexe 2, qui comprend une lettre du FBI acceptant toutes les recommandations. À cet égard, l'annexe 3 donne un aperçu des mesures de suivi et des informations que l'inspecteur général a exigées du FBI pour pouvoir classer définitivement ses recommandations (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Voir la loi sur l'inspecteur général de 1978 (Inspector General Act), §§ 4(5), 5.

([322]) Voir EO 13462.

([323]) Article 1.6(c) de l'EO 12333.

([324]) Article 8(a) de l'EO 13462.

([325]) Article 6(b) de l'EO 13462.

([326]) 42 U.S.C. § 2000ee (g).

([327]) Voir 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Ceux-ci englobent au moins le ministère de la justice, le ministère de la défense, le ministère de la sécurité intérieure, le directeur du renseignement national et l'Agence centrale de renseignement, ainsi que tout autre service, agence ou entité du pouvoir exécutif désigné par le PCLOB comme adéquats pour les examens considérés.

([328]) 42 U.S.C. § 2000ee (e).

([329]) 42 U.S.C. § 2000ee (f).

([330]) Consultable à l'adresse suivante: https://www.pclob.gov/Oversight.

ce qui concerne la mise en œuvre de l'EO 14086, notamment en vérifiant si les procédures des agences sont conformes au décret (voir considérant 126) et en évaluant le fonctionnement correct du mécanisme de recours (voir considérant 194).

(168) Cinquièmement, outre ces mécanismes de contrôle au sein du pouvoir exécutif, des commissions spéciales au sein du Congrès américain (les commissions du renseignement et judiciaires de la Chambre des représentants et du Sénat) exercent des responsabilités de surveillance à l'égard de toutes les activités du renseignement extérieur américain. Les membres de ces commissions ont accès à des informations classifiées et aux méthodes et programmes de renseignement ([331]). Les commissions exercent leurs fonctions de surveillance de différentes manières, notamment au moyen d'auditions, d'enquêtes, d'examens et de rapports ([332]).

(169) Les commissions du Congrès reçoivent des rapports réguliers sur les activités de renseignement, notamment de la part du procureur général, du directeur du renseignement national, des agences de renseignement et d'autres organes de surveillance (par exemple, les inspecteurs généraux), voir considérants 164 et 165. En particulier, d'après la loi sur la sécurité nationale, «[l]e Président veille à ce que les commissions du renseignement du Congrès soient pleinement et régulièrement informées des activités de renseignement des États-Unis, notamment de toute activité importante de renseignement anticipée conformément au présent sous-chapitre» ([333]). De plus, «[l]e Président veille à ce que toute activité de renseignement illégale soit rapportée rapidement aux commissions du renseignement du Congrès, ainsi que toute mesure corrective qui a été prise ou est prévue en lien avec lesdites activités» ([334]).

(170) En outre, des obligations de rendre compte supplémentaires découlent de certaines lois. En particulier, le FISA exige que le procureur général «informe pleinement» les commissions du renseignement et judiciaires de la Chambre et du Sénat au sujet des activités du gouvernement relevant de certains de ses articles ([335]). Elle impose en outre au gouvernement d'adresser aux commissions du Congrès un exemplaire de chaque décision, ordonnance ou avis émis par le FISC ou la FISCR, contenant «une interprétation ou une explication du sens ou de l'intention» des dispositions du FISA. En ce qui concerne le contrôle visé à l'article 702 du FISA, la surveillance parlementaire est exercée au moyen d'une obligation légale de rapports destinés aux commissions du renseignement et judiciaires, et de l'utilisation fréquente de briefings et d'auditions. Il s'agit notamment d'un rapport semestriel du procureur général décrivant l'utilisation de l'article 702 du FISA, accompagné de documents justificatifs comme les rapports du ministère de la justice et de l'ODNI sur le respect des normes et d'une description de tous les cas de non-respect ([336]), et d'une évaluation semestrielle séparée présentée par le procureur général et le DNI afin de démontrer le respect des procédures de ciblage et de minimisation ([337]).

([331]) 50 U.S.C. § 3091.

([332]) Par exemple, les commissions organisent des auditions thématiques (voir par exemple une récente audition de la commission judiciaire de la Chambre des représentants sur les «filets numériques», https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, et une audition de la commission du renseignement de la Chambre des représentants sur l'utilisation de l'IA par la communauté du renseignement, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), ainsi que des auditions de contrôle régulières, par exemple du FBI et de la division de la sécurité nationale du ministère de la justice, voir https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 et https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Pour un exemple d'enquête, voir l'enquête de la commission du renseignement du Sénat sur l'ingérence de la Russie dans les élections américaines de 2016, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. En ce qui concerne les rapports, voir par exemple la vue d'ensemble des activités (de surveillance) de la commission dans le rapport de la commission du renseignement du Sénat couvrant la période du 4 janvier 2019 au 3 janvier 2021 au Sénat, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Voir 50 U.S.C. § 3091(a)(1). Cette disposition contient les exigences générales concernant la surveillance incombant au Congrès en matière de sécurité nationale.

([334]) Voir 50 U.S.C. § 3091(b).

([335]) Voir 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([336]) Voir 50 U.S.C. § 1881f.

([337]) Voir 50 U.S.C. § 1881a(l)(1).

(171) En outre, le FISA exige du gouvernement américain qu'il communique au Congrès (et au grand public) chaque année le nombre d'ordonnances et de directives demandées et obtenues au titre du FISA, ainsi que des estimations du nombre de personnes, américaines ou non, visées par la surveillance, entre autres ([338]). Cet acte législatif exige également par ailleurs la communication publique d'informations sur le nombre de lettres de sécurité nationale (LSN) émises, concernant là aussi des personnes américaines ou non (tout en permettant aux destinataires des ordonnances et certifications FISA, et des demandes liées aux LSN, de publier des rapports de transparence sous certaines conditions) ([339]).

(172) Plus généralement, la communauté du renseignement des États-Unis entreprend divers efforts pour assurer la transparence de ses activités de renseignement (étranger). En 2015, par exemple, l'ODNI a adopté des principes de transparence en matière de renseignement et un plan de mise en œuvre de la transparence, et a demandé à chaque agence de renseignement de désigner un responsable de la transparence en matière de renseignement chargé de favoriser la transparence et de mener des initiatives dans ce domaine ([340]). Dans le cadre de ces initiatives, la communauté du renseignement a rendu et continue de rendre publiques des parties déclassifiées de politiques, de procédures, de rapports de surveillance, de rapports sur les activités menées au titre de l'article 702 du FISA et de l'EO 12333, de décisions du FISC et d'autres documents, notamment sur une page web spécifique intitulée «IC on the Record», gérée par l'ODNI ([341]).

(173) Enfin, la collecte de données à caractère personnel en vertu de l'article 702 du FISA fait l'objet, en plus du contrôle exercé par les organes de surveillance mentionnés aux considérants 162 à 168, d'une surveillance de la part du FISC ([342]). Conformément à l'article 13 du règlement intérieur du FISC, les délégués chargés du respect des règles des agences de renseignement américaines sont tenus de signaler toute violation des procédures de ciblage, de minimisation et d'interrogation de données de l'article 702 du FISA au ministère de la justice et à l'ODNI, qui les signalent à leur tour au FISC. En outre, le ministère de la justice et l'ODNI présentent au FISC des rapports semestriels d'évaluation conjointe de la surveillance, qui recensent les cas de non-respect des procédures de ciblage; fournissent des données statistiques; définissent les catégories de cas de non-respect; décrivent en détail les raisons pour lesquelles certains cas de non-respect des procédures de ciblage se sont produits et exposent les mesures prises par les agences de renseignement pour éviter qu'ils ne se reproduisent ([343]).

(174) Si nécessaire (par exemple si des violations des procédures de ciblage sont constatées), le FISC peut ordonner à l'agence de renseignement compétente de prendre des mesures correctives ([344]). Les mesures en question 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 ([345]). En outre, lors de son

([338]) 50 U.S.C. § 1873(b). En outre, selon l'article 402, «le directeur du renseignement national, en collaboration avec le procureur général, procède à un examen de déclassification de chaque décision, ordonnance ou avis émis par le tribunal de la surveillance du renseignement extérieur ou la FISCR [telle que définie à l'article 601(e)], contenant une interprétation ou une explication du sens ou de l'intention d'une disposition légale, y compris une interprétation ou explication nouvelle de l'expression «critère de sélection spécifique» et, en conformité avec cette révision, mettra à la disposition du public dans la mesure la plus large possible la décision, l'ordonnance ou l'avis en question».

([339]) 50 U.S.C. §§ 1873(b)(7) et 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Voir page web intitulée «IC on the Record», accessible à l'adresse suivante: https://icontherecord.tumblr.com/.

([342]) Par le passé, le FISC a conclu que «[i]l est évident pour le tribunal que les agences chargées de la mise en œuvre, ainsi que [l'ODNI] et [la division de la sécurité nationale du ministère de la justice], consacrent des ressources substantielles à leurs responsabilités en matière de respect des règles et de surveillance au titre de l'article 702. En règle générale, les cas de non-respect sont détectés rapidement et des mesures correctives appropriées sont prises, notamment l'élimination des informations obtenues de manière illicite ou soumises à des exigences de destruction en vertu des procédures applicables». Tribunal FISA, Memorandum Opinion and Order [légende expurgée] (2014), consultable à l'adresse suivante: https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Voir, par exemple, DOJ/ODNI, rapport de vérification de la conformité avec l'article 702 du FISA pour la période allant de juin 2018 à novembre 2018, p. 21 à 65.

([344]) 50 U.S.C. § 1803(h). Voir également PCLOB, rapport sur l'article 702, p. 76. En outre, voir FISC, Memorandum Opinion and Order du 3 octobre 2011 en tant qu'exemple d'une ordonnance de manquement dans laquelle le gouvernement a reçu l'ordre de corriger les manquements constatés dans un délai de 30 jours. Consultable à l'adresse suivante: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Voir Lettre Walton, section 4, p. 10 et 11. Voir également avis du FISC du 18 octobre 2018, consultable à l'adresse suivante: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, tel qu'il est confirmé par la FISCR dans son avis du 12 juillet 2019, consultable à l'adresse suivante: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, dans lequel le FISC a notamment ordonné au gouvernement de se conformer à certaines exigences en matière de notification, de documentation et de rapport au FISC.

([345]) Voir, par exemple, FISC, Memorandum Opinion and Order at 76 (6 décembre 2019) (publication autorisée le 4 septembre 2020), dans lequel le FISC a demandé au gouvernement de présenter un rapport écrit avant le 28 février 2020 sur les mesures prises par le gouvernement pour améliorer les processus d'identification et de suppression des rapports tirés des informations FISA 702 qui ont été rappelés pour des raisons de conformité, ainsi que sur d'autres questions. Voir également annexe VII.

examen annuel des certifications au titre de l'article 702 du FISA, le FISC examine les cas de non-respect afin de déterminer si les certifications soumises sont conformes aux exigences du FISA. De même, si le FISC estime que les certifications du gouvernement ne sont pas suffisantes, notamment en raison de cas de non-respect particuliers, il peut délivrer un «deficiency order» (ordonnance de manquement) exigeant du gouvernement qu'il remédie à la violation dans un délai de 30 jours ou qu'il cesse ou n'entame pas la mise en œuvre de la certification au titre de l'article 702. Enfin, le FISC évalue les problèmes de conformité qu'il constate et peut exiger des changements de procédure ou une surveillance et des rapports supplémentaires pour résoudre ces problèmes ([346]).

3.2.3. ***Recours***

(175) Comme expliqué plus en détail dans la présente section, un certain nombre de voies aux États-Unis offrent aux personnes concernées de l'Union la possibilité d'intenter une action en justice devant un tribunal indépendant et impartial doté de pouvoirs contraignants. Ensemble, elles permettent aux personnes d'avoir accès à leurs données à caractère personnel, de faire contrôler la licéité de l'accès des pouvoirs publics à leurs données et, si une violation est constatée, d'y remédier, notamment par la rectification ou la suppression de leurs données à caractère personnel.

(176) Premièrement, un mécanisme de recours spécifique est mis en place, en vertu de l'EO 14086, complété par le règlement AG instituant la Cour chargée du contrôle de la protection des données, afin de traiter et de résoudre les réclamations déposées par des personnes concernant les activités de renseignement d'origine électromagnétique des États-Unis. Toute personne concernée dans l'Union a le droit d'introduire une réclamation auprès du mécanisme de recours concernant une violation présumée du droit américain régissant les activités de renseignement d'origine électromagnétique (par exemple, l'EO 14086, l'article 702 du FISA, l'EO 12333) qui porte atteinte à ses intérêts en matière de protection de la vie privée et de libertés civiles ([347]). Ce mécanisme de recours en matière de renseignements d'origine électromagnétique est accessible aux personnes originaires de pays ou d'organisations régionales d'intégration économique qui ont été désignés par le procureur général des États-Unis comme des «États admissibles» ([348]). Le 30 juin 2023, l'Union européenne et les trois pays de l'Association européenne de libre-échange, qui constituent ensemble l'Espace économique européen, ont été désignés comme «État admissible» par le procureur général des États-Unis en vertu de l'article 3(f) de l'EO 14086 ([349]). Cette désignation est sans préjudice de l'article 4, paragraphe 2, du traité sur l'Union européenne.

(177) Une personne concernée dans l'Union qui souhaite introduire une telle réclamation doit la soumettre à une autorité de contrôle d'un État membre chargée de la surveillance du traitement des données à caractère personnel par les autorités publiques (APD) ([350]). Cela garantit un accès facile au mécanisme de recours en permettant aux personnes concernées de s'adresser à une autorité géographiquement proche et avec laquelle elles peuvent communiquer dans leur langue. Après vérification des exigences relatives au dépôt d'une réclamation visées au considérant 178, l'APD compétente transmettra, par l'intermédiaire du secrétariat du comité européen de la protection des données, la réclamation au mécanisme de recours.

(178) L'introduction d'une réclamation auprès du mécanisme de recours est soumise à de faibles conditions de recevabilité, car les personnes concernées ne sont pas tenues de démontrer que leurs données ont effectivement fait l'objet d'activités de renseignement d'origine électromagnétique de la part des États-Unis ([351]). Dans le même temps, afin de donner un point de départ au mécanisme de recours pour effectuer un examen, certaines informations de base doivent être fournies, par exemple en ce qui concerne les données à caractère personnel dont il est raisonnable de penser qu'elles ont été transférées vers les États-Unis et les moyens par lesquels on peut penser qu'elles ont été transférées; l'identité des entités du gouvernement américain soupçonnées d'être impliquées dans la violation présumée (si elle est connue); le fondement de la violation présumée du droit américain (bien que, là encore, il ne soit pas nécessaire de démontrer que les données à caractère personnel ont effectivement été collectées par les agences de renseignement américaines) et la nature de la réparation demandée.

([346]) Voir annexe VII.

([347]) Voir article 4(k)(iv) de l'EO 14086, qui prévoit qu'une plainte auprès du mécanisme de recours doit être déposée par un plaignant agissant en son nom propre (c'est-à-dire pas en tant que représentant d'un gouvernement, d'une organisation non gouvernementale ou intergouvernementale). La notion d'«affecté» n'exige pas que le plaignant atteigne un certain seuil pour avoir accès au mécanisme de recours (voir le considérant 178 à cet égard). Elle précise plutôt que l'ODNI CLPO et la DPRC ont le pouvoir de remédier aux violations du droit américain régissant les activités de renseignement d'origine électromagnétique qui affectent la vie privée et les intérêts des libertés civiles d'un plaignant. À l'inverse, les violations des exigences du droit américain applicable qui ne visent pas à protéger les personnes concernées (par exemple, les exigences budgétaires) ne relèveraient pas de la compétence de l'ODNI CLPO ni de la DPRC.

([348]) Article 3(f) de l'EO 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Article 4(d)(v) de l'EO 14086.

([351]) Voir article 4(k)(i)-iv) de l'EO 14086.

(179) L'enquête initiale sur les réclamations déposées auprès de ce mécanisme de recours est menée par l'ODNI CLPO, dont le rôle et les pouvoirs statutaires existants ont été étendus aux mesures spécifiques prises en vertu de l'EO 14086 ([352]). Au sein de la communauté du renseignement, le CLPO est notamment chargé de veiller à ce que la protection des libertés civiles et de la vie privée soit intégrée de manière appropriée dans les politiques et procédures de l'ODNI et des agences de renseignement; de veiller à ce que l'ODNI respecte les exigences applicables en matière de protection de la vie privée et des libertés civiles; et de procéder à des analyses des incidences sur la vie privée ([353]). L'ODNI CLPO ne peut être démis de ses fonctions que par le directeur du renseignement national pour un motif valable, c'est-à-dire en cas d'action fautive, de faute de commission, d'atteinte à la sécurité, de négligence ou d'incapacité ([354]).

(180) Lors de son examen, l'ODNI CLPO a accès aux informations nécessaires à son évaluation et peut compter sur l'assistance obligatoire des délégués à la protection de la vie privée et des libertés civiles des différentes agences de renseignement ([355]). Il est interdit aux agences de renseignement d'entraver ou d'influencer indûment les examens de l'ODNI CLPO. Cela inclut le directeur du renseignement national, qui ne doit pas entraver l'examen ([356]). Lorsqu'il examine une plainte, l'ODNI CLPO doit appliquer la loi «de manière impartiale», en tenant compte à la fois des intérêts de sécurité nationale concernant les activités de renseignement et de la protection de la vie privée ([357]).

(181) Dans le cadre de son examen, l'ODNI CLPO détermine s'il y a eu violation du droit américain applicable et, le cas échéant, décide d'une mesure corrective appropriée ([358]). Il s'agit de mesures qui remédient pleinement à une violation constatée, telles que la cessation de l'obtention illicite de données, la suppression des données collectées illégalement, la suppression des résultats d'interrogations inappropriées de données par ailleurs collectées de manière légale, la limitation de l'accès à des données collectées de manière légale à du personnel dûment formé, ou le rappel des rapports de renseignement contenant des données acquises sans autorisation légale ou qui ont été diffusées de manière illégale ([359]). Les décisions de l'ODNI CLPO sur les réclamations individuelles (y compris sur les mesures correctives) sont contraignantes pour les agences de renseignement concernées ([360]).

(182) L'ODNI CLPO doit conserver la documentation relative à son examen et publier une décision classifiée expliquant le fondement de ses constatations factuelles, l'établissement de l'existence d'une violation couverte et le choix de la mesure corrective appropriée ([361]). Si l'examen de l'ODNI CLPO révèle une violation commise par une autorité faisant l'objet d'une surveillance de la part du FISC, le CLPO doit également fournir un rapport classifié à l'assistant du procureur général chargé de la sécurité nationale, qui est à son tour tenu de signaler le non-respect au FISC, qui peut prendre d'autres mesures répressives (conformément à la procédure décrite aux considérants 173 et 174) ([362]).

(183) Une fois l'examen terminé, l'ODNI CLPO informe le plaignant, par l'intermédiaire de l'autorité nationale, que «l'examen n'a pas mis en évidence de violations couvertes ou que l'ODNI CLPO a rendu une décision exigeant des mesures correctives appropriées» ([363]). Cela permet de protéger la confidentialité des activités menées afin de protéger la sécurité nationale, tout en fournissant aux personnes concernées une décision confirmant que leur réclamation a été dûment examinée et jugée. Cette décision peut d'ailleurs être contestée par la personne concernée. À cette fin, il/elle sera informé(e) de la possibilité de faire appel auprès de la DPRC pour un réexamen des décisions du CLPO (voir considérants 184 et suivants) et du fait que, dans le cas où la Cour serait saisie, un avocat spécial sera sélectionné pour défendre les intérêts du plaignant ([364]).

([352]) Article 3(c)(iv) de l'EO 14086. Voir également la loi sur la sécurité nationale de 1947, 50 U.S.C. § 403-3d, article 103D concernant le rôle du CLPO au sein de l'ODNI.
([353]) 50 U.S.C § 3029(b).
([354]) Article 3(c)(iv) de l'EO 14086.
([355]) Article 3(c)(iii) de l'EO 14086.
([356]) Article 3(c)(iv) de l'EO 14086.
([357]) Article 3(c)(i)(B)(i) et (iii) de l'EO 14086.
([358]) Article 3(c)(i) de l'EO 14086.
([359]) Article 4(a) de l'EO 14086.
([360]) Article 3(c)(d) de l'EO 14086.
([361]) Article 3(c)(i)(F) et (G) de l'EO 14086.
([362]) Voir également l'article 3(c)(i)(D) de l'EO 14086.
([363]) Article 3(c)(i)(E)(i) de l'EO 14086.
([364]) Article 3(c)(i)(E)(2) et (3) de l'EO 14086.

(184) Tout plaignant, ainsi que chaque composante de la communauté du renseignement, peut demander le réexamen de la décision de l'ODNI CLPO devant la Cour chargée du contrôle de la protection des données (DPRC). Ces demandes de réexamen doivent être soumises dans les 60 jours suivant la réception de la notification de l'ODNI CLPO indiquant que son examen est terminé et inclure toute information que la personne concernée souhaite communiquer à la DPRC (par exemple, des arguments sur des questions de droit ou sur l'application du droit aux circonstances de l'espèce) ([365]). Les personnes concernées de l'Union peuvent à nouveau soumettre leur demande à l'APD compétente (voir considérant 177).

(185) La DPRC est un tribunal indépendant établi par le procureur général sur la base de l'EO 14086 ([366]). Elle est composée d'au moins six juges, nommés par le procureur général en consultation avec le PCLOB, le secrétaire d'État américain au commerce et le directeur du renseignement national pour des mandats renouvelables de quatre ans ([367]). La nomination des juges par le procureur général s'appuie sur les critères utilisés par le pouvoir exécutif pour évaluer les candidats à la magistrature fédérale, en tenant compte de leur expérience judiciaire antérieure ([368]). En outre, les juges doivent être des praticiens du droit (c'est-à-dire des membres actifs en règle du barreau et dûment autorisés à pratiquer le droit) et avoir une expérience appropriée en matière de droit de la protection de la vie privée et de la sécurité nationale. Le procureur général doit veiller à ce qu'au moins la moitié des juges aient une expérience judiciaire antérieure et tous les juges doivent être titulaires d'une habilitation de sécurité afin de pouvoir accéder à des informations classifiées relatives à la sécurité nationale ([369]).

(186) Seules les personnes qui satisfont aux qualifications mentionnées au considérant 185 et qui ne sont pas employées du pouvoir exécutif au moment de leur nomination ou ne l'ont pas été au cours des deux années précédentes peuvent être nommées à la DPRC. De même, pendant la durée de leur mandat à la DPRC, les juges ne peuvent exercer aucune fonction officielle ni aucun emploi au sein du gouvernement des États-Unis (autre que celui de juge à la DPRC) ([370]).

(187) L'indépendance du processus de sélection est assurée par un certain nombre de garanties. En particulier, il est interdit au pouvoir exécutif (le procureur général et les agences de renseignement) d'entraver ou d'influencer indûment l'examen de la DPRC ([371]). La DPRC elle-même est tenue de statuer de manière impartiale ([372]) et fonctionne selon son propre règlement intérieur (adopté à la majorité). En outre, les juges de la DPRC ne peuvent être révoqués que par le procureur général et uniquement pour un motif valable (action fautive, faute de commission, atteinte à la sécurité, négligence ou incapacité), après avoir dûment pris en compte les normes applicables aux juges fédéraux énoncées dans les règles relatives à la déontologie judiciaire et à la procédure d'incapacité judiciaire ([373]).

([365]) Article 201.6(a) et (b) du règlement AG.

([366]) Article 3(d)(i) du règlement AG. La Cour suprême des États-Unis a reconnu la possibilité pour le procureur général d'établir des organes indépendants dotés d'un pouvoir de décision, notamment pour statuer sur des cas individuels, voir notamment United States ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954) et United States/Nixon, 418 U.S. 683, 695 (1974). Le respect des différentes exigences de l'EO 14086, par exemple les critères et la procédure de nomination et de révocation des juges de la DPRC, est notamment soumis à la supervision de l'inspecteur général du ministère de la justice (voir également le considérant 109 sur le pouvoir des inspecteurs généraux qui leur est conféré par la loi).

([367]) Article 3(d)(i)(A) de l'EO 14086 et article 201.3(a) du règlement AG.

([368]) Article 201.3(b) du règlement AG.

([369]) Article 3(d)(i)(B) de l'EO 14086.

([370]) Article 3(d)(i)(A) de l'EO 14086 et article 201.3(a) et (c) du règlement AG. Les personnes nommées à la DPRC peuvent participer à des activités extrajudiciaires, y compris des activités commerciales et financières, des activités de collecte de fonds à but non lucratif et des activités fiduciaires, ainsi que pratiquer le droit, pour autant que ces activités n'entravent pas l'exercice impartial de leurs fonctions ou l'efficacité ou l'indépendance de la DPRC [article 201.7(c) du règlement AG].

([371]) Article 3(d)(iii) et (iv) de l'EO 14086 et article 201.7(d) du règlement AG.

([372]) Article 3(d)(i)(D) de l'EO 14086 et article 201.9 du règlement AG.

([373]) Article 3(d)(iv) de l'EO 14086 et article 201.7(d) du règlement AG. Voir également Bumap/États-Unis, 252 U.S. 512, 515 (1920), qui a confirmé le principe de longue date en droit américain selon lequel le pouvoir de révocation est inhérent au pouvoir de nomination [comme le rappelle également l'Office of Legal Counsel du ministère de la justice dans The Constitutional Separation of Powers Betbetween the President and Congress, 20 Op. O.L.C. 124, 166 (1996)].

(188) Les demandes adressées à la DPRC sont examinées par des panels de trois juges, dont un juge président, qui doivent agir conformément au code de conduite des juges américains ([374]). Chaque panel est assisté d'un avocat spécial ([375]), qui a accès à toutes les informations relatives à l'affaire, y compris aux informations classifiées ([376]). Le rôle de cet avocat est de veiller à ce que les intérêts du plaignant soient représentés et à ce que le panel de juges de la DPRC soit bien informé de toutes les questions de droit et de fait pertinentes ([377]). Afin d'éclairer sa position sur une demande de réexamen introduite par une personne auprès de la DPRC, l'avocat spécial peut demander des informations au plaignant en lui posant des questions écrites ([378]).

(189) La DPRC examine les décisions prises par l'ODNI CLPO (tant en ce qui concerne l'existence d'une violation du droit américain applicable qu'en ce qui concerne les mesures correctives appropriées) en se fondant, au minimum, sur le dossier de l'enquête de l'ODNI CLPO, ainsi que sur les informations et observations fournies par le plaignant, l'avocat spécial ou une agence de renseignement ([379]). Un panel de juges de la DPRC a accès à toutes les informations nécessaires à la conduite d'un examen, qu'il peut obtenir par l'intermédiaire de l'ODNI CLPO (le panel de juges peut, par exemple, demander au CLPO de compléter son dossier par des informations supplémentaires ou des constatations factuelles si cela est nécessaire pour mener à bien son examen) ([380]).

(190) Au terme de son examen, la DPRC peut 1) décider qu'il n'existe aucun élément de preuve indiquant que des activités de renseignement d'origine électromagnétique impliquant des données à caractère personnel du plaignant ont eu lieu, 2) décider que les décisions de l'ODNI CLPO étaient juridiquement correctes et étayées par des preuves substantielles, ou 3) si la DPRC est en désaccord avec les décisions de l'ODNI CLPO (sur la question de savoir s'il y a eu violation du droit américain applicable ou sur les mesures correctives appropriées), rendre ses propres décisions ([381]).

([374]) Article 3(d)(i)(B) de l'EO 14086 et article 201.7(a) à (c) du règlement AG. Le bureau des libertés civiles et de la vie privée du ministère de la justice (OPCL), qui est chargé de fournir un soutien administratif à la DPRC et aux avocats spéciaux (voir article 201.5 du règlement AG), sélectionne un panel de trois personnes à tour de rôle, en veillant à ce que chaque panel comprenne au moins un juge ayant une expérience judiciaire antérieure (si aucun des juges du panel n'a une telle expérience, le juge président sera le juge sélectionné en premier par l'OPCL).

([375]) Article 201.4 du règlement AG. Au moins deux avocats spéciaux sont nommés par le procureur général, en consultation avec le secrétaire d'État au commerce, le directeur du renseignement national et le PCLOB, pour des mandats de deux ans renouvelables. Les avocats spéciaux doivent avoir une expérience appropriée dans le domaine du droit de la vie privée et de la sécurité nationale, être des avocats expérimentés, des membres actifs et en règle du barreau et être dûment autorisés à exercer le droit. En outre, lors de leur nomination initiale, ils ne doivent pas avoir été employés du pouvoir exécutif au cours des deux années précédentes. Pour chaque examen d'une demande, le juge président sélectionne un avocat spécial pour assister le panel, voir article 201.8(a) du règlement AG.

([376]) Article 201.8(c) et article 201.11 du règlement AG.

([377]) Article 3(d)(i)(C) de l'EO 14086 et article 201.8(e) du règlement AG. L'avocat spécial ne défend pas les intérêts du plaignant et n'a pas de relation avocat-client avec celui-ci.

([378]) Voir article 201.8(d)(e) du règlement AG. Ces questions sont d'abord examinées par l'OPCL, en consultation avec la composante compétente de la communauté du renseignement, afin de déterminer et d'exclure toutes les informations classifiées, privilégiées ou protégées avant de les transmettre au plaignant. Les informations supplémentaires reçues par l'avocat spécial en réponse à ces questions sont incluses dans ses observations à la DPRC.

([379]) Article 3(d)(i)(D) de l'EO 14086.

([380]) Article 3(d)(iii) de l'EO 14086 et article 201.9(b) du règlement AG.

([381]) Article 3(d)(i)(E) de l'EO 14086 et article 201.9(c) à (e) du règlement AG. Selon la définition des «mesures correctives appropriées» figurant à la section 4, point a), de l'EO 14086, la DPRC doit tenir compte «de la manière dont une violation du type de celle constatée a été habituellement traitée» lorsqu'elle décide d'une mesure corrective visant à remédier pleinement à une violation, c'est-à-dire que la DPRC examinera, entre autres facteurs, la manière dont des problèmes de conformité similaires ont été résolus dans le passé afin de garantir que la mesure corrective est efficace et appropriée.

(191) Dans tous les cas, la DPRC adopte une décision écrite à la majorité. Si l'examen révèle une violation des règles applicables, la décision précisera les mesures correctives appropriées, telles que la suppression des données collectées illégalement, la suppression des résultats d'interrogations inappropriées de données, la limitation de l'accès à des données collectées de manière légale à du personnel dûment formé, ou le rappel des rapports de renseignement contenant des données acquises sans autorisation légale ou qui ont été diffusées de manière illégale ([382]). La décision de la DPRC est contraignante et définitive en ce qui concerne la plainte dont elle est saisie ([383]). En outre, si l'examen révèle une violation commise par une autorité faisant l'objet d'une surveillance de la part du FISC, la DPRC doit également fournir un rapport classifié à l'assistant du procureur général chargé de la sécurité nationale, qui est à son tour tenu de signaler le non-respect au FISC, qui peut prendre d'autres mesures répressives (conformément à la procédure décrite aux considérants 173 et 174) ([384]).

(192) Toute décision d'un panel de juges de la DPRC est transmise à l'ODNI CLPO ([385]). Dans les cas où l'examen de la DPRC a été déclenché par une demande du plaignant, ce dernier est informé par l'intermédiaire de l'autorité nationale que la DPRC a achevé son examen et que «l'examen n'a pas mis en évidence de violations couvertes ou que la DPRC a rendu une décision exigeant des mesures correctives appropriées» ([386]). Le bureau des libertés civiles et de la vie privée du ministère de la justice conserve une archive de toutes les informations examinées par la DPRC et de toutes les décisions rendues, qui est mise à la disposition des futurs panels de juges de la DPRC en tant que précédent non contraignant ([387]).

(193) Le ministère du commerce est également tenu de conserver une archive pour chaque plaignant ayant déposé une plainte ([388]). Afin d'améliorer la transparence, le ministère du commerce doit, au moins tous les cinq ans, contacter les agences de renseignement concernées pour vérifier si les informations relatives à un examen par la DPRC ont été déclassifiées ([389]). Si tel est le cas, la personne concernée sera informée que ces informations peuvent être disponibles en vertu du droit applicable (c'est-à-dire qu'elle peut demander d'y avoir accès en vertu de la loi sur la liberté de l'information, voir considérant 199).

(194) Enfin, le bon fonctionnement de ce mécanisme de recours fera l'objet d'une évaluation régulière et indépendante. Plus précisément, conformément à l'EO 14086, le fonctionnement du mécanisme de recours fait l'objet d'un examen annuel par le PCLOB, un organe indépendant (voir considérant 110) ([390]). Dans le cadre de cet examen, le PCLOB évaluera notamment si l'ODNI CLPO et la DPRC ont traité les réclamations dans les délais impartis; s'ils ont eu pleinement accès aux informations nécessaires; si les garanties substantielles de l'EO 14086 ont été correctement prises en compte dans la procédure d'examen; et si la communauté du renseignement s'est pleinement conformée aux décisions prises par l'ODNI CLPO et la DPRC. Le PCLOB présentera un rapport sur les résultats de son examen au président, au procureur général, au directeur du renseignement national, aux chefs des agences de renseignement, à l'ODNI CLPO et aux commissions du renseignement du Congrès, qui sera également rendu public dans une version non classifiée — et alimentera à son tour le réexamen périodique du fonctionnement de la présente décision qui sera effectué par la Commission. Le procureur général, le directeur du renseignement national, l'ODNI CLPO et les chefs des agences de renseignement sont tenus de mettre en œuvre toutes les recommandations figurant dans ces rapports ou d'y donner suite d'une autre manière. En outre, le PCLOB certifiera publiquement chaque année que le mécanisme de recours traite les réclamations conformément aux exigences de l'EO 14086.

([382]) Article 4(a) de l'EO 14086.

([383]) Article 3(d)(ii) de l'EO 14086 et article 201.9(g) du règlement AG. Étant donné que la décision de la DPRC est définitive et contraignante, aucun(e) autre institution/organe exécutif ou administratif (y compris le président des États-Unis) ne peut annuler la décision de la DPRC. Cela a également été confirmé dans la jurisprudence de la Cour suprême, qui a précisé qu'en déléguant son pouvoir unique au sein du pouvoir exécutif de rendre des décisions contraignantes à un organisme indépendant, le procureur général se prive de la possibilité de dicter de quelque manière que ce soit la décision de cet organisme [voir *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954)].

([384]) Article 3(d)(i)(F) de l'EO 14086 et article 201.9(i) du règlement AG.

([385]) Article 201.9(h) du règlement AG.

([386]) Article 3(d)(i)(H) de l'EO 14086 et article 201.9(h) du règlement AG. En ce qui concerne la nature de la notification, voir article 201.9 (h)(3) du règlement AG.

([387]) Article 201.9(j) du règlement AG.

([388]) Article 3(d)(v)(A) de l'EO 14086.

([389]) Article 3(d)(v) de l'EO 14086.

([390]) Article 3(e) de l'EO 14086. Voir également https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20.

(195) Outre le mécanisme de recours spécifique établi par l'EO 14086, des voies de recours devant les juridictions américaines ordinaires sont à la disposition de toutes les personnes concernées (quelle que soit leur nationalité ou leur lieu de résidence) ([391]).

(196) En particulier, le FISA et une loi connexe prévoient la possibilité pour les personnes concernées: d'intenter un recours civil pour demander des dommages et intérêts aux États-Unis lorsque des informations à leur sujet ont été utilisées ou divulguées illégalement et volontairement ([392]); de poursuivre des fonctionnaires de l'État américain à titre personnel pour obtenir des dommages et intérêts ([393]); et de contester la légalité de la surveillance (et tenter de supprimer les informations) dans le cas où l'État américain envisagerait d'utiliser ou de divulguer toute information obtenue ou découlant de la surveillance électronique, à l'encontre de la personne visée par une procédure judiciaire ou administrative aux États-Unis ([394]). Plus généralement, si le gouvernement envisage d'utiliser des informations obtenues au cours d'opérations de renseignement contre un suspect dans une affaire pénale, les exigences constitutionnelles et légales ([395]) imposent l'obligation de divulguer certaines informations afin que le défendeur puisse contester la légalité de la collecte et de l'utilisation des données par le gouvernement.

(197) En outre, il existe plusieurs voies de recours pour former un recours en justice contre des fonctionnaires de l'État en raison d'un accès ou d'un usage illégal de données à caractère personnel, y compris à des fins prétendues de sécurité nationale [à savoir le Computer Fraud and Abuse Act ([396]); le Electronic Communications Privacy Act ([397]); et le Right to Financial Privacy Act ([398])]. Tous ces recours juridictionnels portent sur des données, des cibles et/ou des types d'accès spécifiques (par exemple l'accès à distance à un ordinateur via l'internet) et peuvent être invoqués dans certaines conditions (notamment un acte intentionnel/délibéré, un acte commis en état d'incapacité, un préjudice subi).

(198) Une possibilité plus générale de recours est contenue dans l'APA ([399]), selon lequel «toute personne subissant un dommage du fait d'une décision d'une agence ou qui est affectée ou lésée par la décision d'une agence» peut former un recours juridictionnel ([400]). Cela inclut la possibilité de demander au tribunal de «déclarer illégales et d'annuler la décision, les constatations et les conclusions de l'agence jugées […] arbitraires, capricieuses, constitutives d'un abus du pouvoir d'appréciation ou non conformes à la loi pour une autre raison» ([401]). Par exemple, une cour d'appel fédérale a statué en 2015 sur une demande de l'APA selon laquelle la collecte en vrac de métadonnées téléphoniques par le gouvernement américain n'était pas autorisée par l'article 501 du FISA ([402]).

([391]) L'accès à ces voies de recours est subordonné au fait de démontrer sa «qualité pour agir». Cette norme, qui s'applique à toute personne indépendamment de sa nationalité, résulte de l'exigence «case or controversy» (une affaire ou un différend) figurant à l'article III de la Constitution américaine. Selon la Cour suprême, il faut pour cela que 1) la personne ait subi un «préjudice de fait» (c'est-à-dire un préjudice d'un intérêt juridiquement protégé qui est concret et particulier et réel ou imminent), 2) qu'il y ait un lien de causalité entre le préjudice et le comportement contesté devant le tribunal, et 3) qu'il soit probable, et non spéculatif, qu'une décision favorable du tribunal remédie au préjudice [voir affaire Lujan/Defenders of Wildlife, 504 U.S. 555 (1992)].

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Voir, respectivement, affaire Brady/Maryland, 373 U.S. 83 (1963), et «Jencks Act», 18 U.S.C. § 3500.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701 à 2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

([400]) Généralement, seules les décisions «finales» d'une agence — par opposition aux décisions préliminaires, procédurales ou intermédiaires — sont soumises au contrôle juridictionnel. Voir 5 U.S.C. § 704.

([401]) 5 U.S.C. § 706(2)(A).

([402]) Voir affaire ACLU/Clapper, 785 F.3d 787 (2d Cir. 2015). Le programme de collecte de données téléphoniques en vrac contesté dans ces affaires a été supprimé par la loi USA FREEDOM Act en 2015.

(199) Enfin, outre les voies de recours mentionnées aux considérants 176 à 198, toute personne a le droit de demander l'accès aux archives existantes des agences fédérales en vertu de la loi sur l'accès à l'information, notamment lorsque ces archives contiennent des données à caractère personnel de la personne concernée ([403]). L'obtention de cet accès peut également faciliter l'introduction de procédures devant les juridictions ordinaires, notamment pour démontrer sa qualité à agir. Les agences peuvent ne pas divulguer les informations qui relèvent de certaines exceptions énumérées, notamment l'accès à des informations classifiées relatives à la sécurité nationale et à des informations concernant les enquêtes des autorités répressives ([404]), mais les plaignants qui ne sont pas satisfaits de la réponse ont la possibilité de la contester en demandant un contrôle administratif et, par la suite, un contrôle juridictionnel (devant les juridictions fédérales) ([405]).

(200) Il ressort de ce qui précède que lorsque les autorités répressives ou les autorités de sécurité nationale américaines accèdent à des données à caractère personnel relevant du champ d'application de la présente décision, cet accès est régi par un cadre juridique qui définit les conditions dans lesquelles il peut avoir lieu et qui garantit que l'accès à ces données et leur utilisation ultérieure sont limités à ce qui est nécessaire et proportionné à l'objectif d'intérêt public poursuivi. Ces garanties peuvent être invoquées par les personnes qui bénéficient de droits de recours effectifs.

4. **CONCLUSIONS**

(201) La Commission considère que les États-Unis — dans le cadre des principes publiés par le CPD UE - États-Unis — garantissent un niveau de protection des données à caractère personnel transférées de l'Union vers des organisations certifiées aux États-Unis en vertu du cadre de protection des données UE - États-Unis essentiellement équivalent à celui garanti par le règlement (UE) 2016/679.

(202) De plus, la Commission estime que l'application effective des principes est garantie par les obligations de transparence et par le fait que le ministère du commerce gère le CPD. En outre, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit américain permettent de détecter et de sanctionner, en pratique, les violations des règles en matière de protection des données et offrent aux personnes concernées des voies de recours pour accéder aux données à caractère personnel les concernant et, in fine, obtenir leur rectification ou leur suppression.

(203) Enfin, sur la base des informations disponibles concernant l'ordre juridique américain, y compris les informations figurant aux annexes VI et VII, la Commission considère que toute atteinte aux droits fondamentaux des particuliers dont les données à caractère personnel sont transférées de l'Union européenne vers les États-Unis en vertu du cadre de protection des données UE - États-Unis pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale, 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. Par conséquent, à la lumière des constatations ci-dessus, il convient de décider que les États-Unis assurent un niveau de protection adéquat, au sens de l'article 45 du règlement (UE) 2016/679, interprété à la lumière de la Charte des droits fondamentaux de l'Union européenne, des données à caractère personnel transférées de l'Union européenne vers des organisations certifiées en vertu du cadre de protection des données UE - États-Unis.

(204) Étant donné que les limitations, les garanties et le mécanisme de recours établis par l'EO 14086 sont des éléments essentiels du cadre juridique américain sur lequel se fonde l'évaluation de la Commission, l'adoption de la présente décision est notamment fondée sur l'adoption, par toutes les agences de renseignement américaines, des politiques et de procédures actualisées pour mettre en œuvre l'EO 14086 et la désignation de l'Union en tant qu'organisation remplissant les conditions requises aux fins du mécanisme de recours, qui ont eu lieu respectivement le 3 juillet 2023 (voir considérant 126) et le 30 juin 2023 (voir considérant 176).

([403]) 5 U.S.C. § 552. Il existe des législations analogues au niveau des États.

([404]) Si tel est le cas, la personne recevra normalement une réponse standard dans laquelle l'agence se refuse à confirmer ou infirmer l'existence des documents concernés. Voir affaire ACLU/CIA, 710 F.3d 422 (D.C. Cir. 2014). Les critères et la durée de classification sont fixés dans le décret présidentiel n° 13526, qui prévoit, en règle générale, qu'il convient d'établir une date ou un événement précis pour la déclassification en fonction de la durée de la sensibilité des informations pour la sécurité nationale, moment auquel les informations doivent être automatiquement déclassifiées (voir article 1.5 de l'EO 13526).

([405]) Le tribunal détermine de novo si l'accès aux archives a été refusé légalement et peut obliger les pouvoirs publics à donner accès à ces archives [5 U.S.C. § 552(a)(4)(B)].

5. EFFETS DE LA PRÉSENTE DÉCISION ET ACTION DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES

(205) Les États membres et leurs organes sont tenus de prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés à la suite d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité.

(206) En conséquence, une décision d'adéquation de la Commission adoptée en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de contrôle indépendantes. En particulier, les transferts d'un responsable du traitement ou d'un sous-traitant situé dans l'Union à des organisations certifiées situées aux États-Unis peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation supplémentaire.

(207) Il convient de rappeler que, comme prévu à l'article 58, paragraphe 5, du règlement (UE) 2016/679 et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems ([406]), lorsqu'une autorité nationale chargée de la protection des données met en cause, notamment après avoir été saisie d'une plainte, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui, en cas de doute, doivent surseoir à statuer et procéder à un renvoi préjudiciel devant la Cour de justice ([407]).

6. SUIVI ET EXAMEN DE LA PRÉSENTE DÉCISION

(208) Conformément à la jurisprudence de la Cour de justice ([408]), et comme consacré par l'article 45, paragraphe 4, du règlement (UE) 2016/679, la Commission devrait suivre, de manière permanente, les évolutions dans le pays tiers après l'adoption d'une décision d'adéquation, afin de déterminer si le pays tiers continue de garantir un niveau de protection essentiellement équivalent. Une telle vérification s'impose, en tout état de cause, lorsque la Commission reçoit des informations faisant naître un doute justifié à cet égard.

(209) Par conséquent, la Commission devrait surveiller de manière permanente la situation aux États-Unis en ce qui concerne le cadre juridique et la pratique proprement dite de traitement des données à caractère personnel tels qu'évalués dans la présente décision. Pour faciliter ce processus, les autorités américaines devraient informer rapidement la Commission de toute évolution importante de l'ordre juridique américain ayant une incidence sur le cadre juridique qui fait l'objet de la présente décision, ainsi que de toute évolution des pratiques relatives au traitement des données à caractère personnel évaluées dans la présente décision, en ce qui concerne tant le traitement des données à caractère personnel par les organisations certifiées aux États-Unis que les limitations et garanties applicables à l'accès des autorités publiques aux données à caractère personnel.

(210) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de suivi, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales chargées de la protection des données, en particulier en ce qui concerne les questions ou les réclamations des personnes concernées de l'Union au sujet du transfert de données à caractère personnel des autorités compétentes de l'Union vers des organisations certifiées aux États-Unis. La Commission devrait également être informée de tout élément indiquant que les actions des autorités publiques américaines responsables de la prévention, de la détection, des enquêtes et des poursuites en matière d'infractions pénales, ou de la sécurité nationale, y compris de tout organisme de surveillance, n'assurent pas le niveau de protection requis.

([406]) Arrêt Schrems, point 65.

([407]) Arrêt Schrems, point 65: «À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.».

([408]) Arrêt Schrems, point 76.

(211) En application de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ([409]), la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par les États-Unis en vertu du CPD UE - États-Unis sont toujours justifiées en fait et en droit. Étant donné que l'EO 14086 et le règlement AG exigent notamment la création de nouveaux mécanismes et la mise en œuvre de nouvelles garanties, la présente décision doit faire l'objet d'un premier examen dans un délai d'un an à compter de son entrée en vigueur, afin de vérifier si tous les éléments pertinents ont été pleinement mis en œuvre et fonctionnent efficacement dans la pratique. Après ce premier examen, et en fonction de son résultat, la Commission se prononcera, en étroite concertation avec le comité institué en vertu de l'article 93, paragraphe 1, du règlement (UE) 2016/679 et le comité européen de la protection des données, sur la périodicité des futurs examens ([410]).

(212) En vue de la réalisation de ces examens, la Commission devrait rencontrer le ministère du commerce, la FTC et le ministère des transports, accompagnés, s'il y a lieu, d'autres services et agences participant à la mise en œuvre du CPD UE - États-Unis, ainsi que, pour les questions ayant trait à l'accès des pouvoirs publics aux données, des représentants du ministère de la justice, de l'ODNI (notamment le CLPO), d'autres composantes de la communauté du renseignement, de la DPRC et des avocats spéciaux. La participation à cette réunion devrait être ouverte aux représentants des membres du comité européen de la protection des données.

(213) Les examens devraient couvrir tous les aspects relatifs au fonctionnement de la présente décision concernant le traitement des données à caractère personnel aux États-Unis et, en particulier, l'application et la mise en œuvre des principes, en accordant une attention particulière aux protections accordées en cas de transferts ultérieurs; les évolutions pertinentes de la jurisprudence; le caractère effectif de l'exercice des droits individuels; la surveillance du respect des principes et la mise en conformité avec ceux-ci; ainsi que les limitations et garanties en ce qui concerne l'accès des pouvoirs publics aux données, notamment la mise en œuvre et l'application des garanties introduites par l'EO 14086, y compris au moyen de politiques et de procédures élaborées par les agences de renseignement; l'interaction entre l'EO 14086 et l'article 702 du FISA et l'EO 12333; et l'efficacité des mécanismes de surveillance et des voies de recours (y compris le fonctionnement du nouveau mécanisme de recours établi au titre de l'EO 14086). Dans le cadre de ces examens, une attention particulière sera également accordée à la coopération entre les APD et les autorités compétentes des États-Unis, prévoyant notamment l'élaboration d'orientations et d'autres outils d'interprétation sur l'application des principes ainsi que sur d'autres aspects du fonctionnement du cadre.

(214) Sur la base de l'examen, la Commission devrait élaborer un rapport public qui sera présenté au Parlement européen et au Conseil.

7. **SUSPENSION, ABROGATION OU MODIFICATION DE LA PRÉSENTE DÉCISION**

(215) Lorsque des informations disponibles, en particulier les informations résultant du suivi de la présente décision ou fournies par les autorités américaines ou des États membres, révèlent que le niveau de protection conféré aux données transférées en vertu de la présente décision pourrait ne plus être adéquat, la Commission devrait en informer rapidement les autorités américaines compétentes et demander que des mesures appropriées soient prises dans un délai raisonnable bien défini.

(216) Si, à l'expiration de la période précisée, les autorités américaines compétentes n'ont pas pris ces mesures ou échouent à démontrer de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission lancera la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679 en vue de la suspension partielle ou complète ou de l'abrogation de la présente décision.

(217) À défaut, la Commission lancera cette procédure visant à modifier la présente décision, notamment en soumettant les transferts de données à des conditions supplémentaires ou en limitant le constat d'adéquation aux seuls transferts de données pour lesquels un niveau de protection adéquat continue à être garanti.

([409]) Conformément à l'article 45, paragraphe 3, du règlement (UE) 2016/679, «[l]'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale».

([410]) L'article 45, paragraphe 3, du règlement (UE) 2016/679 dispose qu'un examen périodique doit avoir lieu «au moins tous les quatre ans». Voir également comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rév. 01.

(218) Plus particulièrement, la Commission devrait lancer la procédure de suspension ou d'abrogation en présence:

a) d'éléments indiquant que les organisations qui ont reçu des données à caractère personnel depuis l'Union en vertu de la présente décision ne respectent pas les principes et que ce non-respect n'est pas traité efficacement par les organes de surveillance et les services répressifs compétents;

b) d'éléments indiquant que les autorités américaines ne respectent pas les conditions et limitations applicables à l'accès à des données à caractère personnel transférées en vertu du CPD UE - États-Unis par les autorités publiques américaines à des fins répressives et de sécurité nationale; ou

c) d'éléments indiquant que les réclamations déposées par les personnes concernées de l'Union ne sont pas traitées efficacement, notamment par l'ODNI CLPO et/ou la DPRC.

(219) La Commission devrait également envisager de lancer la procédure conduisant à la modification, à la suspension ou à l'abrogation de la présente décision si les autorités américaines compétentes ne fournissent pas les informations ou les clarifications nécessaires pour apprécier le niveau de protection conféré aux données à caractère personnel transférées de l'Union européenne vers les États-Unis, ou concernant le respect de la présente décision. À cet égard, la Commission devrait prendre en compte la mesure dans laquelle les informations concernées peuvent être obtenues auprès d'autres sources.

(220) Pour des raisons d'urgence impérieuse dûment justifiées, par exemple si l'EO 14086 ou le règlement AG étaient modifiés d'une manière qui compromettrait le niveau de protection décrit dans la présente décision ou si la désignation, par le procureur général, de l'Union en tant qu'organisation remplissant les conditions requises aux fins du mécanisme de recours est retirée, la Commission aura recours à la possibilité d'adopter, conformément à la procédure visée à l'article 93, paragraphe 3, du règlement (UE) 2016/679, des actes d'exécution immédiatement applicables suspendant, abrogeant ou modifiant la décision.

8. **CONSIDÉRATIONS FINALES**

(221) Le comité européen de la protection des données a publié son avis ([411]), dont il a été tenu compte dans l'élaboration de la présente décision.

(222) Le Parlement européen a adopté une résolution sur l'adéquation de la protection assurée par le cadre de protection des données UE - États-Unis ([412]).

(223) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué par l'article 93, paragraphe 1, du règlement (UE) 2016/679,

A ADOPTÉ LA PRÉSENTE DÉCISION

Article premier

Aux fins de l'article 45 du règlement (UE) 2016/679, les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis qui figurent sur la «liste du cadre de protection des données», tenue à jour et publiée par le ministère du commerce, conformément à la section I.3 de l'annexe I.

Article 2

Lorsque, afin de protéger les personnes à l'égard du traitement de leurs données à caractère personnel, les autorités compétentes des États membres exercent les pouvoirs que leur confère l'article 58 du règlement (UE) 2016/679 concernant les transferts de données visés à l'article 1er de la présente décision, l'État membre concerné en informe la Commission sans délai.

([411]) 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 du 28 février 2023.

([412]) Résolution du Parlement européen du 11 mai 2023 sur l'adéquation de la protection assurée par le cadre de protection des données UE - États-Unis [2023/2501 (RSP)].

Article 3

1. La Commission suit de manière permanente l'application du cadre juridique sur lequel se fonde la présente décision, notamment les conditions dans lesquelles les transferts ultérieurs sont effectués, les droits individuels sont exercés et les autorités publiques américaines ont accès aux données transférées sur la base de la présente décision, dans le but de déterminer si les États-Unis continuent d'assurer un niveau de protection adéquat au sens de l'article 1er.

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels les organismes américains dotés du pouvoir réglementaire de faire respecter les principes énoncés à l'annexe I ne prévoient pas de mécanismes de détection et de surveillance permettant de détecter et de sanctionner en pratique les infractions à ces principes.

3. Les États membres et la Commission s'informent mutuellement de tout élément indiquant que les interférences des autorités publiques américaines responsables du maintien de la sécurité nationale, de l'application de la loi ou d'autres intérêts publics avec le droit de l'individu à la protection de ses données à caractère personnel vont au-delà de ce qui est nécessaire et proportionné et/ou qu'il n'existe pas de protection juridictionnelle effective contre des interférences de cette nature.

4. Dans un délai d'un an à compter de la date de notification de la présente décision aux États membres, et ensuite selon une périodicité qui sera définie en étroite consultation avec le comité institué en vertu de l'article 93, paragraphe 1, du règlement (UE) 2016/679 et le comité européen de la protection des données, la Commission évalue le constat établi à l'article 1er, paragraphe 1, sur la base de toutes les informations disponibles, notamment les informations obtenues dans le cadre de l'examen conjoint réalisé avec les autorités américaines compétentes.

5. Lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités américaines compétentes. Si nécessaire, elle décidera de suspendre, de modifier ou d'abroger la présente décision, ou d'en restreindre le champ d'application, conformément à l'article 45, paragraphe 5, du règlement (UE) 2016/679. La Commission peut également adopter une telle décision si le défaut de coopération de la part des autorités américaines l'empêche de déterminer si les États-Unis continuent d'assurer un niveau de protection adéquat.

Article 4

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 10 juillet 2023.

Par la Commission
Didier REYNDERS
Membre de la Commission

ANNEXE I

PRINCIPES DU CADRE DE PROTECTION DES DONNÉES UE — ÉTATS-UNIS PUBLIÉS PAR LE MINISTÈRE AMÉRICAIN DU COMMERCE

I. VUE D'ENSEMBLE

1. Même si les États-Unis et l'Union européenne (ci-après l'«Union») ont comme engagement commun de protéger davantage la vie privée et l'état de droit et reconnaissent l'importance des flux de données transatlantiques pour leurs citoyens, économies et sociétés respectifs, les États-Unis préconisent une approche en matière de protection de la vie privée différente de celle de l'Union. Ils se basent, en effet, sur un système sectoriel qui fait appel à un ensemble disparate de dispositions législatives et réglementaires ainsi qu'à des codes d'autoréglementation. 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 complémentaires (ci-après collectivement dénommés les «principes») et l'annexe I des principes (ci-après l'«annexe I») en vertu de sa compétence légale pour encourager, promouvoir et développer le commerce international (15 U.S.C. § 1512). Les principes ont été élaborés en concertation avec la Commission européenne (ci-après la «Commission»), le secteur d'activité concerné et d'autres parties intéressées dans le but de faciliter le commerce et les relations d'affaires entre les États-Unis et l'Union. Les principes, un élément clé du cadre de protection des données UE — États-Unis (ci-après le «CPD UE — États-Unis») offrent aux organisations établies aux États-Unis un mécanisme fiable pour les transferts de données à caractère personnel vers les États-Unis depuis l'Union tout en veillant à ce que les personnes concernées de l'Union continuent de bénéficier de garanties et de protections efficaces comme l'exige la législation européenne en ce qui concerne le traitement de leurs données à caractère personnel transférées vers des pays non membres de l'Union. Les principes sont exclusivement destinés aux organisations éligibles établies aux États-Unis recevant des données à caractère personnel en provenance de l'Union, aux fins de leur permettre d'adhérer au CPD UE — États-Unis et de bénéficier ainsi de la décision d'adéquation de la Commission ([1]). Les principes n'ont aucune incidence sur l'application du règlement (UE) 2016/679 (ci-après le «règlement général sur la protection des données» ou le «RGPD») ([2]), qui s'applique au traitement des données à caractère personnel dans les États membres de l'Union. Ils ne limitent pas non plus les obligations en matière de protection de la vie privée applicables par ailleurs en vertu de la législation des États-Unis.

2. Pour pouvoir se prévaloir du CPD UE — États-Unis afin de transférer des données à caractère personnel depuis l'Union, une organisation doit autocertifier son adhésion aux principes auprès du ministère (ou auprès de la personne désignée par celui-ci). Si la décision d'adhérer au CPD UE — États-Unis est entièrement volontaire, le respect de ses règles est quant à lui obligatoire: les organisations qui autocertifient leur adhésion auprès du ministère et qui annoncent publiquement leur engagement à respecter les principes sont tenues de se conformer pleinement à ces derniers. Pour adhérer au CPD UE — États-Unis, une organisation doit: a) être soumise aux pouvoirs d'enquête et aux pouvoirs répressifs de la Commission fédérale du commerce (ci-après la «FTC»), du ministère des transports ou d'un autre organisme officiel qui garantira concrètement le respect des principes (*d'autres organes officiels américains reconnus par l'Union européenne peuvent être inclus sous forme d'une annexe à l'avenir*); b) déclarer publiquement son engagement à respecter les principes; c) publier sa politique en matière de protection de la vie privée, qui doit être conforme aux principes; et d) appliquer les principes dans leur intégralité ([3]). Tout manquement d'une organisation au respect de ces conditions peut être sanctionné par la FTC conformément à l'article 5 du Federal Trade Commission Act (ci-après le «FTC Act», qui interdit les pratiques déloyales ou frauduleuses dans le domaine du commerce (15 U.S.C. § 45); par le ministère des transports en vertu du titre 49, section 41712, de l'U.S.C. qui interdit aux transporteurs et aux agents de billetterie toute pratique déloyale ou frauduleuse ou tout acte de concurrence déloyale relative au transport aérien ou à la vente de transport aérien; ou en vertu de toute autre loi interdisant de tels actes.

([1]) Pour autant que la décision de la Commission relative à l'adéquation de la protection assurée par le CPD UE — États-Unis s'applique à l'Islande, au Liechtenstein et à la Norvège, le CPD UE — États-Unis couvrira non seulement l'Union, mais également ces trois pays. Dès lors, les références à l'Union et à ses États membres doivent s'entendre comme incluant également l'Islande, le Liechtenstein et la Norvège.

([2]) 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).

([3]) Les principes du cadre «bouclier de protection des données UE — États-Unis» ont été modifiés en tant que «principes du cadre de protection des données UE — États-Unis» (*Voir* principe complémentaire sur l'autocertification).

3. Le ministère tiendra et mettra à la disposition du public une liste officielle des organisations des États-Unis qui ont autocertifié leur adhésion auprès du ministère et qui ont déclaré leur engagement à respecter les principes (la «liste du cadre de protection des données»). Une organisation peut prétendre aux avantages offerts par le CPD UE — États-Unis dès le moment où le ministère l'inscrit sur la liste du cadre de protection des données. Le ministère supprimera une organisation de la liste du cadre de protection des données si cette organisation se retire volontairement du CPD UE — États-Unis ou si elle manque à son obligation de recertification annuelle auprès du ministère; l'organisation doit alors continuer d'appliquer les principes aux informations à caractère personnel qu'elle a reçues alors qu'elle participait au CPD UE — États-Unis et déclarer annuellement au ministère son engagement à le faire (c'est-à-dire aussi longtemps qu'elle conserve ces informations), ou assurer une protection «adéquate» des informations par un autre moyen autorisé (par exemple en utilisant un contrat qui reflète pleinement les exigences des clauses contractuelles standard adoptées par la Commission européenne), ou restituer ou supprimer les informations concernées. Le ministère supprimera également de la liste du cadre de protection des données les organisations qui, de manière récurrente, ne respectent pas les principes; ces organisations doivent restituer ou supprimer les informations à caractère personnel qu'elles ont reçues alors qu'elles participaient au CPD UE — États-Unis. La suppression d'une organisation de la liste du cadre de protection des données a pour conséquence que cette organisation ne peut plus prétendre au bénéfice de la décision d'adéquation de la Commission pour recevoir des informations à caractère personnel en provenance de l'Union.

4. Le ministère tiendra et mettra également à la disposition du public une liste officielle des organisations des États-Unis qui avaient précédemment autocertifié leur adhésion auprès du ministère mais qui ont été supprimées de la liste du cadre de protection des données. Le ministère publiera une mise en garde claire indiquant que ces organisations ne participent pas au CPD UE — États-Unis, que leur suppression de la liste du cadre de protection des données signifie qu'elles ne peuvent pas prétendre se conformer au CPD UE — États-Unis et qu'elles doivent éviter toute déclaration ou toute pratique trompeuse qui laissent entendre qu'elles participent au CPD UE — États-Unis, et qu'elles ne peuvent plus prétendre au bénéfice de la décision d'adéquation de la Commission pour recevoir des informations à caractère personnel en provenance de l'Union. Toute organisation qui continue de prétendre participer au CPD UE — États-Unis ou qui fait d'autres déclarations trompeuses relatives au CPD UE — États-Unis après avoir été supprimée de la liste du cadre de protection des données est susceptible de faire l'objet de mesures répressives de la part de la FTC, du ministère des transports ou d'autres autorités répressives.

5. L'adhésion aux principes peut être limitée: a) à la mesure nécessaire pour se conformer à une décision de justice ou pour répondre à des exigences relatives à l'intérêt public, au respect de la législation ou à la sécurité nationale, y compris lorsque les textes législatifs ou les règlements administratifs créent des obligations contradictoires; b) par des textes législatifs, des décisions de justice ou des règlements administratifs qui créent des autorisations explicites, pour autant qu'une organisation qui s'appuie sur une telle autorisation puisse démontrer que le non-respect des principes est limité à la mesure nécessaire pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; ou c) par les exceptions ou les dérogations prévues par le RGPD, dans les conditions qui y sont énoncées, pour autant que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Dans ce contexte, les garanties prévues par le droit américain pour protéger la vie privée et les libertés civiles comprennent celles requises par le décret présidentiel 14086 ([4]) dans les conditions qui y sont énoncées (notamment les exigences de nécessité et de proportionnalité). Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations devraient s'atteler à appliquer ces principes de manière complète et transparente, y compris en s'efforçant d'indiquer dans leur politique en matière de protection de la vie privée dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront. Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé.

6. Les organisations sont tenues d'appliquer les principes à toutes les données à caractère personnel transférées sur la foi du CPD UE — États-Unis après leur adhésion à celui-ci. Les organisations qui décident d'étendre les avantages du CPD UE — États-Unis à des informations à caractère personnel tirées de fichiers qui concernent les ressources humaines en provenance de l'Union afin de les utiliser dans le cadre d'une relation de travail doivent mentionner cette intention lorsqu'elles autocertifient leur adhésion auprès du ministère et doivent se conformer aux exigences exposées dans le principe complémentaire relatif à l'autocertification.

([4]) Décret présidentiel du 7 octobre 2022 intitulé «Enhancing Safeguards for United States Signals Intelligence Activities».

7. Le droit des États-Unis est applicable en ce qui concerne l'interprétation et le respect des principes et des politiques pertinentes en matière de protection de la vie privée par les organisations participant au CPD UE — États-Unis, à l'exception des cas dans lesquels les organisations se sont engagées à coopérer avec les autorités européennes chargées de la protection des données (ci-après les «APD»). Sauf indication contraire, toutes les dispositions des principes sont applicables lorsqu'elles sont pertinentes.

8. Définitions:

   a. Par «donnée à caractère personnel» et «information à caractère personnel», il faut entendre toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application du RGPD, qui est transférée de l'Union vers une organisation aux États-Unis et qui est enregistrée sous quelque forme que ce soit.

   b. Par «traitement de données à caractère personnel», il faut entendre toute activité ou ensemble d'activités effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion, l'effacement ou la destruction.

   c. Par «responsable du traitement», il faut entendre la personne ou l'organisation qui, seule ou conjointement avec d'autres, détermine les finalités et moyens du traitement de données à caractère personnel.

9. La date d'entrée en vigueur des principes et de l'annexe I des principes est la date d'entrée en vigueur de la décision d'adéquation de la Commission européenne.

II. PRINCIPES

1. NOTIFICATION

a. Toute organisation doit informer les personnes concernées:

   i. de sa participation au CPD UE — États-Unis, en fournissant un lien vers la liste du cadre de protection des données ou l'adresse web de celle-ci,

   ii. des types de données à caractère personnel collectées et, le cas échéant, des entités ou filiales américaines de l'organisation qui adhèrent également aux principes;

   iii. de son engagement à appliquer les principes à toutes les données à caractère personnel reçues depuis l'Union européenne sur la foi du CPD UE — États-Unis;

   iv. des fins auxquelles elle collecte et utilise des informations à caractère personnel les concernant;

   v. de la façon de contacter l'organisation pour toute question ou réclamation, y compris les coordonnées de tout établissement situé dans l'Union européenne qui soit en mesure de répondre à ces questions ou réclamations;

   vi. du type ou de l'identité des tiers auxquels elle divulgue des informations à caractère personnel et des fins auxquelles elle leur communique ces informations;

   vii. du droit d'accès des personnes à leurs données à caractère personnel;

   viii. des possibilités et moyens offerts par l'organisation aux personnes pour restreindre l'utilisation et la divulgation de leurs données à caractère personnel;

   ix. de l'organe indépendant de règlement des litiges désigné pour traiter les réclamations et mettre gratuitement à la disposition des personnes des voies de recours appropriées, en précisant si cet organe est: 1) le panel établi par les autorités chargées de la protection des données, 2) un organe de règlement extrajudiciaire des litiges établi dans l'Union ou 3) un organe de règlement extrajudiciaire des litiges établi aux États-Unis;

   x. du fait qu'elle est soumise aux pouvoirs d'enquête et aux pouvoirs répressifs de la FTC, du ministère des transports ou de tout autre organisme officiel américain;

   xi. de la possibilité pour la personne, sous certaines conditions, de faire appel à un arbitrage contraignant ([5]);

   xii. de l'obligation de divulguer les informations à caractère personnel en réponse à des demandes légales formulées par les pouvoirs publics, notamment pour répondre à des besoins de sécurité nationale ou d'application des lois; et

   xiii. de sa responsabilité en cas de transferts ultérieurs à des tiers.

([5]) *Voir, par exemple,* section c) du principe «Voies de recours, application et responsabilité».

b. Cette notification doit être communiquée de manière claire et visible aux personnes lorsque celles-ci sont invitées pour la première fois à fournir des informations à caractère personnel ou dès que possible après cette invitation et, en tout état de cause, avant que les données ne soient utilisées dans un but différent de celui pour lequel elles ont été initialement collectées ou traitées par l'organisation ayant effectué le transfert ou avant qu'elles ne soient diffusées pour la première fois à un tiers.

2. **CHOIX**

a. Toute organisation doit offrir aux personnes la possibilité d'accepter ou non que leurs informations à caractère personnel: i) soient divulguées à un tiers; ou ii) soient utilisées dans un but matériellement différent du ou des objectifs pour lesquels elles ont été initialement collectées ou du ou des objectifs approuvés ultérieurement par les personnes concernées. Les personnes concernées doivent disposer de mécanismes clairs, visibles et d'accès facile pour opérer leur choix.

b. Par dérogation au paragraphe précédent, il n'est pas nécessaire d'offrir un choix quand des données sont communiquées à un tiers qui est chargé d'effectuer des travaux pour le compte et selon les instructions de l'organisation. Dans ce cas cependant, l'organisation doit toujours conclure un contrat avec le mandataire concerné.

c. En ce qui concerne les informations sensibles (par exemple, les données concernant le dossier médical ou l'état de santé d'une personne, son origine raciale ou ethnique, ses opinions politiques, ses croyances religieuses ou ses convictions philosophiques, son affiliation à un syndicat ou sa sexualité), les organisations doivent obtenir l'accord explicite et positif (à savoir, le consentement) des personnes concernées pour que ces informations puissent être: i) divulguées à un tiers; ou ii) utilisées dans un but qui diffère de l'objectif initial de la collecte ou de tout autre objectif approuvé ultérieurement par la personne concernée exerçant son droit de consentement. En outre, une organisation doit considérer comme sensible toute information à caractère personnel reçue d'un tiers qui indique que cette information est sensible, et doit la traiter comme telle.

3. **RESPONSABILITÉ EN CAS DE TRANSFERT ULTÉRIEUR**

a. Pour transférer des informations à caractère personnel à un tiers agissant en qualité de responsable du traitement, les organisations sont tenues d'appliquer les principes «Notification» et «Choix». Les organisations doivent également conclure un contrat avec le tiers responsable du traitement prévoyant que ces données peuvent être traitées uniquement à des fins limitées et spécifiques, conformément au consentement donné par la personne concernée, et que le destinataire assurera un niveau de protection équivalent à celui prévu par les principes et notifiera l'organisation s'il constate qu'il ne peut plus satisfaire à cette obligation. Le contrat prévoira que, si une telle constatation est faite, le tiers responsable du traitement cesse le traitement ou prend d'autres mesures raisonnables et adéquates pour remédier à cette situation.

b. Pour transférer des données à caractère personnel à un tiers agissant en qualité de mandataire, les organisations doivent: i) transférer les données concernées uniquement à des fins limitées et spécifiques; ii) s'assurer que le mandataire est tenu de garantir un niveau de protection au moins égal à celui requis par les principes; iii) prendre des mesures raisonnables et adéquates pour veiller à ce que le mandataire traite effectivement les informations à caractère personnel transférées d'une façon conforme aux obligations incombant à l'organisation en vertu des principes; iv) imposer au mandataire de notifier l'organisation s'il constate qu'il ne peut plus satisfaire à l'obligation d'assurer un niveau de protection équivalent à celui prévu par les principes; v) à la suite d'une notification, y compris au titre du point iv), prendre des mesures raisonnables et adéquates pour faire cesser tout traitement non autorisé et y remédier; et vi) fournir au ministère, sur demande, une synthèse ou une copie représentative des dispositions relatives à la vie privée contenues dans son contrat avec le mandataire concerné.

4. **SÉCURITÉ**

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

5. **INTÉGRITÉ DES DONNÉES ET LIMITATION DES FINALITÉS**

a. Dans le droit-fil des principes, les informations à caractère personnel doivent se limiter aux informations pertinentes aux fins du traitement ([6]). Une organisation ne peut pas traiter des données à caractère personnel d'une manière qui est incompatible avec les objectifs pour lesquels elles ont été collectées ou avec les objectifs approuvés ultérieurement par la personne concernée. Toute organisation doit prendre les mesures qui s'imposent, dans la limite nécessaire à la réalisation de ces objectifs, pour assurer la fiabilité des données à caractère personnel par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité. Une organisation doit respecter les principes aussi longtemps qu'elle conserve ces informations.

b. Des informations peuvent être conservées sous une forme identifiant la personne concernée ou la rendant identifiable ([7]) uniquement tant que cette conservation sert à atteindre l'objectif de traitement au sens du point 5 a). Cette restriction n'empêche pas les organisations de traiter des informations à caractère personnel pour des durées plus longues aussi longtemps que, et dans la mesure où, ce traitement vise raisonnablement à atteindre les finalités suivantes: archivage dans l'intérêt public, journalisme, littérature et art, recherche scientifique ou historique, et analyse statistique. Dans ces cas, le traitement est soumis aux autres principes et dispositions du cadre du CPD UE — États-Unis. Les organisations devraient prendre des mesures raisonnables et adéquates lorsqu'elles respectent cette disposition.

6. **ACCÈS**

a. Lorsqu'une organisation détient des informations à caractère personnel sur une personne, celle-ci doit avoir accès à ces données et doit pouvoir les corriger, les modifier ou les supprimer lorsqu'elles sont inexactes ou lorsqu'elles ont été traitées d'une façon contraire aux principes. Font toutefois exception à cette règle les cas où la charge de travail ou la dépense qu'occasionnerait le droit d'accès sont disproportionnées par rapport aux risques pesant sur la vie privée de la personne concernée ainsi que les cas susceptibles d'entraîner une violation des droits d'autres personnes.

7. **VOIES DE RECOURS, APPLICATION ET RESPONSABILITÉ**

a. Pour protéger efficacement la vie privée, il convient notamment de mettre au point des mécanismes robustes permettant d'assurer le respect des principes, de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les organisations qui n'ont pas appliqué les principes alors qu'elles s'y sont engagées. Ces mécanismes doivent comprendre au minimum:

i. des mécanismes de recours indépendants aisément accessibles, permettant d'examiner et de trancher toute réclamation et tout litige, rapidement et sans frais pour les personnes concernées, en se référant aux principes et d'accorder des dédommagements lorsque la loi applicable ou les initiatives du secteur privé le prévoient;

ii. des procédures de suivi permettant de vérifier que les attestations et les déclarations des organisations relatives à leurs pratiques en matière de protection de la vie privée sont exactes et que ces pratiques sont mises en œuvre conformément aux déclarations des organisations et, en particulier, en ce qui concerne les cas de non-conformité; et

iii. des dispositions aux termes desquelles les organisations qui affirment souscrire aux principes sont tenues de résoudre les problèmes qui découlent du non-respect de ceux-ci et d'assumer les conséquences qui en résultent. Les sanctions doivent être suffisamment dissuasives pour garantir le respect des principes par les organisations.

b. Les organisations et les mécanismes de recours indépendant qu'elles ont sélectionnés doivent réagir rapidement aux questions et aux demandes d'informations émanant du ministère concernant le CPD UE — États-Unis. Toutes les organisations doivent répondre sans retard aux réclamations concernant le respect des principes que les autorités des États membres de l'Union leur transmettent par l'intermédiaire du ministère. Les organisations qui ont choisi de coopérer avec des APD, notamment les organisations qui traitent des données concernant les ressources humaines, doivent répondre directement à ces autorités lorsqu'il s'agit d'examiner et de trancher des réclamations.

([6]) Selon les circonstances, les finalités de traitement compatibles peuvent par exemple comprendre celles qui ont raisonnablement pour objectif les relations avec la clientèle, le respect de la réglementation et les considérations juridiques, l'audit, la sécurité et la prévention de la fraude, la préservation ou la défense des droits de l'organisation reconnus par la loi, ou d'autres finalités conformes aux attentes d'une personne raisonnable compte tenu du contexte dans lequel s'inscrit la collecte.

([7]) Dans ce contexte, si, compte tenu des moyens d'identification raisonnablement susceptibles d'être utilisés (en prenant entre autres en considération les frais et le temps nécessaires pour identifier la personne concernée ainsi que la technologie disponible au moment du traitement) et de la forme sous laquelle les données sont conservées, une personne concernée peut raisonnablement être identifiée par l'organisation, ou un tiers si celui-ci a accès aux données, on peut considérer que la personne concernée est «identifiable».

c. Les organisations sont tenues d'assurer l'arbitrage des réclamations et de respecter les conditions exposées à l'annexe I, pour autant qu'une personne ait demandé le recours à un arbitrage contraignant en le notifiant à l'organisation en cause et en suivant les procédures et en respectant les conditions exposées à l'annexe I.

d. Dans le contexte d'un transfert ultérieur, toute organisation participant au CPD UE — États-Unis assume la responsabilité du traitement des informations à caractère personnel qu'elle reçoit au titre de celui-ci et qu'elle transfère ultérieurement à un tiers agissant pour son compte en qualité de mandataire. L'organisation participant au CPD UE — États-Unis reste responsable au titre des principes si son mandataire traite ces informations à caractère personnel d'une manière non conforme aux principes, sauf si elle apporte la preuve qu'elle n'est pas responsable des événements donnant lieu au préjudice.

e. Toute organisation qui fait l'objet, au motif du non-respect des principes, d'une ordonnance judiciaire ou d'une ordonnance d'un organisme officiel américain (par exemple, la FTC ou le ministère des transports) mentionné dans les principes ou dans une future annexe aux principes est tenue de rendre publiques les parties liées au CPD UE — États-Unis de tout rapport de conformité ou d'évaluation soumis à au tribunal ou à l'organisme officiel américain dans les limites des exigences de confidentialité. Le ministère a mis en place un point de contact spécifique que les APD peuvent contacter pour tout problème de non-conformité par les organisations participant au CPD UE — États-Unis. La FTC et le ministère des transports examineront en priorité les dossiers de non-conformité avec les principes déférés par le ministère et par les autorités des États membres de l'Union et échangeront sans retard des informations relatives à chaque dossier avec les autorités de l'État membre qui a soumis le dossier, dans le respect des restrictions de confidentialité en vigueur.

III. PRINCIPES COMPLÉMENTAIRES

1. Données sensibles

a. Une organisation n'est pas tenue d'obtenir un consentement explicite et positif à l'égard de données sensibles dans les cas où le traitement est:

i. dans l'intérêt vital de la personne concernée ou d'une autre personne;

ii. nécessaire à la constatation d'un droit ou d'une défense en justice;

iii. nécessaire pour dispenser des soins médicaux à des fins de diagnostic;

iv. effectué au cours d'activités légitimes par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, et à condition que le traitement se rapporte aux seuls membres de l'organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées;

v. nécessaire aux fins de respecter les obligations de l'organisation en matière de droit du travail; ou

vi. lié à des données manifestement rendues publiques par la personne concernée.

2. Exceptions journalistiques

a. Compte tenu des garanties qu'offre la Constitution américaine en ce qui concerne la liberté de la presse, lorsque les droits de la presse visés dans le premier amendement à la Constitution des États-Unis ne sont pas compatibles avec la protection de la vie privée, le premier amendement doit primer pour les activités qui sont le fait de personnes ou d'organisations américaines.

b. Les informations à caractère personnel qui sont collectées à des fins de publication, de diffusion ou d'autres formes de communication publique, qu'elles soient utilisées ou non, ainsi que les informations qui ont été publiées antérieurement, puis archivées ne sont pas soumises aux principes.

3. Responsabilité secondaire

a. Les fournisseurs d'accès à l'internet (FAI), les sociétés de télécommunications et d'autres organismes ne sont pas soumis aux principes lorsqu'ils se limitent à transmettre, acheminer, remplacer ou masquer des informations pour le compte d'un autre organisme. Le CPD UE — États-Unis ne fait pas naître de responsabilité secondaire. Dans la mesure où une organisation sert uniquement de vecteur à des données transmises par des tiers et ne détermine ni les buts ni les moyens de traitement de ces données à caractère personnel, sa responsabilité ne peut être engagée.

4. **Mesures de diligence raisonnable et réalisation d'audits**

a. Les activités des commissaires aux comptes et des banques d'investissement peuvent impliquer le traitement de données à caractère personnel sans le consentement ou à l'insu de la personne concernée. Les principes «Notification», «Choix» et «Accès» l'autorisent dans les circonstances décrites ci-dessous.

b. Les sociétés cotées en bourse et les entreprises non cotées, parmi lesquelles des organisations participant au CPD UE — États-Unis, font régulièrement l'objet d'audits. Ces audits, en particulier ceux qui examinent d'éventuelles malversations, pourraient être mis en péril par une divulgation prématurée. De même, une organisation participant au CPD UE — États-Unis qui se trouve impliquée dans une fusion ou une acquisition potentielle doit prendre des mesures de «diligence raisonnable» ou se soumettre à de telles mesures. Cette procédure nécessite souvent la collecte et le traitement de données à caractère personnel, par exemple des informations relatives aux dirigeants et aux autres membres clés du personnel. Une divulgation prématurée pourrait entraver la transaction envisagée, voire enfreindre la législation boursière en vigueur. Les banques d'investissement et les avocats qui assurent les démarches de diligence raisonnable, ainsi que les commissaires aux comptes chargés d'un audit, peuvent traiter des informations à l'insu de la personne concernée, uniquement dans la mesure et pendant la durée nécessaires pour satisfaire à des dispositions réglementaires ou à des exigences liées à l'intérêt général ainsi que dans d'autres circonstances où l'application de ces principes porterait atteinte aux intérêts légitimes de l'organisme. Parmi ces intérêts légitimes figurent la surveillance du respect, par les organisations, de leurs obligations légales et de leurs activités comptables légitimes ainsi que la confidentialité qui doit être observée dans le contexte d'éventuelles acquisitions, fusions, coentreprises ou d'autres transactions de nature comparable effectuées par les banques d'investissement ou les commissaires aux comptes.

5. **Rôle des autorités chargées de la protection des données**

a. Les organisations respecteront leur engagement à coopérer avec les APD selon les modalités décrites ci-dessous. Dans le cadre du CPD UE — États-Unis, les organisations américaines recevant des données à caractère personnel en provenance de l'Union doivent s'engager à utiliser des mécanismes efficaces assurant le respect des principes. Plus précisément, comme le prévoit le principe «Voies de recours, application et responsabilité», les organisations participantes doivent prévoir: a) i) des voies de recours pour les personnes auxquelles les données se réfèrent; a) ii) des procédures de suivi permettant de vérifier que les affirmations et les déclarations qu'elles ont faites en ce qui concerne le respect de la vie privée sont exactes; et a) iii) des déclarations faisant obligation de résoudre les problèmes résultant du non-respect des principes et prévoyant des sanctions pour les contrevenants. Une organisation peut satisfaire aux points a) i) et a) iii) du principe «Voies de recours, application et responsabilité» si elle adhère aux exigences énoncées ici pour la coopération avec les APD.

b. Une organisation s'engage à coopérer avec les APD en indiquant, dans la déclaration d'autocertification aux fins du CPD UE — États-Unis qu'elle adresse au ministère du commerce (voir principe complémentaire «Autocertification»), qu'elle:

i. décide de se conformer aux dispositions des points a) i) et a) iii) du principe «Voies de recours, application et responsabilité» en s'engageant à coopérer avec les APD;

ii. coopérera avec les APD pour examiner et trancher les réclamations introduites au titre des principes; et

iii. suivra tout avis donné par les APD selon lequel l'organisation doit prendre des mesures spécifiques pour respecter les principes, y compris toute mesure de réparation ou d'indemnisation au bénéfice des personnes qui ont subi un préjudice en raison du non-respect desdits principes, et confirmera par écrit aux APD que lesdites mesures ont été prises.

c. Fonctionnement des panels d'APD

i. La coopération des APD prendra la forme d'informations et d'avis donnés selon les modalités suivantes:

1. Les APD seront consultées par l'intermédiaire d'un panel informel d'APD établi au niveau de l'Union qui, notamment, contribuera à définir une approche harmonisée et cohérente.

2. Le panel conseillera les organisations américaines concernées au sujet de réclamations en suspens introduites par des personnes et portant sur le traitement d'informations à caractère personnel qui ont été transférées au départ de l'Union européenne au titre du CPD UE — États-Unis. Les conseils donnés viseront à assurer une application correcte des principes et contiendront également des mécanismes de règlement des litiges que les APD jugeront appropriés pour la ou les personnes concernées.

3. Le panel donnera son avis en réponse à des renvois formés par les organisations concernées et/ou à des réclamations introduites directement par des personnes contre des organisations qui se sont engagées à coopérer avec les APD aux fins du respect des principes du CPD UE — États-Unis, tout en encourageant et, s'il y a lieu, en aidant ces personnes à faire d'abord usage des mécanismes internes de traitement des réclamations dont l'organisation dispose.

4. L'avis ne sera donné qu'après avoir mis les deux parties en mesure de présenter leurs observations et, le cas échéant, de produire leurs moyens de preuve. Le panel veillera à donner son avis dans les meilleurs délais tout en respectant les principes du procès équitable. En principe, le panel se prononcera au plus tard dans un délai de soixante jours à compter de la réception de la réclamation ou du renvoi.

5. S'il le juge approprié, le panel rendra publics les résultats de l'examen des réclamations dont il a été saisi.

6. L'avis du panel n'engage ni le panel ni les APD qui le composent.

ii. Les organisations optant pour ce mode de règlement des litiges doivent s'engager à se conformer aux avis émis par les APD. Si une organisation ne s'exécute pas dans un délai de vingt-cinq jours à compter de la notification de l'avis sans pouvoir fournir de motif valable, le panel pourra décider de renvoyer l'affaire à la FTC, au ministère des transports ou à un autre organisme officiel américain ou de conclure à un manquement grave à l'engagement de coopérer, lequel devra, en conséquence, être considéré comme nul et non avenu. Dans le dernier cas, le panel informera le ministère afin que celui-ci corrige la liste du cadre de protection des données. Tout manquement à l'engagement de coopérer avec les APD ainsi que tout non-respect des principes seront considérés comme constitutifs d'un acte frauduleux en vertu de l'article 5 du FTC Act (15 U.S.C. § 45), du titre 49 U.S.C., § 41712, ou de lois équivalentes.

d. Une organisation qui souhaite utiliser les avantages conférés par son adhésion au CPD UE — États-Unis pour couvrir les données relatives aux ressources humaines transférées depuis l'Union dans le contexte d'une relation de travail doit s'engager à coopérer avec les APD en ce qui concerne ces données (voir principe complémentaire «Données relatives aux ressources humaines»).

e. Les organisations optant pour cette formule devront verser une cotisation annuelle qui sera destinée à couvrir les frais de gestion du panel. Elles pourront également, le cas échéant, être invitées à participer aux frais de traduction résultant de l'examen, par le panel, des renvois et des réclamations introduites contre elles. La cotisation annuelle sera déterminée par le ministère après consultation de la Commission. La perception de la cotisation peut être effectuée par un tiers choisi par le ministère pour être le dépositaire des fonds collectés à cette fin. Le ministère coopérera étroitement avec la Commission et les APD sur l'établissement de procédures appropriées pour la distribution des fonds collectés au moyen de la cotisation, ainsi que sur d'autres aspects procéduraux et administratifs du panel. Le ministère et la Commission peuvent convenir de modifier la fréquence de perception de la cotisation.

6. **Autocertification**

a. Une organisation peut prétendre aux avantages du CPD UE — États-Unis dès le moment où le ministère l'inscrit sur la liste du cadre de protection des données. Le ministère n'inscrira une organisation sur la liste du cadre de protection des données qu'après avoir déterminé que sa déclaration d'autocertification initiale est complète, et il la supprimera de la liste si l'organisation se retire volontairement, manque à son obligation de recertification annuelle ou ne respecte pas les principes de manière persistante (*voir* principe complémentaire «Résolution des litiges et application des décisions»).

b. Pour autocertifier ou, par la suite, recertifier son adhésion au CPD UE — États-Unis, une organisation doit remettre au ministère une déclaration signée par un dirigeant de l'organisation qui autocertifie ou recertifie (le cas échéant) son adhésion aux principes ([8]), contenant au moins les informations suivantes:

([8]) La déclaration doit être effectuée via le site web du cadre de protection des données du ministère par une personne au sein de l'organisation qui est autorisée à faire des déclarations au nom de l'organisation et de toutes ses entités couvertes concernant son adhésion aux principes.

i. le nom de l'organisation américaine présentant la déclaration d'autocertification ou de recertification, ainsi que le ou les noms de ses entités ou filiales américaines adhérant également aux principes que l'organisation souhaite couvrir;

ii. une description des activités de l'organisation en lien avec les informations à caractère personnel qui seraient reçues de l'Union en vertu du CPD UE — États-Unis;

iii. une description de la politique en matière de protection de la vie privée de l'organisation appliquée par l'organisation auxdites informations, précisant:

1. si l'organisation possède un site web public, l'adresse web à laquelle cette politique est accessible ou, si l'organisation ne possède pas de site web public, le lieu où le texte de cette politique peut être consulté par le public, et

2. la date de mise en œuvre effective de cette politique;

iv. le service à contacter au sein de l'organisation en cas de réclamation, pour des demandes d'accès et pour toute autre question relevant des principes ([9]), notamment:

1. le ou les noms, la ou les fonctions, l'adresse ou les adresses électroniques et le ou les numéros de téléphone de la ou des personnes de contact ou du ou des services à contacter au sein de l'organisation, et

2. l'adresse postale de l'organisation aux États-Unis;

v. le nom de l'organisme officiel spécifique compétent pour connaître des plaintes déposées, le cas échéant, contre l'organisation pour pratiques déloyales ou frauduleuses et pour infraction aux lois ou aux réglementations régissant la protection de la vie privée (et qui est mentionnée dans les principes ou une future annexe aux principes);

vi. l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation;

vii. la méthode de vérification (par exemple, l'autoévaluation ou des contrôles extérieurs de la conformité, y compris le tiers qui effectue ces contrôles) ([10]); et

viii. le ou les mécanismes de recours indépendants qui pourront instruire les réclamations en suspens liées aux principes ([11]).

c. Une organisation peut étendre les avantages du CPD UE — États-Unis à des informations relatives aux ressources humaines qui sont transférées depuis l'Union afin d'être utilisées dans le cadre de relations de travail, lorsque l'un des organismes officiels mentionnés dans les principes ou une future annexe aux principes est compétent pour connaître des plaintes déposées contre l'organisation en raison du traitement des informations relatives aux ressources humaines. En outre, l'organisation doit indiquer dans sa déclaration d'autocertification initiale, ainsi que dans toute déclaration de recertification, qu'elle désire couvrir de telles informations, qu'elle s'engage à coopérer avec les autorités compétentes de l'Union européenne conformément aux termes des principes complémentaires «Données relatives aux ressources humaines» et «Rôle des autorités chargées de la protection des données», et qu'elle observera les conseils donnés par ces autorités. L'organisation doit également fournir au ministère une copie de sa politique en matière de protection de la vie privée concernant les ressources humaines et indiquer le lieu où cette politique peut être consultée par les salariés concernés.

([9]) Le «contact principal au sein de l'organisation» ou le «dirigeant de l'organisation» ne peut pas être extérieur à l'organisation (par exemple, un avocat ou un consultant externe).

([10]) *Voir* principe complémentaire «Vérification».

([11]) *Voir* principe complémentaire «Résolution des litiges et application des décisions».

d. Le ministère tiendra et mettra à la disposition du public la liste du cadre de protection des données énumérant les organisations qui ont déposé des déclarations d'autocertification initiales complètes et mettra cette liste à jour sur la base des déclarations annuelles de recertification complètes, ainsi que des notifications reçues conformément au principe complémentaire «Résolution des litiges et application des décisions». Les déclarations de recertification doivent être déposées au moins une fois par an; à défaut, l'organisation sera supprimée de la liste du cadre de protection des données et ne bénéficiera plus des avantages découlant du CPD UE — États-Unis. Toute organisation inscrite sur la liste du cadre de protection des données par le ministère doit disposer d'une politique en matière de protection de la vie privée qui respecte le principe «Notification» et mentionner, dans cette politique, qu'elle adhère aux principes ([12]). Si elle est disponible en ligne, la politique en matière de protection de la vie privée d'une organisation doit inclure un hyperlien vers le site web du cadre de protection des données du ministère et un hyperlien vers le site ou le formulaire d'introduction d'une réclamation du mécanisme de recours indépendant qui pourra instruire gratuitement pour les personnes les réclamations en suspens liées aux principes.

e. Les principes s'appliquent dès l'autocertification. Les organisations participantes qui ont antérieurement autocertifié leur respect des principes du bouclier de protection des données devront mettre à jour leur politique en matière de protection de la vie privée pour qu'elle fasse désormais référence aux «principes du cadre de protection des données UE — États-Unis». Ces organisations doivent inclure cette référence dès que possible et, en tout état de cause, au plus tard trois mois après la date d'entrée en vigueur des principes du cadre de protection des données UE — États-Unis.

f. Une organisation doit appliquer les principes à toutes les données à caractère personnel reçues depuis l'Union sur la foi du CPD UE — États-Unis. L'engagement d'adhérer aux principes n'est pas limité dans le temps en ce qui concerne les données à caractère personnel reçues au cours de la période durant laquelle l'organisation bénéficie des avantages du CPD UE — États-Unis; son engagement signifie qu'elle continuera à appliquer les principes à ces données aussi longtemps qu'elle stockera, utilisera ou divulguera celles-ci, même si elle quitte ultérieurement le CPD UE — États-Unis pour quelque raison que ce soit. Une organisation qui souhaite se retirer du CPD UE — États-Unis doit le notifier à l'avance au ministère. Cette notification doit également indiquer ce que l'organisation compte faire avec les données à caractère personnel qu'elle a reçues sur la foi du CPD UE — États-Unis (à savoir, conserver, restituer ou supprimer les données, et dans le cas où elle conserve les données, les moyens autorisés par lesquels elle assurera la protection des données). Une organisation qui se retire du CPD UE — États-Unis mais qui souhaite conserver ces données doit déclarer annuellement au ministère son engagement à continuer d'appliquer les principes ou à assurer une protection «adéquate» des données par un autre moyen autorisé (par exemple en utilisant un contrat qui reflète pleinement les exigences des clauses contractuelles standard adoptées par la Commission); dans le cas contraire, l'organisation doit restituer ou supprimer les données concernées ([13]). Une organisation qui se retire du CPD UE — États-Unis doit supprimer de toute politique en matière de protection de la vie privée concernée toute référence à celui-ci donnant à penser que l'organisation continue de participer au CPD UE — États-Unis et peut prétendre à ses avantages.

([12]) Une organisation qui autocertifie son adhésion au CPD UE — États-Unis pour la première fois ne peut prétendre participer à celui-ci dans sa politique finale en matière de protection de la vie privée tant que le ministère ne l'a pas autorisée à le faire. L'organisation doit fournir au ministère un projet de politique en matière de protection de la vie privée conforme aux principes lorsqu'elle soumet sa déclaration d'autocertification initiale. Une fois que le ministère aura déterminé que la déclaration d'autocertification initiale de l'organisation est complète, il informera l'organisation qu'elle doit finaliser (par exemple, publier s'il y a lieu) sa politique en matière de protection de la vie privée conforme au CPD UE — États-Unis. Dès que sa politique en matière de protection de la vie privée est finalisée, l'organisation doit en informer le ministère sans délai, après quoi le ministère l'inscrira sur la liste du cadre de protection des données.

([13]) Si une organisation choisit, au moment de son retrait, de conserver les données à caractère personnel qu'elle a reçues sur la foi du CPD UE — États-Unis et déclare annuellement au ministère qu'elle continue d'appliquer les principes à ces données, l'organisation doit indiquer au ministère une fois par an après son retrait (c'est-à-dire jusqu'à ce que l'organisation assure une protection «adéquate» de ces données par un autre moyen autorisé, ou restitue ou supprime toutes ces données et notifie cette action au ministère) ce qu'elle a fait de ces données à caractère personnel, ce qu'elle compte faire de toutes les données à caractère personnel qu'elle continue à conserver, et qui servira de point de contact permanent pour les questions relatives aux principes.

g. Une organisation qui cessera d'exister en tant qu'entité juridique distincte en raison d'un changement de statut, par exemple à la suite d'une opération de fusion, d'une opération d'absorption, d'une faillite ou d'une dissolution, doit le notifier à l'avance au ministère. La notification devrait également indiquer si l'entité issue du changement de statut i) continuera de participer au CPD UE — États-Unis dans le cadre d'une autocertification existante; ii) autocertifiera son adhésion aux principes en tant que nouvelle organisation participant au CPD UE — États-Unis (par exemple, lorsque la nouvelle entité ou l'entité survivante ne dispose pas déjà d'une autocertification lui permettant de participer au CPD UE — États-Unis); ou iii) mettra en place d'autres garanties telles qu'un accord écrit certifiant qu'elle continuera d'appliquer les principes à toutes les données à caractère personnel que l'organisation a reçues dans le cadre du CPD UE — États-Unis et qu'elle conservera. Si aucune des solutions visées aux points i), ii) et iii) n'est mise en œuvre, toute donnée à caractère personnel reçue dans le cadre du CPD UE — États-Unis doit être restituée ou effacée sans tarder.

h. Une organisation qui se retire du CPD UE — États-Unis pour quelque raison que ce soit doit supprimer toute déclaration donnant à penser qu'elle continue de participer au CPD UE — États-Unis ou qu'elle peut prétendre aux avantages du CPD UE — États-Unis. La marque de certification du CPD UE — États-Unis, dans les cas où elle est utilisée, doit également être supprimée. Toute fausse déclaration au grand public concernant l'adhésion d'une organisation aux principes peut donner lieu à des poursuites devant la FTC, le ministère des transports ou toute autre instance administrative compétente. Toute fausse déclaration au ministère peut donner lieu à des poursuites au titre de la loi sur les fausses déclarations (18 U.S.C., § 1001).

7. **Vérification**

a. Les organisations sont tenues de prévoir des procédures de suivi afin de vérifier que leurs attestations et déclarations relatives à leurs pratiques en matière de protection de la vie privée en vertu du CPD UE — États-Unis sont exactes et que ces pratiques ont été mises en œuvre comme elles l'ont annoncé et conformément aux principes.

b. Pour répondre aux exigences de vérification du principe «Voies de recours, application et responsabilité», une organisation doit vérifier les attestations et déclarations de ce type en organisant une autoévaluation ou un contrôle extérieur de la conformité.

c. Si l'organisation opte pour l'autoévaluation, la vérification doit démontrer que sa politique en matière de protection de la vie privée, en ce qui concerne les informations à caractère personnel reçues de l'Union, est appropriée, complète, facilement accessible, qu'elle est conforme aux principes et qu'elle est totalement mise en œuvre (c'est-à-dire respectée). Elle doit aussi montrer que les personnes sont informées de l'existence de tout mécanisme interne de traitement des réclamations et des mécanismes de recours indépendants par le truchement desquels ils peuvent diligenter leurs réclamations, que l'organisation dispose de procédures de formation des salariés à cet effet et que des sanctions leur sont infligées s'ils ne les respectent pas, et qu'il existe des procédures internes visant à contrôler régulièrement et objectivement la conformité avec ce qui précède. Une déclaration confirmant que l'autoévaluation a été menée à bien doit être signée au moins une fois par an par un responsable de la société ou tout autre représentant mandaté et transmise à la demande des personnes concernées ou dans le cadre d'une enquête ou d'une réclamation pour non-conformité.

d. Si l'organisation opte pour un contrôle extérieur de la conformité, la vérification doit démontrer que sa politique de protection de la vie privée, en ce qui concerne les informations à caractère personnel reçues de l'Union, est appropriée, complète, facilement accessible, qu'elle est conforme aux principes et qu'elle est totalement mise en œuvre (c'est-à-dire respectée). Elle doit aussi montrer que les particuliers sont informés du ou des mécanismes leur permettant d'introduire des réclamations. Les méthodes utilisées sont diverses. Il peut s'agir (liste non exhaustive) d'un audit, d'une vérification menée de façon aléatoire, de l'utilisation de «leurres» ou d'outils technologiques. Une déclaration confirmant qu'un contrôle extérieur de la conformité a été mené à bien doit être signée au moins une fois par an par le contrôleur, le responsable de la société ou tout autre représentant mandaté et transmise à la demande des personnes concernées ou dans le cadre d'une enquête ou d'une réclamation pour non-conformité.

e. Les organisations doivent conserver des archives sur la mise en œuvre de leurs pratiques relatives à la protection de la vie privée en vertu du CPD UE — États-Unis et remettre celles-ci sur demande, dans le cadre d'une enquête ou d'une réclamation pour non-conformité, à l'organe indépendant de règlement des litiges responsable de l'examen des réclamations ou à l'agence compétente en matière de pratiques déloyales et frauduleuses. Les organisations doivent également répondre rapidement aux questions et autres demandes d'informations émanant du ministère concernant leur respect des principes.

8. **Accès**

a. Le principe «Accès» dans la pratique

i. Conformément aux principes, le droit d'accès est un élément fondamental de la protection de la vie privée. Il permet, notamment, à chaque personne de vérifier l'exactitude des informations la concernant. Le principe «Accès» signifie que les personnes ont le droit:

1. d'obtenir d'une organisation la confirmation du fait que cette organisation traite ou non des données à caractère personnel les concernant ([14]);

2. de se faire communiquer ces données afin de pouvoir vérifier leur exactitude et la licéité du traitement; et

3. d'obtenir la correction, la modification ou la suppression des données inexactes ou traitées d'une manière contraire aux principes.

ii. Les personnes concernées ne sont pas tenues de justifier une demande d'accès à leurs propres données. Lorsqu'elle répond aux demandes d'accès individuelles, l'organisation doit avant tout être guidée par la ou les motivations de leur auteur. Par exemple, si une demande d'accès est vague ou a une portée très large, l'organisation peut engager un dialogue avec le demandeur afin de mieux comprendre sa démarche et de trouver les informations appropriées. L'organisation peut chercher à déterminer avec quels services la personne concernée a eu des contacts ou quelle est la nature ou l'utilisation des informations qui font l'objet de la demande d'accès.

iii. Le droit d'accès étant par nature un élément fondamental de la protection de la vie privée, les organisations doivent, toujours et en toute bonne foi, faire des efforts pour fournir l'accès. Par exemple, s'il convient de protéger certaines informations et que celles-ci peuvent être aisément séparées des informations à caractère personnel qui font l'objet d'une demande d'accès, l'organisation doit procéder à la séparation des données confidentielles et répondre à la demande en rendant les autres informations disponibles. Si l'organisation décide de restreindre l'accès dans un cas précis, elle doit motiver sa décision et communiquer les coordonnées d'une personne à contacter pour plus d'informations.

b. Charge de travail ou dépense occasionnée par l'accès

i. Le droit d'accès aux informations à caractère personnel peut être restreint dans des circonstances exceptionnelles, dans les cas où la charge de travail ou la dépense qu'occasionnerait le droit d'accès sont disproportionnées par rapport aux risques pesant sur la vie privée de la personne concernée ainsi que les cas susceptibles d'entraîner une violation des droits d'autres personnes. Les coûts et la charge constituent des facteurs importants qui sont à prendre en compte, mais qui ne sont pas décisifs lorsqu'il s'agit de déterminer le caractère raisonnable de l'accès.

ii. Ainsi, conformément aux autres dispositions des présents principes complémentaires, si les informations à caractère personnel sont utilisées pour prendre des décisions qui auront des conséquences majeures pour la personne (par exemple, le refus ou l'octroi d'avantages importants, tels qu'une assurance, une hypothèque ou un emploi), l'organisation est tenue de les communiquer, même si cela s'avère relativement difficile ou coûteux. Lorsque les informations à caractère personnel demandées ne sont pas sensibles ou ne sont pas utilisées pour prendre des décisions qui auront des conséquences majeures pour la personne, mais qu'elles sont aisément disponibles et que leur transmission est peu coûteuse, l'organisation est tenue de permettre l'accès à ces informations.

c. Informations commerciales confidentielles

i. Les informations commerciales confidentielles sont des informations qu'une organisation veille à ne pas divulguer car elles favoriseraient ses concurrents. Les organisations peuvent refuser ou limiter l'accès si elles craignent de voir divulguées leurs informations commerciales confidentielles – notamment les inférences ou les classifications commerciales établies par l'organisation – ou des informations commerciales confidentielles appartenant à d'autres organisations et soumises à une obligation contractuelle de confidentialité.

([14]) Les organisations devraient répondre aux questions de personnes concernées portant sur les finalités du traitement, les catégories de données à caractère personnel sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données à caractère personnel sont communiquées.

ii. Si les informations commerciales confidentielles peuvent être aisément séparées des autres informations à caractère personnel qui font l'objet d'une demande d'accès, l'organisation devrait expurger les informations confidentielles et rendre accessibles les informations non confidentielles.

d. Organisation de bases de données

i. L'accès peut être fourni sous la forme de la communication des informations à caractère personnel concernées par l'organisation à la personne concernée et n'implique pas obligatoirement que cette dernière consulte la base de données de l'organisation.

ii. L'accès ne doit être fourni que dans la mesure où l'organisation stocke les informations à caractère personnel. Le principe «Accès» ne crée en soi aucune obligation de conservation, de gestion, de réorganisation ou de restructuration des fichiers d'informations à caractère personnel.

e. Circonstances permettant de restreindre l'accès

i. Étant donné que les organisations sont toujours tenues de faire des efforts de bonne foi pour permettre aux personnes d'accéder à leurs données à caractère personnel, les circonstances dans lesquelles les organisations peuvent restreindre cet accès sont limitées et toute restriction d'accès doit être motivée par des raisons précises. Tout comme en vertu du RGPD, l'organisation peut restreindre l'accès à certaines informations pour autant que leur diffusion risque de porter atteinte à d'importants intérêts publics, tels que la sécurité nationale, la défense ou la sécurité publique. L'accès peut également être refusé lorsque les informations à caractère personnel sont traitées uniquement à des fins statistiques ou de recherche. D'autres motifs justifient le refus ou la limitation de l'accès:

1. une entrave à l'exécution ou à l'application de la loi ou aux actions civiles en justice, notamment à la prévention de la criminalité, à la détection des infractions et délits et aux enquêtes y afférentes ou encore au droit à un procès équitable;

2. les cas où la divulgation entraînerait une violation des droits légitimes ou d'intérêts importants de tiers;

3. le non-respect d'une obligation ou d'un privilège légal ou professionnel;

4. une entrave aux enquêtes sur la sécurité des employés et aux procédures d'arbitrage, ou lors de l'organisation des remplacements et des restructurations; ou

5. le fait de porter atteinte à la confidentialité nécessaire au contrôle, à l'inspection ou aux fonctions réglementaires en rapport avec une gestion saine, ou dans le cadre de négociations futures ou en cours impliquant l'organisation.

ii. Il incombe à l'organisation qui invoque l'exception d'en prouver le bien-fondé, d'indiquer les motifs de la limitation de l'accès et de communiquer les coordonnées d'une personne à contacter pour plus d'informations.

f. Droit d'obtenir une confirmation de possession d'informations et possibilité de rendre l'accès payant pour couvrir les frais

i. Toute personne a le droit d'obtenir la confirmation qu'une organisation possède ou non des données à caractère personnel la concernant. Toute personne a également le droit de se faire communiquer les données à caractère personnel la concernant. Les organisations peuvent demander le paiement d'une redevance, pour autant qu'elle ne soit pas excessive.

ii. Le fait d'exiger le paiement d'une redevance peut être justifié, par exemple, dans le cas de demandes manifestement excessives, en particulier du fait de leur caractère répétitif.

iii. L'accès ne peut pas être refusé pour des raisons de coût si la personne concernée propose de prendre en charge les frais occasionnés.

g. Demandes d'accès répétitives ou vexatoires

i. Une organisation peut fixer une limite acceptable au nombre de demandes d'accès déposées au cours d'une période donnée. Lorsqu'elle fixe ces limites, l'organisation doit tenir compte de facteurs tels que la fréquence de mise à jour des informations, le but de l'utilisation des données et la nature des informations.

h. Demandes d'accès frauduleuses

i. L'organisation n'est pas tenue de fournir l'accès si elle ne reçoit pas les informations nécessaires à l'identification du demandeur.

i. Délai de réponse

i. Les organisations doivent répondre aux demandes d'accès dans un délai raisonnable, de façon raisonnable et sous une forme aisément compréhensible pour la personne concernée. Une organisation qui fournit des informations aux personnes concernées à intervalles réguliers peut répondre à une demande d'accès individuelle dans le cadre de sa communication régulière si cela n'entraîne pas de délai excessif.

9. **Données relatives aux ressources humaines**

a. Couverture par le CPD UE — États-Unis

i. Si une organisation située dans l'Union transfère des informations à caractère personnel relatives à ses salariés (actuels ou anciens) collectées dans le cadre d'une relation de travail à une société mère, affiliée ou non affiliée qui fournit des services aux États-Unis et qui participe au CPD UE — États-Unis, ce transfert bénéficie des avantages du CPD UE — États-Unis. Dans ce cas, la collecte d'informations ainsi que leur traitement avant le transfert sont soumis aux lois nationales de l'État membre de l'Union où la collecte est réalisée et toutes les conditions ou les restrictions fixées en la matière par celles-ci doivent être respectées.

ii. Les principes ne sont pertinents qu'en cas de transfert ou d'accès à des dossiers individuels identifiés ou identifiables. Les rapports statistiques fondés sur les données agrégées en matière d'emploi et qui ne contiennent pas de données à caractère personnel ou qui utilisent des données rendues anonymes ne présentent pas de risques pour la vie privée.

b. Application des principes «Notification» et «Choix»

i. Une organisation américaine qui a reçu des informations en provenance de l'Union sur les salariés en vertu du CPD UE — États-Unis peut les communiquer à des tiers et/ou les utiliser à d'autres fins uniquement si les principes «Notification» et «Choix» sont respectés. Ainsi, si une organisation américaine veut utiliser les informations à caractère personnel collectées dans le cadre d'une relation de travail dans un but qui n'est pas lié à cette relation de travail – par exemple l'envoi de messages de marketing –, elle doit, au préalable, en laisser le choix aux personnes concernées, à moins que celles-ci n'aient déjà donné leur autorisation pour que les informations soient utilisées à de telles fins. Une telle utilisation ne peut pas être incompatible avec les finalités pour lesquelles les informations à caractère personnel ont été collectées ou avec les finalités approuvées ultérieurement par la personne concernée. En outre, l'employeur ne peut utiliser les choix exprimés pour entraver la carrière professionnelle de ses salariés ou prendre des sanctions à leur égard.

ii. Il convient de signaler que certaines conditions applicables de manière générale au transfert à partir de quelques États membres de l'Union peuvent exclure d'autres utilisations de ces informations, même après leur transfert en dehors du territoire de l'Union, et que ces conditions doivent être respectées.

iii. Par ailleurs, les employeurs devraient s'efforcer raisonnablement de tenir compte des préférences du salarié en ce qui concerne la protection de sa vie privée. Il peut s'agir, par exemple, de restreindre l'accès aux données à caractère personnel, d'en rendre certaines anonymes ou de leur attribuer des codes ou pseudonymes lorsque l'objectif de gestion poursuivi ne requiert pas l'utilisation des vrais noms.

iv. Dans la mesure nécessaire et pour aussi longtemps que nécessaire, pour éviter de limiter les capacités de l'organisation dans le cadre de promotions, d'engagements ou d'autres décisions similaires relatives à l'emploi, une organisation n'est pas tenue de respecter les principes «Notification» et «Choix».

c. Application du principe «Accès»

i. Le principe complémentaire «Accès» fournit des indications sur les raisons qui peuvent justifier le refus ou la restriction de l'accès demandé dans le contexte des ressources humaines. Dans l'Union, les employeurs doivent naturellement respecter les réglementations locales et veiller à ce que les salariés de l'Union aient accès à ces informations, conformément à la loi de leur pays d'origine, quel que soit le lieu de traitement et de conservation des données. Dans le contexte du CPD UE — États-Unis, une organisation traitant de telles données aux États-Unis doit coopérer en fournissant cet accès, soit directement, soit par l'intermédiaire de l'employeur de l'Union.

d. Exécution

i. Dans la mesure où les informations à caractère personnel sont utilisées uniquement dans le cadre d'une relation de travail, la responsabilité principale des données vis-à-vis du salarié incombe toujours à l'organisation située dans l'Union européenne. C'est la raison pour laquelle, si un salarié européen se plaint du non-respect de son droit à la protection des données et n'est pas satisfait des résultats des procédures internes d'évaluation, de réclamation et d'appel (ou de toute procédure d'arbitrage applicable en vertu d'un contrat conclu avec un syndicat), il convient de l'orienter vers les autorités nationales responsables des questions du travail ou de la protection des données dans la juridiction où il travaille. Cela comprend les cas où le mauvais usage allégué de l'information personnelle relève de la responsabilité de l'organisation américaine qui a reçu l'information de l'employeur, et entraîne donc une violation alléguée des principes. C'est le moyen le plus efficace de résoudre les chevauchements qui existent souvent entre les droits et obligations définis par la législation du travail et les conventions collectives locales ainsi que par la loi relative à la protection des données.

ii. Une organisation américaine participant au CPD UE — États-Unis qui utilise des données relatives aux ressources humaines transférées à partir de l'Union dans le cadre d'une relation de travail et qui souhaite que ces transferts soient couverts par le CPD UE — États-Unis doit s'engager à cet effet à coopérer aux enquêtes des autorités compétentes de l'Union et à respecter l'avis de celles-ci.

e. Application du principe «Responsabilité en cas de transfert ultérieur»

i. Pour des besoins opérationnels liés à l'emploi occasionnel d'une organisation participant au CPD UE — États-Unis en ce qui concerne des données à caractère personnel transférées au titre de celui-ci, comme la réservation d'un vol, d'une chambre d'hôtel ou la couverture d'assurance, les données à caractère personnel d'un petit nombre d'employés peuvent être transférées aux responsables du traitement sans appliquer le principe «Accès» et sans conclure de contrat avec le responsable du traitement tiers (comme l'exige normalement le principe «Responsabilité en cas de transfert ultérieur»), pour autant que l'organisation participant au CPD UE — États-Unis ait respecté les principes «Notification» et «Choix».

10. **Contrats obligatoires pour les transferts ultérieurs**

a. Contrats de traitement de données

i. Le transfert de l'Union vers les États-Unis de données à caractère personnel uniquement pour des besoins de traitement nécessite un contrat, indépendamment de la participation du sous-traitant au CPD UE — États-Unis.

ii. Un contrat est toujours exigé de la part des responsables de traitement européens pour un transfert en vue d'un simple traitement, que cette opération soit effectuée à l'intérieur ou à l'extérieur de l'Union, et que le sous-traitant participe ou non au CPD UE — États-Unis. Le contrat a pour objet de faire en sorte que le sous-traitant:

1. n'agisse que sur instruction du responsable du traitement;

2. mette en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, et comprenne si un transfert ultérieur est autorisé ou non; et

3. compte tenu de la nature du traitement, aide le responsable du traitement à répondre aux personnes qui exercent leurs droits au titre des principes.

iii. Étant donné que les organisations participant au CPD UE — États-Unis assurent une protection adéquate, les contrats de simple traitement conclus avec ces dernières ne nécessitent pas d'autorisation préalable.

b. Transferts au sein d'un groupe contrôlé d'entreprises ou d'entités

i. Lorsque des informations à caractère personnel sont transférées entre deux responsables du traitement au sein d'un groupe contrôlé d'entreprises ou d'entités, un contrat n'est pas toujours requis en vertu du principe «Responsabilité en cas de transfert ultérieur». Les responsables du traitement au sein d'un groupe contrôlé d'entreprises ou d'entités peuvent fonder ces transferts sur d'autres instruments, comme les règles d'entreprise contraignantes de l'Union ou d'autres instruments intragroupe (par ex. les programmes de conformité et de contrôle), garantissant ainsi la continuité de la protection des informations à caractère personnel conformément aux principes. Dans le cas de tels transferts, l'organisation participant au CPD UE — États-Unis reste responsable du respect des principes.

c. Transferts entre responsables du traitement

i. Pour les transferts entre responsables du traitement, le responsable du traitement qui reçoit les données ne doit pas nécessairement être une organisation participant au CPD UE — États-Unis ni posséder de mécanisme de recours indépendant. L'organisation participant au CPD UE — États-Unis doit conclure, avec le responsable du traitement tiers qui reçoit les données, un contrat prévoyant un niveau de protection égal à celui requis en vertu du CPD UE — États-Unis, à ceci près que le responsable du traitement tiers ne doit pas être une organisation participant au CPD UE — États-Unis ni posséder de mécanisme de recours indépendant pour autant qu'il mette à disposition un mécanisme équivalent.

11. **Résolution des litiges et application des décisions**

a. Le principe «Voies de recours, application et responsabilité» fixe les exigences relatives à l'application du CPD UE — États-Unis. Le principe complémentaire «Vérification» explique la manière de satisfaire les exigences énoncées au point a) ii). Le présent principe complémentaire traite des points a) i) et a) iii), qui nécessitent tous deux des mécanismes de recours indépendants. Ces mécanismes peuvent prendre différentes formes, mais doivent répondre aux exigences énoncées au titre du principe «Voies de recours, application et responsabilité». Les organisations satisfont à ces exigences: i) en participant à des programmes du secteur privé en matière de protection de la vie privée intégrant dans leurs règles les principes et comportant des mécanismes de mise en œuvre efficaces, de même nature que ceux qui sont décrits dans le principe «Voies de recours, application et responsabilité»; ii) en se conformant aux instructions des organes légaux ou statutaires de surveillance qui assurent le traitement des réclamations de personnes et la résolution des litiges; ou iii) en s'engageant à coopérer avec les APD situées dans l'Union ou avec leurs représentants autorisés.

b. La présente liste a valeur indicative et n'est pas restrictive. Le secteur privé peut concevoir d'autres mécanismes de mise en œuvre pour autant que ceux-ci répondent aux exigences du principe «Voies de recours, application et responsabilité» ainsi qu'aux principes complémentaires. On notera que les exigences du principe «Voies de recours, application et responsabilité» s'ajoutent à l'exigence selon laquelle les mesures d'autoréglementation doivent être mises en application conformément à l'article 5 du FTC Act (15 U.S.C. § 45), qui interdit les pratiques déloyales ou frauduleuses, au titre 49 U.S.C., § 41712, qui interdit aux transporteurs et aux agents de billetterie toute pratique déloyale ou frauduleuse dans le domaine du transport aérien ou de la vente de transport aérien, ou à toute autre législation du même type.

c. Afin de garantir le respect de leurs engagements en vertu du CPD UE — États-Unis et de faciliter l'administration du programme, les organisations ainsi que leurs mécanismes de recours indépendants doivent fournir des informations relatives au CPD UE — États-Unis à la demande du ministère. En outre, les organisations doivent répondre sans retard aux réclamations relatives au respect des principes que les APD leur transmettent par l'intermédiaire du ministère. La réponse doit déterminer si la réclamation est fondée et, le cas échéant, comment l'organisation compte corriger le problème. Le ministère protégera la confidentialité des informations qu'il reçoit conformément au droit des États-Unis.

d. Mécanismes de recours

i. Les personnes devraient être encouragées à soumettre toute réclamation éventuelle à l'organisation concernée avant de faire appel à des mécanismes de recours indépendants. Les organisations doivent répondre aux personnes dans les 45 jours suivant la réception d'une réclamation. L'indépendance d'un mécanisme de recours est à apprécier selon des critères objectifs, notamment son impartialité, la transparence de sa composition et de son financement ou un bilan positif dans son domaine d'activité. Comme le prévoit le principe «Voies de recours, application et responsabilité», la voie de recours dont disposent les personnes doit être facilement accessible et gratuite. Les organes indépendants de règlement des litiges devraient étudier toutes les réclamations introduites par des personnes, à moins qu'elles ne soient manifestement non fondées ou abusives. Cette condition n'empêche pas l'établissement, par l'organe indépendant de règlement des litiges, de critères d'éligibilité, mais ceux-ci devraient être transparents et justifiés (ils pourraient viser, par exemple, à exclure les réclamations qui ne rentrent pas dans le champ d'application du programme ou qui relèvent des compétences d'une autre instance) et ne devraient pas avoir pour effet de compromettre l'engagement à examiner les réclamations légitimes. Les mécanismes de recours devraient, en outre, fournir aux personnes des informations complètes et facilement accessibles sur le fonctionnement de la procédure lors de l'introduction d'une réclamation. Ces informations devraient inclure une description des pratiques suivies en matière de protection de la vie privée, conformément aux principes. Les mécanismes devraient, en outre, coopérer en vue de mettre au point des outils, tels que des formulaires types de réclamation, destinés à faciliter le fonctionnement de la procédure de traitement des réclamations.

ii. Les mécanismes de recours indépendants doivent inclure sur leurs sites web publics des informations relatives aux principes et aux services qu'ils fournissent en vertu du CPD UE — États-Unis. Ces informations doivent comprendre: 1) des informations relatives aux exigences en matière de mécanismes de recours indépendants au titre des principes, ou un lien vers ces exigences; 2) un lien vers le site web «cadre de protection des données» du ministère; 3) l'indication que les services de règlement des litiges qu'elles proposent en vertu du CPD UE — États-Unis sont gratuits pour les personnes; 4) une description des modalités d'introduction d'une réclamation relative aux principes; 5) le délai de traitement des réclamations relatives aux principes; et 6) une description des possibilités de recours.

iii. Les mécanismes de recours indépendants doivent publier un rapport annuel présentant des statistiques agrégées relatives à leurs services de règlement des litiges. Ce rapport annuel doit indiquer: 1) le nombre total de réclamations relatives aux principes reçues au cours de l'année faisant l'objet du rapport; 2) les types de réclamations reçues; 3) des indicateurs de qualité du règlement des litiges, par exemple le délai de traitement des réclamations; et 4) les résultats du traitement des réclamations reçues, notamment le nombre et les types de recours et les sanctions infligées.

iv. Comme indiqué à l'annexe I, une personne peut opter pour l'arbitrage en vue de déterminer, pour les plaintes résiduelles, si une organisation participant au CPD UE — États-Unis n'a pas satisfait à ses obligations au titre des principes envers cette personne et si cette infraction reste entièrement ou partiellement sans réparation. Cette possibilité est offerte uniquement à ces fins. Elle n'est pas disponible, par exemple, en ce qui concerne les exceptions aux principes ([15]) ou en ce qui concerne une allégation relative à l'adéquation du CPD UE — États-Unis. Dans le cadre de cette option d'arbitrage, le «panel du cadre de protection des données UE — États-Unis» (composé d'un ou de trois arbitres, à la convenance des parties) est habilité à imposer une mesure de réparation équitable non pécuniaire propre à chaque personne (par exemple l'accès, la correction, la suppression ou la restitution des données concernées de cette personne) nécessaire pour remédier à la violation des principes uniquement en ce qui concerne cette personne. Les personnes et les organisations participant au CPD UE — États-Unis pourront demander le contrôle juridictionnel et l'application des décisions d'arbitrage conformément au droit américain au titre de la loi fédérale sur l'arbitrage (Federal Arbitration Act ou FAA).

e. Recours et sanctions

i. Tout recours auprès de l'organe indépendant de règlement des litiges devrait aboutir à l'annulation ou à la correction, dans la mesure du possible, des effets du non-respect des principes par l'organisation, au respect des principes lors des traitements futurs par cette même organisation et, s'il y a lieu, à l'arrêt du traitement des données à caractère personnel de la personne qui a introduit la réclamation. Les sanctions doivent être suffisamment dissuasives pour garantir le respect des principes de la part de l'organisation. Une série de sanctions ayant des degrés de sévérité différents permettra aux organes de règlement des litiges de répondre de manière adéquate à des niveaux différents de non-respect. Les sanctions doivent

([15]) Les principes, Vue d'ensemble, point 5.

inclure à la fois la publication des violations et l'obligation d'effacer les données dans certaines circonstances ([16]). D'autres sanctions pourraient être la suspension ou le retrait de l'agrément, l'indemnisation des pertes subies par les particuliers en raison du non-respect et des injonctions. Les organes indépendants de résolution des litiges et les organismes d'autoréglementation du secteur privé doivent signaler aux pouvoirs publics compétents ou aux juridictions, selon le cas, et au ministère les organisations participant au CPD UE — États-Unis qui ne respectent pas leurs décisions.

f. Action de la FTC

i. La FTC s'est engagée à examiner en priorité les cas de non-conformité alléguée aux principes qui lui sont soumis par: i) les organismes d'autoréglementation en matière de protection de la vie privée et les autres organes indépendants de règlement des litiges; ii) les États membres de l'Union; et iii) le ministère, afin de déterminer s'il y a eu une violation de l'article 5 du FTC Act, qui interdit les actions ou pratiques déloyales ou frauduleuses dans le commerce. Si la FTC conclut qu'il y a lieu de croire que la section 5 a été violée, elle peut résoudre l'affaire en demandant une injonction administrative de cessation interdisant les pratiques contestées ou en déposant une plainte auprès d'une cour de district fédérale qui, si la plainte aboutit, peut rendre un arrêt dans le même sens. Les infractions concernées incluent les déclarations mensongères d'adhésion aux principes ou de participation au CPD UE — États-Unis par des organisations qui ont été supprimées de la liste du cadre de protection des données ou qui n'ont jamais autocertifié leur adhésion auprès du ministère. La FTC peut requérir des sanctions civiles en cas de violation d'une injonction administrative de cessation et poursuivre le contrevenant pour outrage au tribunal de nature civile ou pénale s'il viole l'arrêt d'une cour fédérale. La FTC informe le ministère de toute action de ce type qu'elle entreprend. Le ministère encourage les autres organismes publics à lui communiquer l'issue de toutes les affaires analogues ou d'autres décisions concernant l'adhésion aux principes.

g. Non-respect persistant

i. Si une organisation ne respecte pas les principes de manière persistante, elle n'est plus en droit de bénéficier des avantages du CPD UE — États-Unis. Les organisations qui ne respectent pas les principes de manière persistante seront supprimées de la liste du cadre de protection des données par le ministère, et elles devront restituer ou supprimer les informations à caractère personnel qu'elles ont reçues alors qu'elles participaient au CPD UE — États-Unis.

ii. Il y a non-respect persistant lorsqu'une organisation qui a autocertifié son adhésion auprès du ministère refuse de se conformer à une décision définitive prise par un organisme d'autoréglementation du respect de la vie privée, un organisme indépendant de règlement des litiges ou un organisme public, ou lorsqu'un tel organisme, notamment le ministère, constate qu'elle viole fréquemment les principes, au point que sa déclaration d'adhésion n'est plus crédible. Dans les cas où une telle décision est prise par un organisme autre que le ministère, l'organisation doit alors en informer sans retard le ministère. Dans le cas contraire, elle est passible de sanctions en vertu de la loi sur les fausses déclarations (False Statements Act, 18 U.S.C., § 1001). Une organisation qui se retire d'un programme d'autoréglementation sur la protection de la vie privée géré par le secteur privé ou d'un mécanisme indépendant de résolution des litiges n'est pas exonérée de son obligation de respecter les principes. Une telle organisation se rendrait de ce fait coupable de non-respect persistant.

iii. Le ministère supprimera une organisation de la liste du cadre de protection des données en cas de non-respect persistant, notamment en réaction à toute notification qu'il recevrait d'un tel cas de non-respect de l'organisation elle-même, d'un organisme d'autoréglementation du respect de la vie privée, d'un autre organe indépendant de règlement des litiges ou d'un organisme public, mais seulement après avoir accordé à l'organisation concernée un préavis de 30 jours et la possibilité de répondre ([17]). La liste du cadre de protection des données tenue par le ministère précisera donc quelles organisations bénéficient des avantages du CPD UE — États-Unis et quelles organisations n'en bénéficient plus.

iv. Toute organisation demandant à être soumise à l'autorité d'un organisme d'autoréglementation afin de pouvoir bénéficier à nouveau des avantages du CPD UE — États-Unis devra fournir à cet organisme des informations exhaustives sur sa participation antérieure au CPD UE — États-Unis.

([16]) Les circonstances dans lesquelles ces sanctions doivent être appliquées sont laissées à l'appréciation des organes indépendants de règlement des litiges. Lorsque l'on décide s'il convient d'exiger l'effacement des données, il faut notamment prendre en compte le caractère sensible des informations concernées et déterminer si elles ont été collectées, employées ou dévoilées en violation manifeste des principes.

([17]) Le ministère indiquera dans la notification le délai, qui sera nécessairement inférieur à 30 jours, dont dispose l'organisation pour répondre à la notification.

12. **Choix – Moment de l'exercice du droit de refus (ou d'acceptation)**

a. D'une manière générale, le principe «Choix» a pour but de s'assurer que les informations à caractère personnel sont utilisées et communiquées conformément aux attentes et aux choix de la personne concernée. Par conséquent, lorsque des informations à caractère personnel sont utilisées dans le cadre d'une action de marketing direct, toute personne concernée devrait pouvoir exercer son droit de refus (ou d'acceptation) à tout moment, dans certaines limites définies par l'organisation (par exemple, délai pour permettre à l'organisation d'appliquer le refus). L'organisation peut également requérir un certain nombre d'informations pour confirmer l'identité de la personne qui fait part de son opposition. Aux États-Unis, ce droit peut être exercé dans le cadre d'un programme central de refus. En tout état de cause, le recours à cette option doit être facile et peu coûteux.

b. De même, une organisation peut utiliser des informations à certaines fins de marketing direct lorsque les conditions ne permettent pas de laisser le choix avant l'utilisation des données, à condition qu'elle donne ensuite rapidement (et à tout moment sur demande) aux personnes concernées la possibilité de refuser, sans aucuns frais, toute autre communication de marketing direct et qu'elle se conforme aux souhaits de ces dernières.

13. **Informations sur les voyages**

a. Dans différentes circonstances, il est permis de communiquer à des organisations situées en dehors de l'Union les informations concernant les passagers des transports aériens (fournies notamment lors des réservations), telles que celles concernant les clients réguliers ou les réservations d'hôtel ainsi que les demandes spéciales – par exemple la composition des repas conformément à certains principes religieux ou une assistance physique. En vertu du RGPD, en l'absence d'une décision d'adéquation, les données à caractère personnel peuvent être transférées vers un pays tiers si des garanties appropriées en matière de protection des données sont fournies conformément à l'article 46 du RGPD ou, dans certaines situations, si l'une des conditions de l'article 49 du RGPD est remplie (par exemple, lorsque la personne concernée a donné son consentement explicite au transfert). Les organisations américaines participant au CPD UE — États-Unis assurent une protection adéquate des données à caractère personnel et peuvent donc recevoir des transferts de données de l'Union sur la base de l'article 45 du RGPD, sans avoir à mettre en place un instrument de transfert conformément à l'article 46 du RGPD ou à remplir les conditions de l'article 49 du RGPD. Étant donné que le CPD UE — États-Unis comporte des règles spécifiques concernant les informations sensibles, ce type d'information (pouvant concerner, par exemple, la nécessité, pour un client, de bénéficier d'une assistance physique) peut figurer parmi les données transférées aux organisations participant au CPD UE — États-Unis. L'organisation transférant l'information doit cependant appliquer dans chaque cas la législation nationale de l'État membre de l'Union où elle opère, laquelle législation peut entre autres imposer des conditions spéciales au traitement des données sensibles.

14. **Produits pharmaceutiques et médicaux**

a. Application de la législation des États membres de l'Union ou des principes

i. La législation des États membres de l'Union s'applique à la collecte des données à caractère personnel et à tout traitement intervenant avant le transfert aux États-Unis. Les principes s'appliquent aux données une fois qu'elles ont été transférées aux États-Unis. Les données utilisées pour la recherche pharmaceutique et à d'autres fins devraient être rendues anonymes le cas échéant.

b. Recherche scientifique future

i. Les données à caractère personnel élaborées dans le cadre d'études médicales ou pharmaceutiques jouent souvent un rôle précieux dans la recherche scientifique. Lorsque les données à caractère personnel collectées pour une étude sont transférées à une organisation des États-Unis en vertu du CPD UE — États-Unis, cette organisation peut utiliser les données pour une nouvelle activité de recherche scientifique s'il a été prévu au départ une notification et un choix approprié. Cette notification doit fournir des informations sur toute utilisation spécifique future des données, telles que le suivi périodique, les études associées ou la commercialisation.

ii. Toutes les utilisations futures des données ne peuvent être spécifiées, puisqu'un nouvel examen des données originales, des découvertes et progrès médicaux nouveaux et des évolutions en matière de santé publique et de réglementation peuvent engendrer de nouvelles utilisations de la recherche. La notification devrait donc inclure, le cas échéant, une indication que les données personnelles peuvent être utilisées pour des activités de recherche médicale et pharmaceutique futures non planifiées à l'avance. Si cette utilisation n'est pas cohérente avec les objectifs de recherche généraux pour lesquels les données à caractère personnel ont été originalement collectées ou auxquels la personne concernée a consenti par la suite, il convient d'obtenir un nouveau consentement.

c. Retrait d'un essai clinique

i. Les participants peuvent à tout moment décider de se retirer d'un essai clinique ou être priés de le faire. Toutes les données à caractère personnel collectées avant le retrait peuvent encore être traitées avec les autres données collectées dans le cadre de l'essai clinique, à condition que cela ait été précisé au participant dans la notification au moment où il a donné son accord.

d. Transferts à des fins de réglementation et de contrôle

i. Les sociétés d'appareils pharmaceutiques et médicaux ont le droit de fournir des données à caractère personnel extraites des essais cliniques réalisés dans l'Union européenne aux autorités des États-Unis à des fins de réglementation et de contrôle. Ce type de transfert vers des parties autres que les autorités de réglementation, telles que des sites de sociétés et d'autres chercheurs, est autorisé en conformité avec les principes «Notification» et «Choix».

e. Études «masquées»

i. Pour garantir l'objectivité de nombreux essais cliniques, l'accès aux informations relatives au traitement reçu par les participants est interdit à ceux-ci et, fréquemment, aussi aux chercheurs. Cela risquerait de compromettre la validité de l'étude et des résultats de la recherche. Un participant à ces essais cliniques (qualifiés d'études «masquées») ne doit pas nécessairement avoir accès aux données relatives à son traitement pendant l'essai si cette restriction lui a été expliquée lorsqu'il a commencé l'essai et si la révélation de cette information était susceptible de nuire à l'intégrité de l'effort de recherche.

ii. L'accord à la participation à l'essai dans ces conditions implique de renoncer au droit d'accès. Après l'achèvement de l'essai et l'analyse des résultats, les participants devraient avoir accès à leurs données s'ils le demandent. Ils devraient le demander, en premier lieu, au médecin ou autre prestataire de soins de santé qui les a traités pendant l'essai clinique ou, en second lieu, auprès de l'organisation commanditaire.

f. Contrôle de la sécurité et de l'efficacité du produit

i. Les sociétés d'appareils pharmaceutiques ou médicaux ne doivent pas appliquer les principes «Notification», «Choix», «Responsabilité en cas de transfert ultérieur» et «Accès» à leurs activités de contrôle de la sécurité et de l'efficacité du produit, y compris le compte rendu d'incidents et le suivi des malades ou sujets recourant à certains médicaments ou dispositifs médicaux, dans la mesure où le respect de ces principes entre en conflit avec les exigences réglementaires. Cela est vrai pour ce qui concerne, par exemple, les rapports effectués tant par les prestataires de soins de santé aux sociétés d'appareils pharmaceutiques et médicaux que par les sociétés d'appareils pharmaceutiques et médicaux à des agences gouvernementales telles que la Food and Drug Administration (organisme de surveillance des aliments et des médicaments).

g. Données codées

i. Les données de la recherche sont toujours codées de manière unique à leur source par le chercheur principal, pour ne pas révéler l'identité des personnes concernées. Les sociétés pharmaceutiques qui commanditent ce type de recherche ne reçoivent pas la clé de ce code. Le code de la clé unique est détenu par le seul chercheur, pour qu'il puisse identifier la personne concernée dans des circonstances spéciales (par exemple, si un suivi médical est requis). Le transfert de l'Union européenne aux États-Unis de données ainsi codées qui constituent des données à caractère personnel en vertu du droit de l'Union serait couvert par les principes.

15. **Informations des registres publics et informations accessibles au public**

a. Une organisation doit appliquer les principes «Sécurité» et «Intégrité des données et limitation des finalités», ainsi que le principe «Voies de recours, application et responsabilité» aux données à caractère personnel obtenues auprès de sources accessibles au public. Ces principes s'appliquent également aux données à caractère personnel collectées auprès de registres publics (c'est-à-dire des registres conservés par les services des autorités gouvernementales ou d'autres administrations publiques à quelque niveau que ce soit qui peuvent être consultés par tous).

b. Les principes «Notification», «Choix» ou «Responsabilité en cas de transfert ultérieur» ne doivent pas être appliqués aux informations des registres publics si ces dernières ne sont pas combinées à des informations non publiques et si les conditions de consultation établies par la juridiction compétente sont respectées. Les informations accessibles au public ne requièrent pas davantage l'application des principes «Notification», «Choix» ou «Responsabilité en cas de transfert ultérieur», à moins que l'auteur européen du transfert ne précise qu'elles font l'objet de restrictions qui exigent l'application de ces principes lors de leur utilisation par l'organisation. L'organisation ne sera pas tenue responsable de l'utilisation faite de ces informations par ceux qui les tirent de publications.

c. S'il s'avère qu'une organisation a volontairement publié des données à caractère personnel en violation des principes de manière qu'elle-même ou des tiers puissent bénéficier de ces exceptions, elle sera exclue du CPD UE — États-Unis.

d. Le principe «Accès» ne doit pas être appliqué aux informations issues de registres publics tant que ces informations ne sont pas associées à d'autres informations à caractère personnel (à l'exception des quelques informations utilisées pour indexer ou organiser les informations des registres publics). Il convient cependant de respecter les éventuelles conditions de consultation fixées par la juridiction concernée. En revanche, lorsque des informations tirées de registres publics sont associées à d'autres données non publiques (exception faite du cas précisé ci-dessus), l'organisation est tenue d'en permettre l'accès, pour autant que ces informations ne fassent pas l'objet d'autres dérogations.

e. Tout comme dans le cas des informations tirées des registres publics, il n'est pas nécessaire d'accorder l'accès aux informations qui sont déjà à la disposition du public, pour autant que ces informations ne soient pas associées à d'autres données non publiques. Les organisations spécialisées dans la vente d'informations accessibles au public peuvent répondre à des demandes d'accès contre le paiement d'une participation correspondant au montant habituellement demandé par l'organisation. Chacun peut, par ailleurs, obtenir les informations qui le concernent en s'adressant directement à l'organisation qui a compilé les données à l'origine.

16. **Demandes d'accès par les autorités publiques**

a. Afin d'assurer la transparence à l'égard des demandes licites d'accès à des informations à caractère personnel émanant d'autorités publiques, les organisations participant au CPD UE — États-Unis peuvent, sur une base volontaire, publier périodiquement des rapports de transparence indiquant le nombre de demandes d'informations à caractère personnel reçues de la part d'autorités publiques à des fins de mise en application des lois ou pour des raisons de sécurité nationale, dans la mesure où ces divulgations sont autorisées par la législation en vigueur.

b. Les informations fournies dans ces rapports par les organisations participant au CPD UE — États-Unis, associées aux informations publiées par la communauté du renseignement et d'autres informations, peuvent être utilisées pour éclairer l'examen conjoint périodique du fonctionnement du CPD UE — États-Unis conformément aux principes.

c. L'absence de notification en conformité avec le point a) xii) du principe «Notification» n'entrave pas la capacité d'une organisation à répondre à toute demande licite.

ANNEXE I: MODÈLE ARBITRAL

La présente annexe définit les conditions selon lesquelles les organisations participant au CPD UE — États-Unis sont tenues d'assurer l'arbitrage des plaintes, au titre du principe «Voies de recours, application et responsabilité». L'option d'arbitrage contraignant décrite ci-dessous s'applique à certaines plaintes «résiduelles» concernant des données couvertes par le CPD UE — États-Unis. Elle vise à proposer, au choix des personnes concernées, un mécanisme rapide, indépendant et équitable permettant de résoudre toute violation alléguée des principes qui n'aurait pas été résolue par les autres mécanismes mis en place au titre du CPD UE — États-Unis.

A. **Portée**

Une personne peut opter pour cette solution d'arbitrage en vue de déterminer, pour une plainte résiduelle, si une organisation participant au CPD UE — États-Unis n'a pas satisfait à ses obligations au titre des principes envers cette personne et si cette infraction reste entièrement ou partiellement sans réparation. Cette possibilité est offerte uniquement à ces fins. Elle n'est pas disponible, par exemple, en ce qui concerne les exceptions aux principes ([1]) ou en ce qui concerne une allégation relative à l'adéquation du CPD UE — États-Unis.

B. **Mesures de réparation possibles**

Dans le cadre de cette option d'arbitrage, le «panel du cadre de protection des données UE — États-Unis (le panel d'arbitrage composé d'un ou de trois arbitres, suivant ce dont les parties ont convenu) est habilité à imposer une mesure de réparation équitable non pécuniaire propre à la personne concernée (par ex. l'accès, la correction, la suppression ou la restitution des données concernées de cette personne), nécessaire pour remédier à la violation des principes uniquement en ce qui concerne cette personne. Il s'agit des seuls pouvoirs du panel du cadre de protection des données UE — États-Unis en matière de mesures de réparation. Dans son examen des recours, le panel du cadre de protection des données UE — États-Unis est tenu de prendre en considération les mesures de réparation déjà imposées par d'autres instances dans le cadre du CPD UE — États-Unis. Les dommages-intérêts, portant sur des honoraires, frais ou dépens, ou autres mesures de réparation ne sont pas possibles. Chaque partie supporte ses propres frais d'avocat.

C. **Exigences préalables à l'arbitrage**

Une personne qui décide de se prévaloir de cette option d'arbitrage doit accomplir les démarches suivantes avant de lancer une demande d'arbitrage: 1) faire part de la violation alléguée directement à l'organisation et donner à celle-ci la possibilité de régler le problème dans le délai fixé à la section d) i) du principe complémentaire «Résolution des litiges et application des décisions»; 2) faire appel au mécanisme de recours indépendant prévu par les principes, gratuit pour les personnes; et 3) faire part du problème au ministère par l'intermédiaire de son APD et laisser au ministère la possibilité de faire tout ce qui est en son pouvoir pour résoudre le problème dans les délais fixés dans la lettre de l'International Trade Administration (direction du commerce international) du ministère, sans frais pour la personne concernée.

Cette option d'arbitrage ne peut pas être invoquée si la violation des principes avancée par la personne concernée 1) a fait précédemment l'objet d'un arbitrage contraignant; 2) a fait l'objet d'une décision de justice définitive dans le cadre d'une procédure à laquelle la personne était partie; ou 3) a été réglée précédemment par les parties. Cette option ne peut pas non plus être invoquée si une APD 1) est compétente au titre des principes complémentaires «Rôle des autorités chargées de la protection des données» ou «Données relatives aux ressources humaines»; ou 2) est compétente pour résoudre la violation alléguée directement avec l'organisation. La compétence d'une APD pour statuer sur la même violation alléguée à l'encontre d'un responsable du traitement dans l'Union n'empêche pas à elle seule de recourir à cette option d'arbitrage à l'encontre d'une autre entité juridique qui n'est pas soumise à la compétence de cette APD.

D. **Caractère contraignant des décisions**

La décision d'une personne de recourir à cette option d'arbitrage contraignant est entièrement volontaire. Les décisions arbitrales engageront toutes les parties à l'arbitrage. Une fois l'option d'arbitrage invoquée, la personne concernée renonce à toute possibilité de recours contre la même violation alléguée devant une autre instance, sous réserve du fait que, si la mesure de réparation équitable non pécuniaire ne permet pas de remédier totalement à la violation alléguée, l'invocation par cette personne de l'option d'arbitrage n'exclut pas une action en dommages-intérêts devant les instances judiciaires.

([1]) Les principes, Vue d'ensemble, point 5.

E. **Contrôle et application**

Les personnes et les organisations participant au CPD UE — États-Unis pourront demander le contrôle juridictionnel et l'application des décisions arbitrales conformément à la législation américaine au titre du Federal Arbitration Act ([2]). Toute affaire de ce type doit être portée devant le tribunal fédéral de première instance compétent pour le lieu principal d'activité de l'organisation participant au CPD UE — États-Unis.

Cette option d'arbitrage vise à résoudre des litiges individuels. De plus, les décisions arbitrales n'ont pas pour vocation d'établir une jurisprudence contraignante ou dont il convient de tenir compte dans des dossiers impliquant d'autres parties, y compris dans des procédures d'arbitrage futures devant les tribunaux de l'Union ou des États-Unis ou dans le cadre de procédures lancées par la FTC.

F. **Le panel d'arbitrage**

Les parties sélectionneront les arbitres du panel du cadre de protection des données UE — États-Unis dans la liste d'arbitres décrite ci-dessous.

Conformément au droit applicable, le ministère et la Commission dresseront une liste d'au moins dix arbitres, sélectionnés sur la base de leur indépendance, de leur intégrité et de leur expertise. Pour ce faire, les principes suivants s'appliqueront:

Les arbitres:

1) resteront sur la liste pendant une période de trois ans, sauf circonstances exceptionnelles ou motif valable, cette période étant renouvelable une fois par le ministère, avec notification préalable à la Commission;

2) ne recevront aucune consigne ni des parties, ni d'une organisation participant au CPD UE — États-Unis, ni des États-Unis, de l'Union européenne ou d'un État membre de l'Union, ni de tout autre organe étatique, autorité publique ou autorité répressive; ils ne seront pas davantage affiliés à ces parties, organisations, États, organes ou autorités; et

3) doivent être habilités à pratiquer le droit aux États-Unis, être experts en droit américain de la vie privée et posséder une expertise en droit de l'Union en matière de protection des données.

([2]) Le chapitre 2 du Federal Arbitration Act (ci-après la «FAA») dispose qu'«[u]n accord arbitral ou une sentence arbitrale découlant d'une relation juridique, contractuelle ou non, et considérée comme étant de nature commerciale, notamment une transaction, un contrat ou une convention au sens de [la section 2 de la FAA] relève du champ d'application de la convention [du 10 juin 1958 sur la reconnaissance et l'exécution des sentences arbitrales prononcées à l'étranger, 21 U.S.T. 2519, TIAS n° 6997 (la «convention de New York»)]». 9 U.S.C. § 202. La FAA dispose également qu'«une convention ou sentence découlant d'une relation de ce type et concernant exclusivement des citoyens des États-Unis sera réputée ne pas relever du champ d'application de la convention [de New York] sauf si cette relation implique des biens situés à l'étranger, envisage une exécution ou une application à l'étranger ou présente tout autre lien raisonnable avec un ou plusieurs États étrangers». Ibidem au chapitre 2, «toute partie à l'arbitrage peut s'adresser à toute instance judiciaire compétente au titre du présent chapitre pour obtenir une ordonnance confirmant la sentence à l'encontre de toute autre partie à l'arbitrage. Le tribunal confirmera la sentence sauf s'il constate l'existence de l'un des motifs de refus ou de report de reconnaissance ou d'application de la sentence définis dans ladite convention [de New York]». Ibidem § 207. Le chapitre 2 dispose que «les tribunaux de première instance des États-Unis […] exercent la compétence originale sur […] les actions ou procédures [au titre de la convention de New York], quel que soit le montant du litige». Ibidem § 203.
Le chapitre 2 dispose également que «le chapitre 1 s'applique aux actions et procédures intentées au titre du présent chapitre dans la mesure où ce chapitre n'est pas contraire au présent chapitre ni à la convention [de New York] ratifiée par les États-Unis». Ibidem § 208. Le chapitre 1, quant à lui, dispose qu'«une disposition d'un […] contrat démontrant une transaction dans le domaine du commerce en vue de régler par voie d'arbitrage une controverse découlant de ce contrat ou de cette transaction, ou du refus d'exécuter tout ou partie de ce contrat ou de cette transaction, ou une convention écrite engageant les parties à soumettre à l'arbitrage une controverse existante découlant d'un contrat, d'une transaction ou d'un refus de ce type est valide, irrévocable et exécutoire, sous réserve des motifs prévus par la loi ou par le principe d'équité pour la révocation de tout contrat». Ibidem § 2. Le chapitre 1 dispose également que «toute partie à l'arbitrage peut s'adresser au tribunal ainsi défini en vue d'obtenir une ordonnance confirmant la sentence. Le tribunal est tenu de rendre cette ordonnance sauf dans les cas où la sentence est annulée, modifiée ou corrigée conformément aux dispositions des sections 10 et 11 de la [FAA]». Ibidem § 9.

G. **Procédures d'arbitrage**

Le ministère et la Commission sont convenus, dans le respect du droit en vigueur, d'adopter des règles d'arbitrage pour régir les procédures devant le panel du cadre de protection des données UE — États-Unis ([3]). Si les règles régissant les procédures doivent être modifiées, le ministère et la Commission conviendront de modifier ces règles ou d'adopter un autre ensemble de procédures arbitrales américaines existantes et bien établies, selon le cas, sous réserve de chacune des considérations suivantes:

1. Une personne peut lancer une procédure d'arbitrage contraignant moyennant le respect des conditions préalables à l'arbitrage exposées ci-dessus, en remettant une «notification» à l'organisation. Cette notification doit contenir un résumé des démarches accomplies au titre du paragraphe C pour résoudre la plainte, une description de la violation alléguée et, à sa discrétion, toutes pièces justificatives et/ou une analyse de la législation applicable à la plainte alléguée.

2. Des procédures seront mises en place afin qu'une même violation invoquée par une personne ne fasse pas l'objet de plusieurs recours ou procédures.

3. Une action auprès de la FTC peut être menée parallèlement à l'arbitrage.

4. Aucun représentant des États-Unis, de l'Union ou d'un État membre de l'Union ou de tout autre organe étatique, autorité publique ou autorité répressive ne peut participer à ces arbitrages, étant entendu qu'à la demande d'une personne de l'Union, les APD peuvent apporter une assistance dans la préparation de la notification uniquement. Les APD ne peuvent en revanche pas avoir accès aux communications des pièces du dossier avant l'audience ni à aucun autre document relatif à ces arbitrages.

5. L'arbitrage sera organisé aux États-Unis. La personne concernée peut décider d'y participer par une vidéoconférence ou une téléconférence, mise en place gratuitement. La participation en personne ne sera pas imposée.

6. Sauf accord contraire des parties, l'arbitrage se fera en anglais. Sur demande motivée, et en tenant compte de la représentation ou non de la personne par un avocat, l'interprétation lors des auditions d'arbitrage ainsi que la traduction des documents d'arbitrage seront assurées gratuitement pour la personne concernée, sauf si le panel du cadre de protection des données UE — États-Unis estime que, dans les circonstances particulières du dossier d'arbitrage concerné, ce service engendrerait des coûts injustifiés ou disproportionnés.

7. Les documents soumis aux arbitres seront traités de manière confidentielle et seront utilisés uniquement dans le cadre de l'arbitrage.

8. Des mesures de communication des pièces avant audience propres à la personne concernée peuvent être autorisées si nécessaire et ces pièces seront traitées de manière confidentielle par les parties et seront utilisées uniquement dans le cadre de l'arbitrage.

9. Sauf accord contraire des parties, les procédures d'arbitrage devraient être achevées dans un délai de 90 jours à compter de la remise de la notification à l'organisation concernée.

([3]) L'International Centre for Dispute Resolution (ci-après l'«ICDR»), la division internationale de l'American Arbitration Association (ci-après l'«AAA») (collectivement l'«ICDR-AAA»), a été choisi par le ministère pour gérer les arbitrages conformément à l'annexe I des principes et pour gérer le fonds d'arbitrage décrit dans ladite annexe. Le 15 septembre 2017, le ministère et la Commission sont convenus d'adopter un ensemble de règles d'arbitrage pour régir les procédures arbitrales contraignantes décrites à l'annexe I des principes, ainsi qu'un code de conduite pour les arbitres qui est conforme aux normes éthiques généralement acceptées pour les arbitres commerciaux et à l'annexe I des principes. Le ministère et la Commission sont convenus d'adapter les règles d'arbitrage et le code de conduite pour tenir compte des mises à jour en vertu du CPD UE — États-Unis et le ministère coopérera avec l'ICDR-AAA pour effectuer ces mises à jour.

H. **Coûts**

Les arbitres doivent prendre des mesures raisonnables pour limiter le plus possible les coûts et frais liés à l'arbitrage.

Dans le respect du droit en vigueur, le ministère facilitera la création d'un fonds auquel les organisations participant au CPD UE — États-Unis seront tenues d'apporter une contribution, fondée en partie sur leur taille, qui couvrira les coûts d'arbitrage, y compris les honoraires des arbitres, jusqu'à des montants plafonnés. Le fonds sera géré par un tiers qui rendra compte régulièrement au ministère de son fonctionnement. Le ministère coopérera avec ce tiers pour examiner régulièrement le fonctionnement du fonds, notamment la nécessité d'ajuster le montant des contributions ou des plafonds en fonction des coûts d'arbitrage, et prendra en considération, entre autres, le nombre d'arbitrages et les coûts et durées des arbitrages, étant bien entendu qu'aucune charge financière excessive ne sera imposée aux organisations participant au CPD UE — États-Unis. Le ministère informera la Commission du résultat de ces examens avec le tiers et notifiera au préalable à la Commission tout ajustement du montant des contributions. Les honoraires d'avocats ne sont pas couverts par la présente disposition ni par aucun fonds relevant de la présente disposition.

ANNEXE II

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

6 juillet 2023

Monsieur Didier Reynders
Commissaire à la justice
Commission européenne
Rue de la Loi 200
1049 Bruxelles
Belgique

Monsieur le Commissaire,

Au nom des États-Unis, j'ai le plaisir de vous transmettre, par la présente, un ensemble de textes relevant du cadre de protection des données UE — États-Unis qui, associé au décret présidentiel 14086, intitulé «Enhancing Safeguards for United States Signals Intelligence Activities» et au titre 28 du CFR, partie 201, modifiant les règlements du ministère de la justice pour établir la Cour chargée du contrôle de la protection des données, tient compte des négociations importantes et détaillées visant à renforcer les protections de la vie privée et des libertés civiles. Ces négociations ont abouti à de nouveaux garde-fous visant à garantir que les activités de renseignement d'origine électromagnétique menées par les États-Unis sont nécessaires et proportionnées à la poursuite d'objectifs de sécurité nationale définis et à un nouveau mécanisme permettant aux citoyens de l'Union européenne (l'«UE») de demander réparation s'ils estiment être illégalement ciblés par des activités de renseignement d'origine électromagnétique, éléments qui, ensemble, garantiront la confidentialité des données à caractère personnel de l'Union. Le cadre de protection des données UE — États-Unis sera le fondement d'une économie numérique inclusive et compétitive. Nous pouvons être fiers, les uns comme les autres, des améliorations découlant de ce cadre, qui renforceront la protection de la vie privée dans le monde entier. Cet ensemble de textes, auquel il convient d'ajouter le décret présidentiel, des règlements et d'autres documents accessibles auprès de sources publiques, constitue une base très solide pour une nouvelle décision d'adéquation de la Commission européenne [1].

Les documents suivants sont joints:

— les principes du cadre de protection des données UE — États-Unis, y compris les principes complémentaires (collectivement dénommés «les principes») et l'annexe I des principes (c'est-à-dire une annexe précisant les conditions dans lesquelles les organisations participant au cadre de protection des données sont tenues d'arbitrer certaines plaintes résiduelles concernant des données à caractère personnel couvertes par les principes);

— une lettre de la direction du commerce international du ministère, qui gère le programme du cadre de protection des données, décrivant les engagements pris par notre ministère pour garantir le bon fonctionnement du cadre de protection des données UE — États-Unis;

— une lettre de la Federal Trade Commission décrivant son contrôle de l'application des principes;

— une lettre du ministère des transports des États-Unis décrivant son contrôle de l'application des principes;

— une lettre du bureau du directeur du renseignement national (Office of the Director of National Intelligence) concernant les garanties et les restrictions applicables aux autorités de la sécurité nationale des États-Unis; et

— une lettre du ministère de la justice concernant les garanties et les limites relatives à l'accès du gouvernement américain à des fins répressives ou d'intérêt public.

[1] Pour autant que la décision de la Commission relative à l'adéquation de la protection assurée par le cadre de protection des données UE — États-Unis s'applique à l'Islande, au Liechtenstein et à la Norvège, l'ensemble de textes relevant du CPD UE — États-Unis couvrira non seulement l'Union, mais également ces trois pays.

L'intégralité des textes relevant du cadre de protection des données UE — États-Unis sera publiée sur le site web du cadre de protection des données du ministère et les principes et l'annexe I des principes seront effectifs à compter de la date d'entrée en vigueur de la décision d'adéquation de la Commission européenne.

Soyez assuré que les États-Unis prennent ces engagements au sérieux. Nous nous réjouissons à la perspective de coopérer avec vous dans la mise en œuvre du cadre de protection des données UE — États-Unis et dans la phase suivante de ce processus que nous entamons conjointement.

Je vous prie, Monsieur le Commissaire, d'agréer
l'expression de ma haute considération.

Gina M. Raimondo

ANNEXE III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 décembre 2022

Monsieur Didier Reynders
Commissaire à la justice
Commission européenne
Rue de la Loi 200
1049 Bruxelles
Belgique

Monsieur le Commissaire,

Au nom de la direction du commerce international, j'ai le plaisir de décrire ci-après les engagements pris par le ministère américain du commerce (ci-après le «ministère») pour garantir la protection des données à caractère personnel par sa gestion et sa supervision du programme du cadre de protection des données. La finalisation du cadre de protection des données UE — États-Unis (ci-après le «CPD UE — États-Unis») représente une avancée majeure pour la protection de la vie privée et pour les entreprises des deux côtés de l'Atlantique. Ce cadre permettra aux citoyens de l'Union d'être confiants dans le fait que leurs données seront protégées et qu'ils disposeront de voies de recours pour remédier aux préoccupations liées à leurs données, et permettra à des milliers d'entreprises de continuer à investir et à exercer des activités commerciales de part et d'autre de l'Atlantique, dans l'intérêt de nos économies et de nos citoyens respectifs. Le CPD UE — États-Unis est le résultat de plusieurs années de travail acharné et de collaboration avec vous et vos collègues de la Commission européenne (ci-après la «Commission»). Nous espérons poursuivre notre travail avec la Commission pour faire en sorte que cette collaboration fonctionne de manière efficace.

Le CPD UE — États-Unis procurera des avantages majeurs aux personnes comme aux entreprises. Tout d'abord, il constitue un ensemble important de mesures de protection de la vie privée pour les données des citoyens de l'Union transférées vers les États-Unis. Il exige des organisations américaines participantes qu'elles élaborent une politique conforme en matière de protection de la vie privée, qu'elles s'engagent publiquement à respecter les «principes du cadre de protection des données UE — États-Unis», y compris les principes complémentaires (ci-après collectivement dénommés les «principes») et l'annexe I des principes (précisant les conditions dans lesquelles les organisations participant au CPD UE — États-Unis sont tenues d'arbitrer certaines plaintes résiduelles concernant des données à caractère personnel couvertes par les principes), de sorte que cet engagement devient contraignant en droit américain ([1]), qu'elles recertifient chaque année leur adhésion aux principes auprès du ministère, qu'elles mettent à disposition des citoyens de l'Union un mécanisme de règlement des litiges indépendant et gratuit, et qu'elles soient soumises aux pouvoirs d'enquête et aux pouvoirs répressifs d'un organisme officiel américain mentionné dans les principes [par exemple, la Federal Trade Commission (ci-après la «FTC») et le ministère des transports], ou d'un organisme officiel américain mentionné dans une future annexe aux principes. Si la décision d'une organisation d'autocertifier son adhésion aux principes est volontaire, dès lors qu'elle s'engage publiquement à participer au CPD UE — États-Unis, son engagement est contraignant en droit américain, sous le contrôle de la FTC, du ministère des

([1]) Les organisations qui ont autocertifié leur engagement à respecter les principes du cadre «bouclier de protection des données UE — États-Unis» et souhaitent bénéficier des avantages de la participation au CPD UE — États-Unis doivent respecter les «principes du cadre de protection des données UE — États-Unis». Cet engagement à respecter les «principes du cadre de protection des données UE — États-Unis» doit être reflété dans la politique en matière de protection de la vie privée de ces organisations dès que possible et, en tout état de cause, au plus tard trois mois après la date d'entrée en vigueur des «principes du cadre de protection des données UE — États-Unis» [*Voir* section e) du principe complémentaire sur l'autocertification].

transports ou d'un autre organisme officiel américain, en fonction de l'autorité qui a compétence pour l'organisation participant au CPD UE — États-Unis. En second lieu, le CPD UE — États-Unis permettra aux entreprises établies aux États-Unis, y compris les filiales d'entreprises européennes implantées aux États-Unis, de recevoir des données à caractère personnel de l'Union européenne afin de faciliter les flux de données qui soutiennent le commerce transatlantique. Les flux de données entre les États-Unis et l'Union européenne sont les plus importants au monde et sont le fondement des relations économiques entre les États-Unis et l'Union européenne, qui représentent 7,1 milliards d'USD et soutiennent des millions d'emplois de part et d'autre de l'Atlantique. Les entreprises qui s'appuient sur les flux de données transatlantiques sont issues de tous les secteurs d'activité et comptent de très grandes sociétés de la liste Fortune 500 ainsi que de nombreuses petites et moyennes entreprises. Les flux de données transatlantiques permettent aux organisations américaines de traiter les données nécessaires pour fournir des biens, des services et des possibilités d'emploi aux citoyens européens.

Le ministère s'est engagé à collaborer étroitement et de manière productive avec ses homologues de l'Union afin de gérer et de superviser efficacement le programme du cadre de protection des données. Cet engagement est illustré par le fait que le ministère développe et améliore en permanence une variété de ressources pour aider les organisations dans le processus d'autocertification, la création d'un site web afin de communiquer des informations ciblées aux parties intéressées, la collaboration avec la Commission et les autorités européennes de protection des données (ci-après les «APD») afin de définir des orientations qui clarifient les éléments importants du CPD UE — États-Unis, la sensibilisation pour contribuer à une meilleure connaissance des obligations des organisations en matière de protection des données, et la supervision et le contrôle du respect des exigences du programme par les organisations.

Notre coopération permanente avec nos précieux homologues de l'Union permettra au ministère de veiller à ce que le CPD UE — États-Unis fonctionne efficacement. Le gouvernement américain collabore depuis longtemps avec la Commission en vue de promouvoir des principes communs en matière de protection des données, en comblant les différences entre nos approches juridiques respectives tout en soutenant les échanges et la croissance économique dans l'Union européenne et aux États-Unis. Nous pensons que le CPD UE — États-Unis, qui est un exemple de cette collaboration, permettra à la Commission de prendre une nouvelle décision d'adéquation qui autorisera les organisations à utiliser le CPD UE — États-Unis afin de transférer des données à caractère personnel de l'Union européenne vers les États-Unis conformément au droit de l'Union.

Gestion et supervision du programme du cadre de protection des données par le ministère américain du commerce

Le ministère est fermement engagé à gérer et à superviser de manière efficace le programme du cadre de protection des données et il consacrera les efforts et les ressources nécessaires pour atteindre cet objectif. Le ministère tiendra et mettra à la disposition du public une liste officielle des organisations des États-Unis qui ont autocertifié leur adhésion auprès du ministère et qui ont déclaré leur engagement à respecter les principes (la «liste du cadre de protection des données»). Il mettra à jour cette liste sur la base des déclarations annuelles de recertification présentées par les organisations participantes et en supprimant de celle-ci les organisations qui se retirent volontairement, qui ne procèdent pas au renouvellement annuel de leur certification conformément aux procédures du ministère ou qui, de manière persistante, ne se conforment pas aux principes. Il tiendra et rendra public un registre officiel des organisations américaines qui ont été supprimées de la liste du cadre de protection des données et indiquera, dans chaque cas, la raison pour laquelle l'organisation a été radiée. La liste et le registre officiels susmentionnés resteront accessibles au public sur le site web du cadre de protection des données du ministère. Le site web du cadre de protection des données comprendra un texte explicatif, placé bien en évidence, précisant que toute organisation radiée de la liste du cadre de protection des données doit cesser d'affirmer qu'elle participe au CPD UE — États-Unis ou qu'elle respecte ses principes et qu'elle peut recevoir des informations à caractère personnel conformément au CPD UE — États-Unis. Cette organisation reste néanmoins tenue d'appliquer les principes aux informations à caractère personnel qu'elle a reçues alors qu'elle participait au CPD UE — États-Unis aussi longtemps qu'elle conserve ces informations. Le ministère, dans le cadre de son engagement global et permanent à gérer et à superviser de manière efficace le programme du cadre de protection des données, s'engage spécifiquement à:

Vérifier le respect des exigences liées à l'autocertification

— Le ministère, avant de finaliser l'autocertification initiale d'une organisation ou le renouvellement annuel de sa certification (collectivement appelés l'«autocertification») et d'inscrire ou de maintenir une organisation sur la liste du cadre de protection des données, vérifiera que l'organisation a, au minimum, satisfait aux exigences pertinentes énoncées dans le principe complémentaire sur l'autocertification concernant les informations qu'une organisation doit communiquer au ministère dans sa déclaration d'autocertification et a fourni en temps utile une politique en matière de protection de la vie privée pertinente qui informe les personnes des 13 éléments énumérés dans le principe «Notification». Le ministère vérifiera:

— que l'organisation a fourni l'identité de l'organisation qui présente sa déclaration d'autocertification, ainsi que de toutes les entités ou filiales américaines de l'organisation qui autocertifie son adhésion qui adhèrent également aux principes et que l'organisation souhaite voir couverts par son autocertification;

— qu'elle a fourni les coordonnées qui lui étaient demandées (par exemple, les coordonnées des personnes et/ou des bureaux spécifiques au sein de l'organisation qui autocertifie son adhésion, responsables du traitement des réclamations, des demandes d'accès et de toute autre question soulevée en vertu du CPD UE — États-Unis);

— qu'elle a décrit la ou les finalités pour lesquelles l'organisation collecterait et utiliserait les informations à caractère personnel reçues de l'Union européenne;

— qu'elle a indiqué quelles informations à caractère personnel seraient reçues de l'Union européenne sur la foi du CPD UE — États-Unis et seraient donc couvertes par son autocertification;

— si l'organisation possède un site web public, qu'elle a indiqué l'adresse web à laquelle la politique en matière de protection de la vie privée pertinente est accessible ou, si l'organisation ne possède pas de site web public, qu'elle a communiqué au ministère une copie de cette politique et qu'elle a indiqué le lieu où le texte de cette politique peut être consulté par les personnes concernées (c'est-à-dire par les membres du personnel concernés si les dispositions de protection de la vie privée sont dans le domaine des ressources humaines ou par le public si les dispositions de protection de la vie privée ne sont pas dans le domaine des ressources humaines);

— qu'elle a incorporé dans sa politique en matière de protection de la vie privée en temps utile (c'est-à-dire dans un premier temps, uniquement dans un projet de politique en matière de protection de la vie privée fourni avec le dossier si ce dossier est une autocertification initiale; ensuite, dans une version finale de cette politique de protection de la vie privée qui a été publiée, le cas échéant) une déclaration mentionnant qu'elle adhère aux principes et un hyperlien vers le site web du cadre de protection des données géré par le ministère ou son adresse web (par exemple, la page d'accueil ou la page web consacrée à la liste du cadre de protection des données);

— qu'elle a inséré dans sa politique en matière de protection de la vie privée en temps utile l'ensemble des 12 autres éléments énumérés dans le principe «Notification» (par exemple, la possibilité, sous certaines conditions, pour la personne concernée de l'Union d'invoquer un arbitrage contraignant; l'obligation de divulguer les informations à caractère personnel en réponse à des demandes légales formulées par les pouvoirs publics, notamment pour répondre à des besoins de sécurité nationale ou d'application des lois; et sa responsabilité en cas de transferts ultérieurs à des tiers);

— qu'elle a indiqué le nom de l'organisme officiel spécifique qui est chargé de statuer sur les plaintes déposées, le cas échéant, contre l'organisation pour pratiques déloyales ou frauduleuses et pour infraction aux lois ou aux réglementations régissant la protection de la vie privée (et qui est mentionné dans les principes ou dans une future annexe aux principes);

— qu'elle a indiqué l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation;

— qu'elle a indiqué si la méthode pertinente (c'est-à-dire les procédures de suivi qu'elle doit fournir) pour vérifier son respect des principes est l'«autoévaluation» (c'est-à-dire la vérification interne) ou le «contrôle extérieur de la conformité» (c'est-à-dire la vérification par un tiers) et, si elle a indiqué que la méthode pertinente était le contrôle extérieur de la conformité, qu'elle a également indiqué le tiers qui a effectué ce contrôle;

— qu'elle a indiqué le mécanisme de recours indépendant disponible pour instruire les réclamations introduites au titre des principes et de mettre gratuitement à la disposition des personnes des voies de recours appropriées.

— Si l'organisation a sélectionné un mécanisme de recours indépendant proposé par un organisme de règlement extrajudiciaire des litiges du secteur privé, elle a inséré dans sa politique en matière de protection de la vie privée, un hyperlien vers le site web ou son adresse web, ou le formulaire d'introduction d'une réclamation auprès du mécanisme mis à disposition pour l'instruction des réclamations en suspens introduites au titre des principes.

— Si l'organisation est tenue de coopérer avec les APD compétentes (en ce qui concerne les données relatives aux ressources humaines transférées depuis l'Union européenne dans le cadre de la relation de travail) ou si elle a choisi de coopérer avec ces autorités dans le cadre de l'instruction et de la résolution des réclamations introduites au titre des principes, elle a déclaré qu'elle s'engageait à coopérer avec les APD et à se conformer à leurs conseils de prendre des mesures spécifiques pour respecter les principes.

— Le ministère vérifiera également que l'autocertification de l'organisation est conforme à sa ou ses politiques en matière de protection de la vie privée. Lorsqu'une organisation qui autocertifie son adhésion souhaite couvrir l'une de ses entités ou filiales américaines qui ont des politiques en matière de protection de la vie privée distinctes et pertinentes, le ministère examinera également les politiques en matière de protection de la vie privée pertinentes de ces entités ou filiales couvertes afin de s'assurer qu'elles comprennent tous les éléments requis énoncés dans le principe «Notification».

— Le ministère collaborera avec des organismes officiels (par exemple, la FTC et le ministère des transports) pour vérifier que les organisations sont soumises à la compétence de l'organisme officiel compétent indiqué dans leurs dossiers d'autocertification, lorsque le ministère a des raisons de douter qu'elles sont soumises à cette compétence.

— Le ministère collaborera avec les organes de règlement extrajudiciaire des litiges du secteur privé pour vérifier que les organisations sont activement enregistrées pour le mécanisme de recours indépendant indiqué dans leurs déclarations d'autocertification; et collaborera avec ces organes pour vérifier que les organisations sont activement enregistrées pour le contrôle extérieur de conformité indiqué dans leurs déclarations d'autocertification, lorsque ces organes peuvent proposer les deux types de services.

— Le ministère s'appuiera sur le tiers qu'il aura choisi pour être le dépositaire des fonds collectés au moyen de la cotisation du panel d'APD (c'est-à-dire la cotisation annuelle servant à couvrir les frais de gestion du panel) pour vérifier que les organisations ont acquitté cette cotisation pour l'année concernée, lorsque celles-ci ont indiqué que les APD étaient le mécanisme de recours indépendant pertinent.

— Le ministère coopérera avec le tiers qu'il aura choisi pour gérer les arbitrages conformément à l'annexe I des principes et pour gérer le fonds d'arbitrage décrit dans ladite annexe, afin de vérifier que les organisations ont contribué audit fonds d'arbitrage.

— Lorsque le ministère constate des problèmes lors de son examen des déclarations d'autocertification des organisations, il informe ces dernières qu'elles doivent les résoudre dans le délai approprié fixé par le ministère ([2]). Le ministère les informera également que si elles ne répondent pas dans les délais fixés par le ministère ou si elles ne remplissent pas leur déclaration d'autocertification conformément aux procédures du ministère, ces déclarations seront considérées comme abandonnées, et que toute fausse déclaration d'une organisation concernant sa participation ou sa conformité au CPD UE — États-Unis est susceptible de faire l'objet de mesures répressives de la part de la FTC, du ministère des transports ou de toute autre instance administrative compétente. Le ministère informera les organisations par les moyens de contact que les organisations lui ont communiqués.

Faciliter la coopération avec les organismes de règlement extrajudiciaire des litiges qui fournissent des services liés aux principes

— Le ministère collaborera avec les organismes de règlement extrajudiciaire des litiges du secteur privé proposant des mécanismes de recours indépendants, qui peuvent instruire les réclamations en suspens introduites au titre des principes, afin de vérifier qu'ils satisfont, au minimum, aux exigences énoncées dans le principe complémentaire «Résolution des litiges et application des décisions». Le ministère vérifiera qu'ils:

  — communiquent sur leur site web public des informations relatives aux principes et aux services qu'ils fournissent en vertu du CPD UE — États-Unis, qui doivent comprendre: 1) des informations relatives aux exigences en matière de mécanismes de recours indépendants au titre des principes, ou un hyperlien vers ces exigences; 2) un hyperlien vers le site web «cadre de protection des données» du ministère; 3) l'indication que les services de règlement des litiges qu'ils proposent dans le cadre du CPD UE — États-Unis sont gratuits pour les personnes; 4) une description des modalités de dépôt d'une réclamation relative aux principes; 5) le délai de traitement des réclamations relatives aux principes; et 6) une description des mesures de réparation potentielles. Le ministère informera les organismes en temps utile des modifications importantes apportées à la supervision et à la gestion du programme du cadre de protection des données, lorsque ces modifications sont imminentes ou ont déjà été apportées et qu'elles sont pertinentes pour le rôle joué par les organismes en vertu du CPD UE — États-Unis;

([2]) Par exemple, en ce qui concerne la recertification, il est attendu des organisations qu'elles règlent tous les problèmes dans un délai de 45 jours; sous réserve de la désignation par le ministère d'un autre délai approprié.

— publiera un rapport annuel présentant des statistiques agrégées relatives à leurs services de règlement des litiges, qui doit indiquer: 1) le nombre total de réclamations relatives aux principes reçues au cours de l'année faisant l'objet du rapport; 2) les types de réclamations reçues; 3) des indicateurs de qualité du règlement des litiges, par exemple le délai de traitement des réclamations; et 4) les résultats du traitement des réclamations reçues, notamment le nombre et les types de recours et les sanctions infligées. Le ministère fournira aux organismes des orientations spécifiques et complémentaires sur les informations qu'ils doivent communiquer dans ces rapports annuels, en précisant ces exigences (par exemple, en énumérant les critères spécifiques qu'une réclamation doit remplir pour être considérée comme une réclamation relative aux principes aux fins du rapport annuel), ainsi qu'en indiquant les autres types d'informations qu'ils doivent communiquer (par exemple, si l'organisme propose également un service de vérification lié aux principes, une description de la manière dont l'organisme évite tout conflit d'intérêts potentiel ou réel dans les cas où il fournit à une organisation à la fois des services de vérification et des services de règlement des litiges). Les orientations supplémentaires données par le ministère préciseront également la date à laquelle les rapports annuels des organismes doivent être publiés pour la période de référence concernée.

Assurer le suivi des organisations qui souhaitent être radiées ou ont été radiées de la liste du cadre de protection des données

— Si une organisation souhaite se retirer du CPD UE — États-Unis, le ministère exigera que l'organisation supprime de toute politique en matière de protection de la vie privée pertinente toute référence au CPD UE — États-Unis donnant à penser qu'elle continue de participer au CPD UE — États-Unis et qu'elle peut recevoir des données à caractère personnel conformément au CPD UE — États-Unis (voir description de l'engagement du ministère à rechercher de fausses déclarations de participation). Le ministère exigera également que l'organisation remplisse et transmette au ministère un questionnaire approprié pour vérifier:

  — son souhait de se retirer;

  — ce qu'elle compte faire avec les données à caractère personnel qu'elle a reçues sur la foi du CPD UE — États-Unis pendant qu'elle participait au CPD UE — États-Unis, à savoir: a) conserver ces données, continuer à appliquer les principes à ces données et déclarer annuellement au ministère son engagement à appliquer les principes à ces données; b) conserver ces données et assurer une protection «adéquate» de ces données par un autre moyen autorisé; ou c) restituer ou supprimer toutes ces données à une date déterminée; et

  — qui, au sein de l'organisation, servira de point de contact permanent pour les questions liées aux principes.

— Si une organisation a choisi l'option a) décrite ci-dessus, le ministère exigera également qu'elle remplisse et transmette au ministère chaque année après son retrait (c'est-à-dire avant le premier anniversaire de son retrait, ainsi que pour chaque anniversaire suivant jusqu'à ce que l'organisation assure une protection «adéquate» de ces données par un autre moyen autorisé, ou restitue ou supprime toutes ces données et notifie cette action au ministère) un questionnaire approprié pour vérifier ce qu'elle a fait de ces données à caractère personnel, ce qu'elle compte faire de toutes les données à caractère personnel qu'elle continue à conserver, et qui, en son sein, servira de point de contact permanent pour les questions liées aux principes.

— Si une organisation a laissé son autocertification expirer (c'est-à-dire qu'elle n'a pas procédé à la recertification annuelle de son adhésion aux principes ou qu'elle a été radiée de la liste du cadre de protection des données pour une autre raison, telle que le retrait), le ministère lui demandera de remplir et de lui transmettre un questionnaire approprié afin de vérifier si elle souhaite se retirer ou renouveler sa certification:

  — et si elle souhaite se retirer, vérifier également ce qu'elle compte faire avec les données à caractère personnel qu'elle a reçues sur la foi du CPD UE — États-Unis pendant qu'elle participait au CPD UE — États-Unis (voir description précédente de ce qu'une organisation doit vérifier si elle souhaite se retirer);

  — et si elle souhaite renouveler sa certification, vérifier également que pendant la période d'expiration de sa certification, elle a appliqué les principes aux données à caractère personnel reçues en vertu du CPD UE — États-Unis et préciser les mesures qu'elle prendra pour résoudre les problèmes en suspens qui ont retardé sa recertification.

— Si une organisation est radiée de la liste du cadre de protection des données pour l'une des raisons suivantes: a) retrait du CPD UE — États-Unis, b) manquement à son obligation de recertification annuelle de son adhésion aux principes (c'est-à-dire qu'elle a commencé, mais n'a pas achevé le processus de recertification annuelle dans les délais ou qu'elle n'a même pas commencé le processus de recertification annuelle), ou c) «non-respect persistant», le ministère enverra une notification au(x) contact(s) indiqué(s) dans la déclaration d'autocertification de l'organisation, précisant la raison de la suppression et expliquant qu'elle doit cesser d'affirmer de manière explicite ou implicite qu'elle participe ou se conforme au CPD UE — États-Unis et qu'elle peut recevoir des données à caractère personnel conformément au CPD UE — États-Unis. La notification, qui peut également contenir d'autres éléments adaptés à la raison de la suppression, indiquera que les organisations qui font de fausses déclarations sur leur participation ou leur conformité au CPD UE — États-Unis, notamment lorsqu'elles déclarent participer au CPD UE — États-Unis après avoir été radiées de la liste du cadre de protection des données, sont susceptibles de faire l'objet de mesures répressives de la part de la FTC, du ministère des transports ou de toute autre instance administrative compétente.

Rechercher et réprimer les fausses déclarations de participation

— De manière systématique, lorsqu'une organisation a) se retire du CPD UE — États-Unis, b) manque à son obligation de recertification annuelle de son adhésion aux principes (c'est-à-dire qu'elle a commencé, mais n'a pas achevé le processus de recertification annuelle dans les délais ou qu'elle n'a même pas commencé le processus de recertification annuelle), c) est exclue du CPD UE — États-Unis notamment pour «non-respect persistant» ou d) manque à son obligation d'autocertification initiale de son adhésion aux principes (c'est-à-dire qu'elle a commencé, mais n'a pas achevé le processus d'autocertification initiale dans les délais), le ministère procédera d'office à des vérifications tendant à s'assurer que l'organisation a supprimé de ses déclarations publiques relatives à sa politique en matière de protection de la vie privée toute référence au CPD UE — États-Unis qui laisserait entendre qu'elle participe au CPD UE — États-Unis et qu'elle peut recevoir des données à caractère personnel conformément au CPD UE — États-Unis. Si le ministère constate de telles références, il informera l'organisation qu'il saisira, au besoin, l'organisme compétent pour d'éventuelles mesures coercitives si elle continue de faire de fausses déclarations concernant sa participation au CPD UE — États-Unis. Le ministère informera les organisations par les moyens de contact que les organisations lui ont communiqués ou, si nécessaire, par d'autres moyens appropriés. Si l'organisation ne supprime pas les références ni n'autocertifie son adhésion aux principes du CPD UE — États-Unis conformément aux procédures du ministère, le ministère saisira d'office la FTC, le ministère des transports ou toute autre autorité répressive compétente, ou prendra d'autres mesures qui s'imposent pour garantir l'utilisation appropriée de la marque de certification du CPD UE — États-Unis.

— Le ministère mobilisera d'autres efforts pour détecter les fausses déclarations de participation au CPD UE — États-Unis et l'usage abusif de la marque de certification correspondante, notamment par des organisations qui, contrairement aux organisations décrites ci-dessus, n'ont jamais entamé le processus d'autocertification (par exemple, en effectuant des recherches appropriées sur l'internet pour relever les références au CPD UE — États-Unis dans les politiques en matière de protection de la vie privée adoptées par les organisations). Lorsque, dans le cadre de ces efforts, le ministère constate de fausses déclarations de participation au CPD UE — États-Unis et l'usage abusif de la marque de certification correspondante, il informera l'organisation qu'il saisira, au besoin, l'organisme compétent pour d'éventuelles mesures coercitives si elle continue de faire de fausses déclarations concernant sa participation au CPD UE — États-Unis. Le ministère informera les organisations par les moyens de contact que les organisations lui ont communiqués le cas échéant ou, si nécessaire, par d'autres moyens appropriés. Si l'organisation ne supprime pas les références ni n'autocertifie son adhésion aux principes du CPD UE — États-Unis conformément aux procédures du ministère, le ministère saisira d'office la FTC, le ministère des transports ou toute autre autorité répressive compétente, ou prendra d'autres mesures qui s'imposent pour garantir l'utilisation appropriée de la marque de certification du CPD UE — États-Unis.

— Le ministère étudiera et traitera rapidement les réclamations spécifiques et sérieuses pour fausse déclaration de participation au CPD UE — États-Unis que le ministère reçoit (par exemple, des réclamations reçues des APD, des mécanismes de recours indépendants proposés par des organismes de règlement extrajudiciaire des litiges du secteur privé, des personnes concernées, des entreprises de l'Union et américaines, et d'autres types de tiers).

— En outre, le ministère prendra éventuellement d'autres mesures correctives appropriées. Toute fausse déclaration au ministère peut donner lieu à des poursuites au titre de la loi sur les fausses déclarations (18 U.S.C., § 1001).

Réaliser d'office périodiquement des contrôles de conformité et des évaluations du programme du cadre de protection des données

— De manière permanente, le ministère mobilisera des efforts pour contrôler la conformité effective des organisations participant au CPD UE — États-Unis afin de déceler les problèmes qui pourraient nécessiter un suivi complémentaire. En particulier, le ministère effectuera d'office des contrôles ponctuels d'organisations participant au CPD UE — États-Unis sélectionnées de manière aléatoire, ainsi que des contrôles ponctuels ad hoc de certaines organisations participant au CPD UE — États-Unis lorsque des manquements potentiels sont constatés (par exemple, des manquements potentiels signalés au ministère par des tiers) afin de vérifier: a) que le ou les services à contacter en cas de réclamation, pour des demandes d'accès et pour toute autre question relevant du CPD UE — États-Unis sont disponibles; b) le cas échéant, que les dispositions publiques de la politique en matière de protection de la vie privée de l'organisation peuvent être consultées par le public à la fois sur le site web public de l'organisation et via un hyperlien sur la liste du cadre de protection des données; c) que la politique de protection de la vie privée de l'organisation continue de respecter les exigences en matière d'autocertification décrites dans les principes; et d) que le mécanisme de recours indépendant indiqué par l'organisation peut être saisi en cas de réclamations introduites au titre du CPD UE — États-Unis. Le ministère surveillera également activement les informations qui fournissent des indices crédibles du non-respect des principes par les organisations participant au CPD UE — États-Unis.

— Dans le cadre du contrôle de la conformité, le ministère exigera qu'une organisation participant au CPD UE — États-Unis remplisse et transmette au ministère un questionnaire détaillé lorsque: a) le ministère a reçu des réclamations spécifiques et sérieuses liées au non-respect des principes par l'organisation, b) l'organisation ne répond pas de manière satisfaisante aux demandes d'information du ministère concernant le CPD UE — États-Unis, ou c) des indices crédibles suggèrent que l'organisation ne respecte pas ses engagements au titre du CPD UE — États-Unis. Lorsque le ministère a envoyé un questionnaire détaillé à une organisation et que celle-ci n'y a pas répondu de manière satisfaisante, il informera l'organisation qu'il saisira, au besoin, l'organisme compétent pour d'éventuelles mesures coercitives s'il ne reçoit pas de réponse satisfaisante de l'organisation dans les délais impartis. Le ministère informera les organisations par les moyens de contact que les organisations lui ont communiqués ou, si nécessaire, par d'autres moyens appropriés. Si l'organisation ne donne pas de réponse satisfaisante dans les délais impartis, le ministère saisira d'office la FTC, le ministère des transports ou toute autre autorité répressive compétente, ou prendra d'autres mesures qui s'imposent pour garantir la conformité. Le ministère consultera, le cas échéant, les autorités compétentes chargées de la protection des données à propos de ces contrôles de conformité.

— En outre, le ministère évaluera régulièrement la gestion et la supervision du programme du cadre de protection des données, afin de s'assurer que ses efforts de suivi, notamment les efforts déployés au moyen d'outils de recherche (par exemple, pour vérifier les liens brisés vers les politiques en matière de protection de la vie privée des organisations participant au CPD UE — États-Unis), sont adaptés pour répondre aux problèmes existants et aux nouveaux problèmes à mesure qu'ils se présentent.

Adapter le site web du cadre de protection des données à des publics ciblés

Le ministère organisera le site web du cadre de protection afin de l'adapter aux publics cibles suivants: les citoyens européens, les entreprises de l'Union, les entreprises américaines et les APD. L'inclusion de matériel d'information ciblant directement les citoyens et les entreprises de l'Union favorisera la transparence de plusieurs manières. À l'intention des citoyens de l'Union, le site web expliquera clairement: 1) les droits que le CPD UE — États-Unis confère aux citoyens de l'Union; 2) les mécanismes de recours qui sont à leur disposition s'ils estiment qu'une organisation a violé son engagement de respecter les principes; et 3) comment obtenir des renseignements sur l'autocertification d'une organisation au titre du CPD UE — États-Unis. À l'intention des entreprises de l'Union, il facilitera les vérifications suivantes: 1) la confirmation qu'une organisation participe au CPD UE — États-Unis; 2) le type d'informations couvertes par l'autocertification d'une organisation au titre du CPD UE — États-Unis; 3) la politique en matière de protection de la vie privée qui s'applique aux informations couvertes; et 4) la méthode qu'utilise l'organisation pour vérifier sa conformité aux principes. À l'intention des entreprises américaines, le site web expliquera clairement: 1) les avantages de participer au CPD UE — États-Unis; 2) comment adhérer au CPD UE — États-Unis, ainsi que comment renouveler sa certification ou se retirer du CPD UE — États-Unis; et 3) comment les États-Unis gèrent et font respecter le CPD UE — États-Unis. L'inclusion de matériel d'information ciblant directement les APD (par exemple, sur le point de contact spécifique du ministère pour les APD et un hyperlien vers le contenu relatif aux principes sur le site web de la FTC) favorisera à la fois la coopération et la transparence. Le ministère coopérera également sur une base ad hoc avec la Commission et le comité européen de la protection des données pour concevoir du matériel supplémentaire d'actualité (par exemple, des réponses aux questions fréquemment posées) à utiliser sur le site web du cadre de protection des données, lorsque de telles informations faciliteraient la gestion et la supervision efficaces du programme du cadre de protection des données.

Favoriser la coopération avec les APD

Pour accroître les possibilités de coopération avec les APD, le ministère maintiendra en son sein une personne de contact chargée de la liaison avec les APD. Dans les cas où une APD estime qu'une organisation participant au CPD UE — États-Unis ne se conforme pas aux principes, notamment à la suite d'une réclamation introduite par un citoyen de l'Union, elle pourra s'adresser à la personne de contact au ministère pour que l'organisation soit soumise à un examen plus approfondi. Le ministère mettra tout en œuvre pour faciliter le traitement de la réclamation avec l'organisation participant au CPD UE — États-Unis. Dans les 90 jours suivant la réception de la réclamation, il communiquera l'état d'avancement du dossier à l'APD. La personne de contact recevra également les réclamations qui lui seront déférées concernant des organisations qui prétendent faussement participer au CPD UE — États-Unis. Celle-ci assurera le suivi de toutes les réclamations que les APD transmettent au ministère, lequel établira, dans le cadre du réexamen conjoint décrit ci-après, un rapport analysant sous forme agrégée les réclamations reçues chaque année. Le point de contact aidera les APD qui cherchent à obtenir des renseignements sur l'autocertification ou la participation antérieure d'une organisation donnée au CPD UE — États-Unis et répondra aux demandes d'information des APD concernant la mise en œuvre d'exigences spécifiques du CPD UE — États-Unis. Le ministère coopérera également avec la Commission et le comité européen de la protection des données sur les aspects procéduraux et administratifs du panel d'APD, notamment l'établissement de procédures appropriées pour la distribution des fonds collectés au moyen de la cotisation du panel d'APD. Nous croyons savoir que la Commission coopérera avec le ministère pour faciliter la résolution de tout problème qui pourrait se poser concernant ces procédures. En outre, le ministère fournira aux APD des informations sur le CPD UE — États-Unis pour qu'elles les intègrent à leur propre site web, aux fins de renforcer la transparence pour les citoyens et les entreprises de l'Union. Une sensibilisation accrue au CPD UE — États-Unis ainsi qu'aux droits et devoirs qu'il confère devrait faciliter le recensement des problèmes à mesure qu'ils se présentent et, partant, la mise en place de solutions appropriées.

Remplir ses engagements au titre de l'annexe I des principes

Le ministère remplira ses engagements au titre de l'annexe I des principes, au nombre desquels tenir une liste des arbitres choisis avec la Commission sur la base de leur indépendance, de leur intégrité et de leur expertise, et aider, si nécessaire, le tiers choisi par le ministère pour gérer les arbitrages conformément à l'annexe I des principes ([3]) et pour gérer le fonds d'arbitrage décrit dans ladite annexe. Le ministère coopérera avec ce tiers pour vérifier, entre autres, qu'il possède un site web contenant des orientations sur la procédure d'arbitrage, concernant notamment: 1) comment entamer des poursuites et transmettre des documents; 2) la liste des arbitres tenue par le ministère et comment choisir les arbitres dans cette liste; 3) les procédures d'arbitrage et le code de conduite des arbitres adoptés par le ministère et la Commission ([4]); et 4) la perception et le paiement des redevances d'arbitrage. En outre, le ministère coopérera avec le tiers pour examiner régulièrement le fonctionnement du fonds, notamment la nécessité éventuelle d'ajuster le montant des contributions ou des plafonds, et prendra en considération, entre autres, le nombre d'arbitrages et les coûts et durées des arbitrages, étant bien entendu qu'aucune charge financière excessive ne sera imposée aux organisations participant au CPD UE — États-Unis. Le ministère informera la Commission du résultat de ces examens avec le tiers et notifiera au préalable à la Commission tout ajustement du montant des contributions.

Réaliser des examens conjoints du fonctionnement du CPD UE — États-Unis

Le ministère et, au besoin, d'autres organismes tiendront des réunions périodiques avec la Commission, les APD concernées et les représentants compétents du comité européen de la protection des données, au cours desquelles le ministère fera le point sur le CPD UE — États-Unis. Ces réunions permettront notamment d'examiner les questions d'actualité sur le fonctionnement, la mise en œuvre, la supervision et le contrôle de la mise en application du programme du cadre de protection des données. Elles pourront, au besoin, porter sur des sujets connexes, tels que les autres mécanismes de transfert des données qui bénéficient des garanties en vertu du CPD UE — États-Unis.

([3]) L'International Centre for Dispute Resolution (ci-après l'«ICDR»), la division internationale de l'American Arbitration Association (ci-après l'«AAA») (collectivement l'«ICDR-AAA»), a été choisi par le ministère pour gérer les arbitrages conformément à l'annexe I des principes et pour gérer le fonds d'arbitrage décrit dans ladite annexe.

([4]) Le 15 septembre 2017, le ministère et la Commission sont convenus d'adopter un ensemble de règles d'arbitrage pour régir les procédures arbitrales contraignantes décrites à l'annexe I des principes, ainsi qu'un code de conduite pour les arbitres qui est conforme aux normes éthiques généralement acceptées pour les arbitres commerciaux et à l'annexe I des principes. Le ministère et la Commission sont convenus d'adapter les règles d'arbitrage et le code de conduite pour tenir compte des mises à jour en vertu du CPD UE — États-Unis et le ministère coopérera avec l'ICDR-AAA pour effectuer ces mises à jour.

Mise à jour de la législation

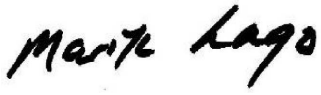
Le ministère mettra tout en œuvre pour informer la Commission de toute évolution importante de la législation aux États-Unis dans la mesure où cela concerne le CPD UE — États-Unis s'agissant du respect de la vie privée à l'égard du traitement des données et des restrictions et garanties applicables à l'accès aux données à caractère personnel par les autorités publiques américaines et l'utilisation ultérieure de ces données.

Accès du gouvernement américain aux données à caractère personnel

Les États-Unis ont publié le décret présidentiel 14086, intitulé «Enhancing Safeguards for United States Signals Intelligence Activities» et le titre 28 du CFR, partie 201, modifiant les règlements du ministère de la justice pour établir la Cour chargée du contrôle de la protection des données (Data Protection Review Court, ci-après la «DPRC») qui assurent une forte protection des données à caractère personnel en ce qui concerne l'accès du gouvernement aux données à des fins de sécurité nationale. Parmi les protections prévues figurent: le renforcement des garanties en matière de protection de la vie privée et des libertés civiles afin de s'assurer que les activités de renseignement d'origine électromagnétique des États-Unis sont nécessaires et proportionnées à la poursuite d'objectifs de sécurité nationale définis; la mise en place d'une nouvelle instance de recours dotée d'une autorité indépendante et contraignante; et le renforcement de la surveillance rigoureuse et à plusieurs niveaux des activités de renseignement d'origine électromagnétique des États-Unis. Grâce à ces protections, les citoyens de l'Union peuvent demander réparation auprès d'une nouvelle instance de recours à plusieurs niveaux qui comprend une DPRC indépendante composée de personnes choisies en dehors du gouvernement des États-Unis. Ces personnes seraient pleinement habilitées à statuer sur les plaintes et à prendre les mesures de réparation nécessaires. Le ministère tiendra un registre des personnes de l'Union qui déposent une réclamation qualifiée en vertu du décret présidentiel 14086 et du titre 28 du CFR, partie 201. Cinq ans après la date de la présente lettre, et tous les cinq ans par la suite, le ministère contactera les organismes concernés pour savoir si les informations relatives à l'examen des réclamations qualifiées ou à l'examen des demandes de révision soumises à la DPRC ont été déclassifiées. Si ces informations ont été déclassifiées, le ministère collaborera avec l'APD compétente pour en informer le citoyen de l'Union. Ces améliorations confirment que les données à caractère personnel de l'Union transférées vers les États-Unis seront traitées d'une manière conforme aux dispositions juridiques de l'Union en ce qui concerne l'accès des pouvoirs publics aux données.

Sur la base des principes, du décret présidentiel 14086, du titre 28 du CFR, partie 201, ainsi que des lettres et documents qui les accompagnent, dont font partie les présents engagements du ministère concernant la gestion et la supervision du dispositif, nous espérons que la Commission considérera que le CPD UE — États-Unis assure un niveau de protection adéquat aux fins du droit de l'Union et que les transferts de données depuis l'Union européenne se poursuivront vers les organisations participant au CPD UE — États-Unis. Nous espérons également que les transferts vers des organisations américaines effectués sur la base de clauses contractuelles types ou de règles d'entreprise contraignantes de l'Union seront encore facilités par les dispositions du CPD UE — États-Unis.

Je vous prie, Monsieur le Commissaire, d'agréer
l'expression de ma haute considération.



Marisa Lago

ANNEXE IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

9 juin 2023

Monsieur Didier Reynders
Commissaire à la justice
Commission européenne
Rue de la Loi, 200
1049 Bruxelles
Belgique

Monsieur le Commissaire,

La commission fédérale du commerce des États-Unis (Federal Trade Commission, ci-après la «FTC») apprécie l'occasion qui lui est donnée d'évoquer son rôle dans l'application des principes du cadre de protection des données UE — États-Unis (ci-après le «CPD UE — États-Unis»). La FTC s'est engagée depuis longtemps à protéger les consommateurs et la vie privée partout dans le monde, et nous nous engageons à faire respecter les aspects de ce cadre relatifs au secteur commercial. La FTC joue ce rôle depuis l'an 2000, en lien avec le cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne, et plus récemment depuis 2016, en lien avec le cadre du bouclier de protection des données UE — États-Unis ([1]). Le 16 juillet 2020, la Cour de justice de l'Union européenne (ci-après la «CJUE») a invalidé la décision d'adéquation de la Commission européenne qui sous-tendait le cadre du bouclier de protection des données UE — États-Unis, sur la base de problèmes autres que les principes commerciaux appliqués par la FTC. Les États-Unis et la Commission européenne ont depuis négocié le cadre de protection des données UE — États-Unis pour tenir compte de cet arrêt de la CJUE.

Je vous adresse la présente lettre afin de confirmer que la FTC s'engage à faire respecter les principes du CPD UE — États-Unis. Nous affirmons notamment notre engagement dans trois domaines clés: 1) la hiérarchisation et l'instruction des dossiers soumis; 2) la recherche et le suivi des ordonnances; et 3) la coopération en matière de mise en application avec les autorités chargées de la protection des données (ci-après les «APD») de l'Union.

I. **Introduction**

a. **Travaux de la FTC concernant le respect de la vie privée et l'élaboration de politiques en la matière**

La FTC possède de larges pouvoirs civils de mise en application visant à promouvoir la protection des consommateurs et la concurrence dans la sphère commerciale. Dans le cadre de son mandat de protection des consommateurs, la FTC veille à l'application d'un large éventail de lois afin de protéger la confidentialité et la sécurité des consommateurs et de leurs

([1]) Lettre de la présidente Edith Ramirez à Věra Jourová, commissaire pour la justice, les consommateurs et l'égalité des genres de la Commission européenne, décrivant l'application par la commission fédérale du commerce du nouveau cadre du bouclier de protection de la vie privée UE — États-Unis (29 février 2016), disponible à l'adresse suivante: https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. La FTC s'était également engagée précédemment à faire respecter le cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne. Lettre de Robert Pitofsky, président de la FTC, à John Mogg, directeur de la DG Marché intérieur, Commission européenne (14 juillet 2000), disponible à l'adresse suivante: https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. La présente lettre remplace ces engagements antérieurs.

données. La législation primaire mise en application par la FTC, la loi portant établissement de la commission fédérale du commerce (ci-après le «FTC Act»), interdit les actes ou pratiques «déloyaux» ou «frauduleux» dans le domaine du commerce ([2]). La FTC applique également une législation ciblée qui vise à protéger les informations en matière de santé, de crédit et d'autres aspects financiers, ainsi que les informations en ligne concernant les enfants; elle a publié des réglementations mettant en œuvre chacun de ces actes ([3]).

La FTC a également lancé récemment de nombreuses initiatives visant à renforcer ses travaux dans le domaine de la protection de la vie privée. En août 2022, la FTC a annoncé qu'elle envisageait d'adopter des règles pour réprimer la surveillance commerciale préjudiciable et la sécurité laxiste des données ([4]). L'objectif de ce projet est de constituer un dossier public solide afin de déterminer si la FTC doit édicter des règles concernant les pratiques de surveillance commerciale et de sécurité des données, et ce à quoi ces règles devraient éventuellement ressembler. Nous avons invité les parties intéressées de l'Union à formuler des observations sur cette initiative et sur d'autres.

Nos conférences «PrivacyCon» continuent de réunir des chercheurs de premier plan pour discuter des dernières recherches et tendances en matière de protection des données des consommateurs et de sécurité des données. Nous avons également renforcé la capacité de notre agence à suivre le rythme des évolutions technologiques qui figurent au cœur de la plupart de nos travaux en matière de protection de la vie privée, en constituant une équipe croissante de techniciens et de chercheurs interdisciplinaires. Comme vous le savez, nous avons également annoncé un dialogue conjoint avec vous et vos collègues de la Commission européenne, qui prévoit d'aborder des sujets liés à la protection de la vie privée tels que les modèles obscurs et les modèles commerciaux caractérisés par une collecte omniprésente de données ([5]). Nous avons également publié récemment un rapport au Congrès mettant en garde contre les inconvénients liés à l'utilisation de l'intelligence artificielle (ci-après l'«IA») pour remédier aux problèmes en ligne observés par le Congrès. Ce rapport a exprimé des inquiétudes quant à l'inexactitude, la partialité, la discrimination et la surveillance commerciale ([6]).

b. **Mesures de protection juridiques aux États-Unis bénéficiant aux consommateurs de l'Union**

Le CPD UE — États-Unis s'inscrira dans le contexte plus large des mesures adoptées aux États-Unis qui protègent aussi les consommateurs de l'Union de différentes façons. L'interdiction des actes et pratiques déloyaux ou frauduleux instaurée par le FTC Act ne se limite pas à protéger les consommateurs américains contre les entreprises américaines, étant donné qu'elle couvre également les pratiques qui 1) entraînent ou sont susceptibles d'entraîner des préjudices raisonnablement prévisibles aux États-Unis ou 2) impliquent un comportement concret aux États-Unis. Pour protéger les consommateurs étrangers, la FTC peut, par ailleurs, user de toutes les mesures de réparation auxquelles il est possible de recourir pour protéger les consommateurs américains ([7]).

La FTC assure aussi le respect d'autres lois ciblées dont la portée en matière de protection s'étend aux consommateurs non américains, comme la loi sur le respect de la vie privée des enfants en ligne (Children's Online Privacy Protection Act, COPPA). Entre autres choses, le COPPA exige des opérateurs de sites internet et de services en ligne destinés aux enfants, ou de sites destinés à un public général qui collectent sciemment des informations à caractère personnel d'enfants âgés de moins de treize ans, qu'ils en informent les parents et qu'ils obtiennent un consentement parental vérifiable. Les sites

([2]) 15 U.S.C. § 45(a). La FTC n'est pas compétente pour faire exécuter la législation pénale ni en ce qui concerne les questions de sécurité nationale. La FTC n'est pas non plus habilitée à se pencher sur la plupart des autres mesures prises par les pouvoirs publics. Il existe par ailleurs des exceptions à la compétence de la FTC en matière de pratiques commerciales, notamment en ce qui concerne les banques, les compagnies aériennes, l'assurance et les activités habituelles des fournisseurs de services de télécommunications. La plupart des organisations sans but lucratif ne sont pas de son ressort, mais elle peut en revanche connaître des fausses organisations caritatives ou autres organisations sans but lucratif dont l'activité vise en fait la réalisation d'un profit. La FTC est également compétente pour contrôler les organisations sans but lucratif qui travaillent pour le bénéfice de leurs membres poursuivant un but lucratif, notamment en assurant des avantages économiques importants à ces membres. Dans certains cas, les compétences de la FTC recoupent celles d'autres agences chargées de l'application des lois. Nous avons établi des relations de travail solides avec les autorités fédérales et les autorités des États, et nous collaborons étroitement avec ces autorités pour coordonner des enquêtes ou procéder à des renvois, s'il a lieu.

([3]) *Voir* FTC, «Privacy and Security», https://www.ftc.gov/business-guidance/privacy-security

([4]) *Voir* communiqué de presse de la FTC, «FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices» (11 août 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

([5]) *Voir* communiqué de presse conjoint de Didier Reynders, commissaire à la justice de la Commission européenne, et de Lina Khan, présidente de la commission fédérale du commerce des États-Unis (30 mars 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf

([6]) *Voir* communiqué de presse de la FTC, «FTC Report Warns About Using Artificial Intelligence to Combat Online Problems» (16 juin 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems

([7]) 15 U.S.C. § 45(a)(4)(B). En outre, les «actes ou pratiques déloyaux ou frauduleux» comprennent les actes ou pratiques concernant le commerce extérieur qui i) entraînent ou sont susceptibles d'entraîner des préjudices raisonnablement prévisibles aux États-Unis; ou ii) impliquent un comportement concret aux États-Unis. 15 U.S.C. § 45(a)(4)(A).

internet et services basés aux États-Unis qui sont soumis à la COPPA et qui collectent des informations à caractère personnel auprès d'enfants étrangers sont tenus de respecter la COPPA. Les sites internet et services en ligne basés à l'étranger doivent également respecter la COPPA s'ils ciblent les enfants américains ou s'ils collectent sciemment des informations à caractère personnel auprès d'enfants aux États-Unis. De plus, outre les lois fédérales américaines dont la FTC assure l'application, d'autres lois en matière de protection des consommateurs, de violation de données et de protection de la vie privée au niveau fédéral et au niveau des États sont susceptibles d'apporter des avantages aux consommateurs de l'Union.

c. **Activité de mise en application de la législation de la FTC**

La FTC a intenté des actions au titre du cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne et du cadre du bouclier de protection des données UE — États-Unis et a continué de faire respecter le bouclier de protection des données UE — États-Unis même après l'invalidation de la décision d'adéquation sous-tendant le cadre du bouclier de protection des données UE — États-Unis ([8]). Plusieurs réclamations récentes de la FTC ont inclus des chefs d'accusation selon lesquels des entreprises auraient violé les dispositions du bouclier de protection des données UE — États-Unis, notamment dans le cadre de procédures engagées contre Twitter ([9]), CafePress ([10]) et Flo ([11]). Dans le cadre de l'action engagée contre Twitter, la FTC a obtenu 150 millions d'USD de la part de Twitter pour avoir violé une ordonnance antérieure de la FTC avec des pratiques touchant plus de 140 millions de clients, notamment la violation du principe 5 du bouclier de protection des données UE — États-Unis (Intégrité des données et limitation des finalités). En outre, l'ordonnance de l'agence exige que Twitter permette aux utilisateurs d'utiliser des méthodes d'authentification sécurisées à plusieurs facteurs qui n'obligent pas les utilisateurs à donner leur numéro de téléphone.

Dans l'affaire *CafePress*, la FTC a allégué que l'entreprise n'avait pas sécurisé les informations sensibles des consommateurs, qu'elle avait dissimulé une importante violation de données et qu'elle avait violé les principes 2 («Choix»), 4 («Sécurité») et 6 («Accès») du bouclier de protection des données UE — États-Unis. L'ordonnance de la FTC impose à l'entreprise de remplacer les mesures d'authentification inadéquates par une authentification multifactorielle, de limiter considérablement la quantité de données qu'elle collecte et conserve, de chiffrer les numéros de sécurité sociale, de faire évaluer ses programmes de sécurité de l'information par un tiers et de communiquer à la FTC une copie de cette évaluation qui pourra être rendue publique.

Dans l'affaire *Flo*, la FTC a allégué que l'application de suivi de la fertilité avait divulgué des informations sur la santé des utilisateurs à des fournisseurs tiers d'analyse de données après s'être engagée à préserver la confidentialité de ces informations. La plainte de la FTC mentionne spécifiquement les interactions de l'entreprise avec les consommateurs de l'Union et indique que Flo a violé les principes 1 («Notification»), 2 («Choix»), 3 («Responsabilité en cas de transfert ultérieur») et 5 («Intégrité des données et limitation des finalités») du bouclier de protection des données UE — États-Unis. L'ordonnance de l'agence impose entre autres à Flo d'informer les utilisateurs concernés de la divulgation de leurs informations à caractère personnel et de demander à tout tiers ayant reçu des informations sur la santé des utilisateurs de détruire ces données. Il importe de signaler que les ordonnances de la FTC protègent, dans le monde entier, tous les consommateurs ayant des interactions avec une entreprise américaine, et pas uniquement les consommateurs qui ont déposé une plainte.

Dans de nombreuses affaires relatives à l'application du cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne et du cadre du bouclier de protection des données UE — États-Unis, il s'agissait d'organisations qui avaient procédé à une autocertification initiale auprès du ministère américain du commerce, mais qui n'avaient pas maintenu leur autocertification annuelle alors qu'elles continuaient à déclarer participer au dispositif. D'autres affaires concernaient de fausses déclarations de participation de la part d'organisations qui n'avaient jamais procédé à une autocertification initiale auprès du ministère américain du commerce. À l'avenir, nous prévoyons de concentrer nos efforts de mise en application proactive sur les types de violations substantielles des principes du CPD UE — États-Unis alléguées dans des affaires telles que Twitter, CafePress et Flo. Dans l'intervalle, le ministère américain du commerce gérera et supervisera le processus d'autocertification, tiendra la liste officielle des participants au CPD UE — États-Unis et traitera d'autres questions relatives aux déclarations de participation au programme ([12]). Il est important de noter que les organisations qui prétendent participer au CPD UE — États-Unis peuvent être soumis à une application substantielle des principes du CPD UE — États-Unis même si elles n'ont pas ou n'ont plus autocertifié leur adhésion auprès du ministère américain du commerce.

([8]) *Voir* annexe A pour une liste des questions relatives à la sphère de sécurité et au bouclier de protection des données de la FTC.

([9]) *Voir* communiqué de presse de la FTC, «FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads» (25 mai 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads

([10]) *Voir* communiqué de presse de la FTC, «FTC Takes Action Against CafePress for Data Breach Cover Up» (15 mars 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover

([11]) *Voir* communiqué de presse de la FTC, «FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others» (22 juin 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

([12]) Lettre de Marisa Lago, sous-secrétaire au commerce chargée du commerce international, à M. Didier Reynders, Commissaire à la justice, Commission européenne (12 décembre 2022).

II. **Hiérarchisation et instruction des dossiers soumis**

Tout comme nous l'avons fait pour le cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne et le cadre du bouclier de protection des données UE — États-Unis, la FTC s'engage à donner la priorité aux dossiers que le ministère du commerce et les États membres de l'Union lui transmettent en lien avec les principes du CPD UE — États-Unis. Nous donnerons également la priorité aux dossiers transmis concernant le non-respect des principes du CPD UE — États-Unis par des organisations d'autoréglementation en matière de protection de la vie privée et d'autres organes indépendants de règlement des litiges.

Afin de faciliter la saisine par les États membres de l'Union en vertu du CPD UE — États-Unis, la FTC a mis en place une procédure normalisée de saisine et a fourni des orientations aux États membres de l'Union quant au type d'informations les mieux à même de l'aider dans l'instruction des dossiers. Dans le cadre de cette démarche, la FTC a désigné un point de contact en son sein pour les dossiers transmis par les États membres de l'Union. Il est vivement recommandé que l'autorité soumettant un dossier ait procédé à une instruction préliminaire sur la violation alléguée et soit en mesure de coopérer avec la FTC dans l'éventualité d'une enquête.

Après avoir été saisie par le ministère américain du commerce, par un État membre de l'Union ou par une organisation d'autoréglementation ou d'autres organes indépendants de règlement des litiges, la FTC peut prendre différentes mesures pour remédier aux problèmes soulevés. Nous pouvons, par exemple, examiner les politiques de protection de la vie privée de l'organisation concernée, obtenir des informations complémentaires directement auprès de l'organisation ou auprès de tiers, assurer un suivi avec l'entité qui a soumis le dossier, déterminer s'il existe une tendance systématique aux violations ou un nombre important de consommateurs affectés, déterminer si le dossier touche à des aspects relevant des compétences du ministère du commerce, étudier l'utilité éventuelle d'efforts supplémentaires pour informer les participants au marché et, le cas échéant, lancer une procédure d'exécution.

Outre la hiérarchisation des dossiers relatifs aux principes du CPD UE — États-Unis soumis par le ministère américain du commerce, par des États membres de l'Union et par des organisations d'autoréglementation ou d'autres organes indépendants de règlement des litiges ([13]), la FTC continuera d'enquêter sur les violations substantielles des principes du CPD UE — États-Unis de sa propre initiative s'il y a lieu, en utilisant un éventail d'outils. Dans le cadre du programme d'enquêtes de la FTC sur les aspects de la protection de la vie privée et de la sécurité impliquant des organisations commerciales, l'agence a régulièrement vérifié si l'entité concernée faisait des déclarations au titre du bouclier de protection des données UE — États-Unis. Dans les cas où l'entité a fait des déclarations de ce type et où l'enquête révèle des violations manifestes des principes du bouclier de protection des données UE — États-Unis, la FTC inclut les allégations de violation des principes du bouclier de protection des données UE — États-Unis dans ses actions de mise en application. Nous poursuivrons notre stratégie proactive, désormais en ce qui concerne le respect des principes du CPD UE — États-Unis.

III. **Recherche et suivi des ordonnances**

La FTC s'engage également à rechercher et à assurer le suivi des ordonnances d'exécution afin de garantir le respect du cadre des principes du CPD UE — États-Unis. Nous exigerons le respect des principes du CPD UE — États-Unis par différentes injonctions appropriées dans les futures ordonnances relatives aux principes du CPD UE — États-Unis. Le non-respect d'ordonnances administratives de la FTC peut entraîner des sanctions civiles allant jusqu'à 50 120 USD par infraction ou 50 120 USD par jour en cas d'infraction persistante ([14]). Dans le cas de pratiques touchant de nombreux consommateurs, ces sanctions peuvent s'élever à plusieurs millions de dollars. Chaque ordonnance par consentement contient également des dispositions en matière de rapport et de mise en conformité. Les entités soumises à une ordonnance doivent conserver les documents attestant de leur conformité pendant un nombre d'années déterminé. Les ordonnances doivent également être communiquées aux membres du personnel chargés d'en assurer le respect.

La FTC contrôle systématiquement le respect des ordonnances existantes relatives aux principes du bouclier de protection des données UE — États-Unis, comme elle le fait pour toutes ses autres ordonnances, et engage des actions en vue de les faire respecter si nécessaire ([15]). Il importe de signaler que les ordonnances de la FTC continueront de protéger, dans le monde entier, tous les consommateurs ayant des interactions avec une entreprise, et pas uniquement les consommateurs qui ont déposé une plainte. Enfin, la FTC tiendra une liste en ligne d'entreprises faisant l'objet d'ordonnances liées à l'application des principes du CPD UE — États-Unis ([16]).

([13]) Même si la FTC n'intervient pas pour traiter les plaintes de consommateurs individuels ou jouer un rôle de médiateur dans ces dossiers, elle affirme qu'elle accordera la priorité aux dossiers relatifs aux principes du CPD UE — États-Unis soumis par les APD de l'Union. Par ailleurs, la FTC utilise les plaintes enregistrées dans sa base de données «Consumer Sentinel», accessible à de nombreux autres organes répressifs, pour repérer les tendances, déterminer les priorités de mise en application et recenser les cibles d'enquêtes potentielles. Les citoyens de l'Union peuvent utiliser le système de plaintes accessible aux ressortissants américains pour soumettre une plainte à la FTC à l'adresse www.ftc.gov/complaint. Pour les plaintes individuelles relatives aux principes du CPD UE — États-Unis, cependant, il peut être préférable pour les citoyens de l'Union de soumettre les plaintes à l'APD de leur État membre ou à un organe indépendant de règlement des litiges.

([14]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Ce montant est régulièrement ajusté en fonction de l'inflation.

([15]) L'année dernière, la FTC a voté en faveur d'une rationalisation de la procédure d'enquêtes sur les récidives. *Voir* communiqué de presse de la FTC, «FTC Authorizes Investigations into Key Enforcement Priorities» (1er juillet 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities

([16]) *Voir* FTC, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield

IV. **Coopération en matière d'application avec les APD de l'Union**

La FTC a conscience du rôle important joué par les APD de l'Union dans le respect des principes du CPD UE — États-Unis et encourage un renforcement des initiatives de consultation et une coopération accrue en matière d'application de la réglementation. En effet, une approche coordonnée des défis posés par l'évolution actuelle du marché numérique et les modèles économiques faisant un usage intensif de données est de plus en plus essentielle. La FTC échangera des informations avec les autorités répressives qui ont soumis les dossiers, notamment sur l'état d'avancement des dossiers soumis, dans le respect des lois et restrictions applicables en matière de confidentialité. Dans la mesure du possible au vu du nombre et du type de dossiers soumis, les informations fournies comprendront une évaluation des éléments du dossier, et notamment une description des questions importantes soulevées et des mesures prises pour combattre les infractions à la loi relevant des compétences de la FTC. La FTC fournira aussi un retour d'information à l'autorité qui a soumis le dossier quant aux types de dossiers reçus afin d'accroître l'efficacité des démarches visant à lutter contre les comportements répréhensibles. Si une autorité répressive soumettant un dossier souhaite obtenir des informations sur l'état d'avancement des dossiers soumis afin de mener sa propre procédure coercitive, la FTC répondra en tenant compte du nombre de dossiers en cours d'examen et dans le respect des exigences de confidentialité et autres exigences légales.

La FTC travaillera également en étroite collaboration avec les APD de l'Union pour apporter une assistance à la mise en application. Selon le cas, cette assistance pourrait inclure un échange d'informations et une aide aux enquêtes conformément à la loi US SAFE WEB, qui autorise la FTC à apporter une assistance aux services répressifs étrangers lorsque le service concerné s'efforce de faire respecter des lois interdisant des pratiques essentiellement semblables aux pratiques interdites par les lois dont la FTC assure le respect ([17]). Dans le cadre de cette assistance, la FTC peut partager des informations obtenues en lien avec une enquête de la FTC, lancer une procédure obligatoire pour le compte de l'APD de l'Union menant sa propre enquête et recueillir le témoignage oral de témoins ou de défendeurs en lien avec la procédure de mise en application de l'APD, dans le respect des exigences de la loi US SAFE WEB. La FTC fait régulièrement usage de ce pouvoir pour apporter son assistance aux autorités du monde entier dans des dossiers de protection de la vie privée et des consommateurs.

Outre les consultations avec les APD sur des questions propres à chaque dossier qu'elles soumettent, la FTC participera à des réunions périodiques avec les représentants désignés du comité européen de la protection des données afin de discuter de manière générale de la façon d'améliorer la coopération en matière d'application. La FTC participera également, aux côtés du ministère américain du commerce, de la Commission européenne et des représentants du comité européen de la protection des données, à l'examen périodique du CPD UE–États-Unis afin de discuter de sa mise en œuvre. La FTC encourage également le développement d'outils qui amélioreront la coopération en matière de mise en application avec les APD de l'Union et avec les autres autorités d'application des règles de protection de la vie privée du monde entier. La FTC est heureuse de réaffirmer son engagement à faire appliquer les aspects du CPD UE — États-Unis relatifs au secteur commercial. Nous considérons notre partenariat avec nos collègues de l'Union comme un élément essentiel de la protection de la vie privée de nos concitoyens et des vôtres.

Je vous prie, Monsieur le Commissaire, d'agréer l'expression de ma haute considération.

Lina Khan

Lina M. KHAN

Présidente, Commission fédérale du commerce

([17]) Lorsqu'elle détermine si elle peut ou non exercer ses compétences au titre de la loi US SAFE WEB, la FTC tient compte, notamment, des éléments suivants: «A) si l'agence demandeuse a convenu de fournir ou fournira une assistance réciproque à la Commission; B) si le fait d'accéder à la demande porterait atteinte à l'intérêt public des États-Unis; et C) si la procédure d'enquête ou de mise en application de l'agence demandeuse porte sur des actes ou pratiques qui causent ou sont susceptibles de causer un préjudice à un nombre important de personnes». 15 U.S.C. § 46(j)(3). Ces compétences ne concernent pas la mise en application des législations relatives à la concurrence.

Appendice A

Application de la sphère de sécurité et du bouclier de protection des données

	Numéro de rôle/Dossier de la FTC nº	**Affaire**	**Lien**
1	Dossier de la FTC nº 2023062 Affaire nº 3:22-cv-03070 (N.D. Cal.)	US v. **Twitter, Inc.**	Twitter
2	Dossier de la FTC nº 192 3209	In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a **CafePress**, and PlanetArt, LLC, d/b/a **CafePress**	CafePress
3	Dossier de la FTC nº 192 3133 Numéro de rôle C-4747	In the Matter of **Flo Health, Inc.**	Flo Health
4	Dossier de la FTC nº 192 3050 Numéro de rôle C-4723	In the Matter of **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5	Dossier de la FTC nº 192 3092 Numéro de rôle C-4709	In the Matter of **T&M Protection, LLC**	T&M Protection
6	Dossier de la FTC nº 192 3084 Numéro de rôle C-4704	In the Matter of **TDARX, Inc.**	TDARX
7	Dossier de la FTC nº 192 3093 Numéro de rôle C-4706	In the Matter of **Global Data Vault, LLC**	Global Data
8	Dossier de la FTC nº 192 3078 Numéro de rôle C-4703	In the Matter of **Incentive Services, Inc.**	Incentive Services
9	Dossier de la FTC nº 192 3090 Numéro de rôle C-4705	In the Matter of **Click Labs, Inc.**	Click Labs
10	Dossier de la FTC nº 182 3192 Numéro de rôle C-4697	In the Matter of **Medable, Inc.**	Medable
11	Dossier de la FTC nº 182 3189 Numéro de rôle 9386	In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to **RagingWire Data Centers, Inc.**	RagingWire
12	Dossier de la FTC nº 182 3196 Numéro de rôle C-4702	In the Matter of **Thru, Inc.**	Thru
13	Dossier de la FTC nº 182 3188 Numéro de rôle C-4698	In the Matter of **DCR Workforce, Inc.**	DCR Workforce
14	Dossier de la FTC nº 182 3194 Numéro de rôle C-4700	In the Matter of **LotaData, Inc.**	LotaData
15	Dossier de la FTC nº 182 3195 Numéro de rôle C-4701	In the Matter of **EmpiriStat, Inc.**	EmpiriStat

16	Dossier de la FTC nº 182 3193 Numéro de rôle C-4699	In the Matter of 214 Technologies, Inc., also d/b/a **Trueface.ai**	Trueface.ai
17	Dossier de la FTC nº 182 3107 Numéro de rôle 9383	In the Matter of **Cambridge Analytica, LLC**	Cambridge Analytica
18	Dossier de la FTC nº 182 3152 Numéro de rôle C-4685	In the Matter of **SecureTest, Inc.**	SecurTest
19	Dossier de la FTC nº 182 3144 Numéro de rôle C-4664	In the Matter of **VenPath, Inc.**	VenPath
20	Dossier de la FTC nº 182 3154 Numéro de rôle C-4666	In the Matter of **SmartStart Employment Screening, Inc.**	SmartStart
21	Dossier de la FTC nº 182 3143 Numéro de rôle C-4663	In the Matter of **mResourceLLC,** d/b/a Loop Works LLC	mResource
22	Dossier de la FTC nº 182 3150 Numéro de rôle C-4665	In the Matter of **Idmission LLC**	IDmission
23	Dossier de la FTC nº 182 3100 Numéro de rôle C-4659	In the Matter of **ReadyTech Corporation**	ReadyTech
24	Dossier de la FTC nº 172 3173 Numéro de rôle C-4630	In the Matter of **Decusoft, LLC**	Decusoft
25	Dossier de la FTC nº 172 3171 Numéro de rôle C-4628	In the Matter of **Tru Communication, Inc.**	Tru
26	Dossier de la FTC nº 172 3172 Numéro de rôle C-4629	In the Matter of **Md7, LLC**	Md7
30	Dossier de la FTC nº 152 3198 Numéro de rôle C-4543	In the Matter of **Jhayrmaine Daniels (d/b/a California Skate-Line)**	Jhayrmaine Daniels
31	Dossier de la FTC nº 152 3190 Numéro de rôle C-4545	In the Matter of **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32	Dossier de la FTC nº 152 3141 Numéro de rôle C-4540	In the Matter of **Golf Connect, LLC**	Golf Connect
33	Dossier de la FTC nº 152 3202 Numéro de rôle C-4546	In the Matter of **Inbox Group, LLC**	Inbox Group
34	Dossier nº 152 3187 Numéro de rôle C-4542	In the Matter of **IOActive, Inc.**	IOActive
35	Dossier de la FTC nº 152 3140 Numéro de rôle C-4549	In the Matter of **Jubilant Clinsys, Inc.**	Jubilant
36	Dossier de la FTC nº 152 3199 Numéro de rôle C-4547	In the Matter of **Just Bagels Manufacturing, Inc.**	Just Bagels

37	Dossier de la FTC nº 152 3138 Numéro de rôle C-4548	In the Matter of **NAICS Association, LLC**	NAICS
38	Dossier de la FTC nº 152 3201 Numéro de rôle C-4544	In the Matter of **One Industries Corp.**	One Industries
39	Dossier de la FTC nº 152 3137 Numéro de rôle C-4550	In the Matter of **Pinger, Inc.**	Pinger
40	Dossier de la FTC nº 152 3193 Numéro de rôle C-4552	In the Matter of **SteriMed Medical Waste Solutions**	SteriMed
41	Dossier de la FTC nº 152 3184 Numéro de rôle C-4541	In the Matter of **Contract Logix, LLC**	Contract Logix
42	Dossier de la FTC nº 152 3185 Numéro de rôle C-4551	In the Matter of **Forensics Consulting Solutions, LLC**	Forensics Consulting
43	Dossier de la FTC nº 152 3051 Numéro de rôle C-4526	In the Matter of **American Int'l Mailing, Inc.**	AIM
44	Dossier de la FTC nº 152 3015 Numéro de rôle C-4525	In the Matter of **TES Franchising, LLC**	TES
45	Dossier de la FTC nº 142 3036 Numéro de rôle C-4459	In the Matter of **American Apparel, Inc.**	American Apparel
46	Dossier de la FTC nº 142 3026 Numéro de rôle C-4469	In the Matter of **Fantage.com, Inc.**	Fantage
47	Dossier de la FTC nº 142 3017 Numéro de rôle C-4461	In the Matter of **Apperian, Inc.**	Apperian
48	Dossier de la FTC nº 142 3018 Numéro de rôle C-4462	In the Matter of **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49	Dossier de la FTC nº 142 3019 Numéro de rôle C-4463	In the Matter of **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50	Dossier de la FTC nº 142 3020 Numéro de rôle C-4464	In the Matter of **BitTorrent, Inc.**	BitTorrent
51	Dossier de la FTC nº 142 3022 Numéro de rôle C-4465	In the Matter of **Charles River Laboratories, Int'l**	Charles River
52	Dossier de la FTC nº 142 3023 Numéro de rôle C-4466	In the Matter of **DataMotion, Inc.**	DataMotion
53	Dossier de la FTC nº 142 3024 Numéro de rôle C-4467	In the Matter of **DDC Laboratories, Inc.**, d/b/a DNA Diagnostics Center	DDC
54	Dossier de la FTC nº 142 3028 Numéro de rôle C-4470	In the Matter of **Level 3 Communications, LLC**	Level 3

55	Dossier de la FTC nº 142 3025 Numéro de rôle C-4468	In the Matter of **PDB Sports, Ltd.**, d/b/a the Denver Broncos Football Club, LLP	Broncos
56	Dossier de la FTC nº 142 3030 Numéro de rôle C-4471	In the Matter of **Reynolds Consumer Products, Inc.**	Reynolds
57	Dossier de la FTC nº 142 3031 Numéro de rôle C-4472	In the Matter of **Receivable Management Services Corporation**	Receivable Mgmt
58	Dossier de la FTC nº 142 3032 Numéro de rôle C-4473	In the Matter of **Tennessee Football, Inc.**	Tennessee Football
59	Dossier de la FTC nº 102 3058 Numéro de rôle C-4369	In the Matter of **Myspace LLC**	Myspace
60	Dossier de la FTC nº 092 3184 Numéro de rôle C-4365	In the Matter of **Facebook, Inc.**	Facebook
61	Dossier de la FTC nº 092 3081 Action civile nº 09-CV-5276 (C.D. Cal.)	FTC v. Javian Karnani, and **Balls of Kryptonite, LLC**, d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC	Balls of Kryptonite
62	Dossier de la FTC nº 102 3136 Numéro de rôle C-4336	In the Matter of **Google, Inc.**	Google
63	Dossier de la FTC nº 092 3137 Numéro de rôle C-4282	In the Matter of **World Innovators, Inc.**	World Innovators
64	Dossier de la FTC nº 092 3141 Numéro de rôle C-4271	In the Matter of **Progressive Gaitways LLC**	Progressive Gaitways
65	Dossier de la FTC nº 092 3139 Numéro de rôle C-4270	In the Matter of **Onyx Graphics, Inc.**	Onyx Graphics
66	Dossier de la FTC nº 092 3138 Numéro de rôle C-4269	In the Matter of **ExpatEdge Partners, LLC**	ExpatEdge
67	Dossier de la FTC nº 092 3140 Numéro de rôle C-4281	In the Matter of **Directors Desk LLC**	Directors Desk
68	Dossier de la FTC nº 092 3142 Numéro de rôle C-4272	In the Matter of **Collectify LLC**	Collectify

ANNEXE V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 juillet 2023

Monsieur Didier Reynders, membre de la Commission
Commission européenne
Rue de la Loi, 200
1049 Bruxelles
Belgique

Monsieur le Commissaire,

Le ministère américain des transports (ci-après le «ministère» ou le «DOT») est heureux d'avoir l'occasion de décrire son rôle dans la mise en œuvre du cadre de protection des données UE — États-Unis (ci-après le «CPD UE — États-Unis»). Le CPD UE — États-Unis jouera un rôle essentiel dans la protection des données à caractère personnel assurée lors de transactions commerciales dans un monde de plus en plus interconnecté. Il permettra aux entreprises de réaliser des transactions importantes au sein de l'économie mondiale tout en garantissant aux citoyens de l'Union des mesures de protection considérables de leur vie privée.

Le DOT a manifesté publiquement pour la première fois son engagement à appliquer le cadre que constituait la sphère de sécurité entre les États-Unis et l'Union européenne dans une lettre transmise à la Commission européenne il y a plus de 22 ans, un engagement qui a été réitéré et renforcé dans une lettre de 2016 concernant le cadre du bouclier de protection des données UE — États-Unis. Dans cette lettre, le DOT s'engageait à appliquer fermement les principes de la sphère de sécurité relatifs à la protection de la vie privée, puis les principes du bouclier de protection des données UE — États-Unis. Le DOT prolonge cet engagement en faveur des principes du CPD UE — États-Unis et la présente lettre consacre cet engagement.

Le DOT confirme notamment son engagement dans les domaines clés suivants: 1) la hiérarchisation des enquêtes sur les allégations de violations des principes du CPD UE — États-Unis; 2) la répression adéquate contre les entités effectuant des déclarations de certification au titre du CPD UE — États-Unis fausses ou frauduleuses; et 3) la surveillance des violations des principes du CPD UE — États-Unis et l'adoption d'ordonnances d'exécution à leur encontre. Nous fournissons des informations sur chacun de ces engagements et, dans les contextes pertinents, des informations utiles sur le rôle du DOT dans la protection de la vie privée des consommateurs et l'application des principes du CPD UE — États-Unis.

1. **Contexte**

A. Compétences du DOT en matière de protection de la vie privée

Le ministère a pris le ferme engagement de garantir le respect de la confidentialité des informations fournies par

les consommateurs aux compagnies aériennes et aux agents de billetterie. La prérogative du DOT de prendre des mesures dans ce domaine est établie au titre 49, section 41712, de l'U.S.C., qui interdit aux transporteurs et aux agents de billetterie «toute pratique déloyale ou frauduleuse ou tout acte de concurrence déloyale» relative au transport aérien ou à la vente de transport aérien. La section 41712 est

calquée sur la section 5 de la loi sur la commission fédérale du commerce (Federal Trade Commission, FTC) (15 U.S.C. 45). Récemment, le DOT a publié des règlements définissant les pratiques déloyales et frauduleuses, conformément aux précédents du DOT et de la FTC (tire 14 du CFR, article 399.79). Plus précisément, une pratique est «déloyale» si elle entraîne ou est .

susceptible d'entraîner un préjudice important que les consommateurs ne sont pas raisonnablement en mesure d'éviter ou qui n'est pas compensé par des avantages pour les consommateurs ou la concurrence. Une pratique est «frauduleuse» pour les consommateurs si elle est susceptible d'induire en erreur un consommateur agissant raisonnablement en fonction des circonstances, sur un aspect essentiel. Un aspect est essentiel s'il est susceptible d'avoir influé sur le comportement ou la décision du consommateur à l'égard d'un produit ou d'un service. Outre ces principes généraux, le DOT interprète spécifiquement la section 41712 comme interdisant aux transporteurs et aux agents de billetterie: 1) de violer les dispositions de sa politique de protection de la vie privée; 2) d'enfreindre les règles établies par le ministère déterminant les pratiques déloyales ou frauduleuses; 3) d'enfreindre la loi sur la protection de la vie privée des enfants en ligne (Children's Online Privacy Protection Act ou «COPPA») ou les règles de la FTC portant exécution de la COPPA; ou 4) de ne pas respecter, en tant que participant au CPD UE — États-Unis, les principes du CPD UE — États-Unis ([1])

Comme indiqué ci-dessus, en vertu du droit fédéral, le DOT est seul compétent pour réglementer les pratiques des compagnies aériennes relatives au respect de la vie privée et partage avec la FTC la compétence en ce qui concerne les pratiques, en matière de respect de la vie privée, des agents de billetterie d'avion dans le cadre de la vente de transport aérien.

Dès lors, lorsqu'un transporteur aérien ou un vendeur de transport aérien s'engage publiquement à respecter les principes du CPD UE — États-Unis, le ministère peut faire usage des pouvoirs qui lui sont conférés par la section 41712 pour assurer le respect de ces principes. Par conséquent, lorsqu'un passager communique des informations à un transporteur ou à un agent de billetterie qui s'est engagé à respecter les principes du CPD UE — États-Unis, tout manquement à cet engagement constituerait une violation de la section 41712.

B. Pratiques en matière de mise en application

Le bureau du ministère des transports pour la protection des consommateurs dans le domaine du transport aérien (Office of Aviation Consumer Protection, ci-après l'«OACP») ([2]) mène des enquêtes et engage des poursuites en vertu du titre 49, section 41712, de l'U.S.C. Il fait appliquer l'interdiction, établie à la section 41712, de pratiques déloyales et frauduleuses, principalement par la négociation, la préparation d'ordonnances de cessation et d'abstention, et l'élaboration d'ordonnances en vue de sanctions civiles. L'OACP prend essentiellement connaissance des violations potentielles grâce aux réclamations qu'il reçoit de personnes, d'agents de voyage, de compagnies aériennes et d'agences gouvernementales américaines et étrangères. Les consommateurs peuvent utiliser le site web du DOT pour introduire des réclamations en matière de respect de la vie privée contre les compagnies aériennes et les agents de billetterie ([3]).

Lorsqu'une transaction raisonnable et appropriée ne peut être conclue, l'OACP est habilité à entamer une procédure d'exécution impliquant une audition de témoins devant un juge de droit administratif relevant du DOT. Le juge de droit administratif est habilité à rendre des ordonnances de cessation et d'abstention et à infliger des sanctions civiles. Le non-respect des dispositions de la section 41712 peut entraîner l'émission d'ordonnances de cessation et d'abstention, et des sanctions de droit civil jusqu'à un montant de 37 377 USD pour chaque violation de la section 41712.

Le ministère n'est pas habilité à accorder des dommages-intérêts ou une réparation pécuniaire aux plaignants. Il est en revanche compétent pour approuver des transactions, conclues à la suite des enquêtes entamées par l'OACP, qui proposent un avantage direct aux consommateurs (par ex. sous forme de liquidités ou de bons d'achat) en échange des amendes payables dues au gouvernement américain. Cela s'est déjà produit dans le passé et pourrait également se produire dans le contexte des principes du CPD UE — États-Unis si les circonstances le justifient. Des infractions répétées à la section 41712 par une compagnie aérienne soulèveraient également des questions quant à la bonne volonté de celle-ci de respecter son engagement. Dans des situations extrêmes, on pourrait considérer qu'elle n'est plus apte à l'exploitation et, par conséquent, elle risquerait de perdre sa licence d'exploitation.

À ce jour, le DOT a reçu relativement peu de réclamations faisant état de violations de la vie privée par des agents de billetterie ou des compagnies aériennes. Lorsqu'il y a réclamation, celle-ci est examinée conformément aux principes susmentionnés.

C. Mesures de protection juridiques adoptées par le DOT bénéficiant aux consommateurs de l'Union

Au titre de la section 41712, l'interdiction des pratiques déloyales ou frauduleuses dans le domaine du transport aérien ou de la vente de transport aérien s'applique aux transporteurs aériens et agents de billetterie américains et étrangers. Le DOT poursuit régulièrement des compagnies aériennes américaines et étrangères pour des pratiques qui affectent des consommateurs tant étrangers et qu'américains, dès lors que ces pratiques sont intervenues dans le cadre de la fourniture de services de transport depuis ou vers les États-Unis. Le DOT utilise et continuera à utiliser tous les moyens à sa disposition pour protéger les consommateurs étrangers et américains contre les pratiques déloyales ou frauduleuses des entités réglementées dans le secteur du transport aérien.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy
([2]) Précédemment connu sous le nom de bureau pour l'application de la législation et les procédures en matière d'aéronautique.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints

En ce qui concerne les compagnies aériennes, le DOT assure aussi le respect d'autres lois ciblées dont la portée en matière de protection s'étend aux consommateurs non américains, comme la loi sur le respect de la vie privée des enfants en ligne (Children's Online Privacy Protection Act ou «COPPA»). Cette dernière exige notamment que les opérateurs de sites web et de services en ligne destinés aux enfants, ou des sites grand public qui collectent sciemment des informations à caractère personnel auprès d'enfants de moins de 13 ans, affichent un avertissement parental et obtiennent un consentement parental vérifiable. Les sites web et services basés aux États-Unis qui sont soumis à la COPPA et qui collectent des informations à caractère personnel auprès d'enfants étrangers sont tenus de respecter la COPPA. Les sites web et services en ligne basés à l'étranger doivent également respecter la COPPA s'ils ciblent les enfants américains ou s'ils collectent sciemment des informations à caractère personnel auprès d'enfants aux États-Unis. Le DOT est compétent pour prendre des mesures répressives à partir du moment où des compagnies aériennes américaines ou étrangères actives aux États-Unis enfreignent la COPPA.

II. **Application des principes du CPD UE — États-Unis**

Lorsqu'une compagnie aérienne ou un agent de billetterie décide de participer au CPD UE — États-Unis et que le ministère reçoit une réclamation alléguant une violation des principes du CPD UE — États-Unis, le ministère prend les mesures suivantes afin d'appliquer fermement les principes du CPD UE — États-Unis.

A. Hiérarchisation des enquêtes sur allégation de violations

L'OACP du ministère des transports enquête sur chaque allégation de violation des principes du CPD UE

États-Unis, y compris les réclamations émanant des autorités de protection des données (ci-après les «APD») de l'Union. Il prend des mesures répressives lorsqu'une violation est avérée. L'OACP coopère en outre avec la FTC et le ministère du commerce et donne la priorité aux allégations de manquement, par les entités réglementées, aux engagements pris en matière de respect de la vie privée dans le cadre du CPD UE — États-Unis.

Lorsqu'une allégation de violation des principes du CPD UE — États-Unis lui parvient, l'OACP peut prendre une série de mesures dans le cadre de son enquête. Il peut, par exemple, examiner la politique de l'agent de billetterie ou de la compagnie aérienne en matière de respect de la vie privée, exiger des informations complémentaires auprès de l'agent de billetterie ou de la compagnie ou de tiers, assurer un suivi auprès de l'entité ayant soumis la plainte et déterminer s'il existe un schéma de violations ou un nombre considérable de consommateurs affectés. Par ailleurs, il détermine si l'affaire comporte des aspects relevant du ministère du commerce ou de la FTC, étudie l'utilité d'une sensibilisation des consommateurs et des entreprises et, s'il y a lieu, entame une procédure d'exécution.

Si des violations potentielles des principes du CPD UE — États-Unis par des agents de billetterie sont portées à sa connaissance, il travaille sur le dossier en coordination avec la FTC. Nous informons également la FTC et le ministère du commerce des résultats de toute action de mise en application des principes du CPD UE — États-Unis.

B. Traitement des déclarations de participation fausses ou frauduleuses

Le ministère maintient son engagement à enquêter sur les violations des principes du CPD UE — États-Unis, y compris les déclarations fausses ou frauduleuses de participation au CPD UE — États-Unis. Nous examinerons en priorité les dossiers soumis par le ministère du commerce concernant les organisations qui, selon lui, affirment indûment participer au CPD UE — États-Unis ou utilisent sans autorisation la marque de certification du CPD UE — États-Unis.

Signalons également que, lorsqu'une organisation affirme, dans sa politique en matière de protection de la vie privée, respecter les principes du CPD UE — États-Unis, le fait qu'elle n'ait pas, ou n'ait plus, autocertifié son adhésion aux principes auprès du ministère du commerce ne suffit pas à empêcher le DOT d'exiger qu'elle respecte ces engagements.

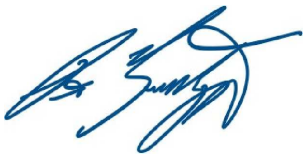
C. Surveillance et délivrance d'ordonnances de mise en œuvre par la sphère publique relatives à des violations du CPD UE — États-Unis

L'OACP du ministère des transports maintient également son engagement à contrôler les ordonnances d'exécution selon les besoins, afin d'assurer le respect des principes du CPD UE — États-Unis. Plus précisément, lorsqu'il délivre une ordonnance exigeant qu'une compagnie aérienne ou un agent de billetterie mette fin ou renonce à des violations des principes du CPD UE — États-Unis et de la section 41712, il contrôle le respect, par l'entité, de la clause de cessation et d'abstention incluse dans l'ordonnance. L'OACP veille en outre à ce que les ordonnances découlant d'affaires pourtant sur les principes du CPD UE — États-Unis soient publiées sur son site web.

Nous nous réjouissons à l'idée de poursuivre notre collaboration avec nos partenaires fédéraux et avec les acteurs de l'Union sur les questions ayant trait au CPD UE — États-Unis.

J'espère que ces informations vous seront utiles et me tiens à votre disposition pour tout renseignement complémentaire.

Je vous prie, Monsieur le Commissaire, d'agréer
l'expression de ma haute considération.



Pete Buttigieg

ANNEXE VI

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General Washington, D.C. 20530

23 juin 2023

M[me] Ana Gallego Torres
Directrice générale de la justice et des consommateurs
Commission européenne
Rue Montoyer 59
1049 Bruxelles
Belgique

Madame,

La présente lettre vous propose 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 ([1]). Toutes les procédures légales décrites dans la présente lettre sont de nature non discriminatoire dans la mesure où elles servent à obtenir des informations auprès de sociétés aux États-Unis, y compris des sociétés qui autocertifieront leur adhésion au cadre de protection des données UE — États-Unis, sans distinction de nationalité ou de lieu de résidence de la personne concernée. En outre, les sociétés qui font l'objet d'une procédure légale aux États-Unis peuvent contester celle-ci devant une juridiction, comme indiqué ci-dessous ([2]).

Le quatrième amendement de la Constitution des États-Unis, particulièrement important en ce qui concerne la saisie de données par des autorités publiques, dispose que «[l]e droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration solennelle, ni sans qu'il décrive avec précision le lieu à fouiller et les personnes ou les choses à saisir». Amendement IV de la Constitution américaine. Comme l'a jugé la Cour suprême des États-Unis dans l'arrêt Berger v. State of New York, «[l]a finalité première [de cet] amendement, telle que reconnue dans de nombreuses décisions de la Cour, est de protéger la vie privée et la sécurité des individus contre les intrusions arbitraires des responsables du gouvernement». 388 U.S. 41, 53 (1967) [citant Camara v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)]. Dans les enquêtes pénales nationales, le quatrième amendement exige généralement des responsables de l'application de la loi qu'ils obtiennent un mandat délivré par un tribunal avant de mener une perquisition. Voir Katz v. United States, 389 U.S. 347, 357 (1967). Les normes relatives à la délivrance d'un mandat, telles que les exigences en matière de motif sérieux et de particularité, s'appliquent aux mandats de perquisition et de saisie

([1]) Le présent aperçu ne décrit pas les outils d'enquête utilisés aux fins de la sécurité nationale par les professionnels de l'application de la loi dans les enquêtes antiterroristes et autres enquêtes de sécurité nationale, notamment les lettres de sécurité nationale envoyées pour obtenir certaines informations figurant dans des rapports de solvabilité, des états financiers et des documents de transactions et d'abonnements électroniques (voir 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709; 50 U.S.C. § 3162) et pour la surveillance électronique, les mandats de perquisition, les dossiers commerciaux et d'autres collectes d'informations au titre de la loi sur la surveillance du renseignement étranger (Foreign Intelligence Surveillance Act) (voir 50 U.S.C. § 1801 et suivants).

([2]) La présente lettre a pour objet les pouvoirs réglementaires et répressifs octroyés au titre du droit fédéral; les violations du droit des États sont examinées par les autorités répressives des États concernés et poursuivies devant les juridictions d'État. Les autorités répressives des États font un usage des mandats de perquisition et des injonctions délivrés au titre du droit des États sensiblement identique à ce qui est décrit dans le présent document, à la différence que les traitements légaux relevant du droit des États peuvent être soumis à des protections supplémentaires au titre de la constitution ou des lois d'un État plus rigoureuses que celles prévues par la Constitution américaine. Les protections octroyées par le droit des États doivent être au moins égales à celles découlant de la Constitution américaine, notamment – mais non exclusivement – de son quatrième amendement.

physiques ainsi qu'aux mandats relatifs au contenu enregistré de communications électroniques délivrés en vertu de la loi sur les communications enregistrées (Stored Communications Act) comme nous le verrons plus loin. Lorsque l'obligation de mandat n'est pas applicable, le quatrième amendement soumet toujours les activités du gouvernement à un critère de «caractère raisonnable». La Constitution elle-même garantit donc que le gouvernement américain n'a pas le pouvoir illimité ou arbitraire de saisir des informations privées ([3]).

Autorités répressives en matière pénale:

Les procureurs fédéraux, qui sont des fonctionnaires du ministère de la justice (Department of Justice ou «DOJ»), et les enquêteurs fédéraux, y compris les agents du Federal Bureau of Investigation («FBI»), un organe répressif relevant du DOJ, peuvent exiger la production de documents et d'autres informations auprès de sociétés aux États-Unis aux fins d'une enquête pénale en utilisant plusieurs types de procédures juridiques contraignantes, au nombre desquelles les citations à comparaître devant un grand jury («grand jury subpoenas»), les injonctions administratives et les mandats de perquisition, et peuvent également obtenir d'autres communications grâce aux pouvoirs fédéraux relatifs aux écoutes téléphoniques et aux enregistreurs graphiques.

Citations à comparaître devant un grand jury: celles-ci sont utilisées dans le cadre d'enquêtes d'application de la loi ciblées. Une citation à comparaître devant un grand jury est une demande officielle émanant d'un grand jury (généralement à la demande d'un procureur fédéral) pour les besoins d'une enquête judiciaire sur une suspicion de violation du droit pénal. Le grand jury est l'organe d'enquête de la cour. Il est présidé par un juge ou un magistrat. L'injonction peut contraindre une personne à témoigner dans le cadre d'une procédure ou à produire ou mettre à disposition des autorités les documents professionnels, informations électroniques ou autres éléments tangibles en sa possession. Les informations doivent être pertinentes pour l'enquête et l'injonction doit rester raisonnable, c'est-à-dire qu'elle ne peut être trop large, trop lourde ou trop oppressive. Le destinataire peut invoquer ces motifs pour contester une injonction. Voir Fed. R. Crim. P. 17. Dans de rares circonstances, les injonctions à produire des documents peuvent être utilisées après la mise en accusation par le grand jury.

Injonctions administratives: les pouvoirs d'injonction administrative peuvent être exercés dans le cadre d'enquêtes pénales ou civiles. Dans le contexte de l'application du droit pénal, plusieurs actes législatifs fédéraux autorisent l'utilisation d'injonctions administratives pour obtenir la production ou la mise à disposition de documents professionnels, d'informations électroniques ou d'autres éléments tangibles pertinents dans le cadre d'enquêtes sur des fraudes à l'assurance maladie, des abus d'enfants, la protection des services secrets, des abus de substances illégales et des enquêtes de l'inspecteur général impliquant des agences gouvernementales. Si les pouvoirs publics demandent l'exécution d'une injonction administrative à une juridiction, le destinataire de l'injonction peut, comme pour une injonction à comparaître, faire valoir que l'injonction présente un caractère déraisonnable car elle est trop large, oppressive ou lourde.

Ordonnances judiciaires relatives aux enregistreurs graphiques et aux dispositifs de traçage: au titre des dispositions relatives à l'utilisation d'enregistreurs graphiques et de dispositifs de traçage en matière pénale, les autorités répressives peuvent obtenir une ordonnance judiciaire afin d'accéder à des informations génériques de composition de numéro de téléphone, de routage, d'adressage et de signalisation, ne portant pas sur le contenu et en temps réel, sur un numéro de téléphone ou une adresse de courrier électronique, à condition de certifier que les informations à fournir sont en rapport avec une enquête pénale en cours. Voir 18 U.S.C. §§ 3121 à 3127. L'utilisation ou l'installation d'un tel dispositif en dehors du cadre prévu par la loi constitue une violation du droit fédéral.

Loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act ou «ECPA»): d'autres règles régissent l'accès des pouvoirs publics aux informations d'abonnement, données de trafic et contenus de communications enregistrés par des fournisseurs de service internet (également appelés «FSI»), des compagnies de téléphone et d'autres fournisseurs de services tiers, conformément au titre II de l'ECPA, également appelée loi sur les communications enregistrées (Stored Communications Act ou «SCA») (18 U.S.C. §§ 2701 à 2712). La SCA établit un système de droits au respect de la vie privée empêchant les autorités répressives d'accéder aux données des clients et abonnés des FSI au-delà de ce qui est prévu par le droit constitutionnel. La SCA prévoit des niveaux accrus de protection de la vie privée en fonction du caractère intrusif de la collecte. Pour les informations relatives à l'enregistrement des abonnés,

([3]) En ce qui concerne les principes du quatrième amendement relatifs à la protection de la vie privée et des intérêts en matière de sécurité qui sont examinés ci-dessus, les juridictions américaines appliquent régulièrement ces principes aux nouveaux types d'outils d'enquête des services répressifs qui sont rendus possibles par l'évolution de la technologie. En 2018, par exemple, la Cour suprême a statué que l'acquisition par le gouvernement, dans le cadre d'une enquête policière, de données rétrospectives sur la localisation des sites cellulaires auprès d'une société de téléphonie mobile pendant une période prolongée constituait une «perquisition» soumise à l'obligation d'obtenir un mandat en vertu du quatrième amendement. Carpenter v. United States, 138 S. Ct. 2206 (2018).

les adresses IP et les données temporelles y afférentes, ainsi que les informations de facturation, les autorités répressives doivent obtenir une injonction. Pour la plupart des autres informations enregistrées ne portant pas sur le contenu, telles que les intitulés de courriers électroniques sans indication d'objet, elles doivent présenter des faits spécifiques à un juge afin de démontrer que les informations demandées sont pertinentes et nécessaires pour une enquête pénale en cours. Afin d'accéder au contenu enregistré de communications électroniques, les autorités répressives doivent, en règle générale, obtenir auprès d'un juge un mandat fondé sur un motif sérieux de croire que le compte en question contient des preuves d'une infraction grave. La SCA prévoit également des sanctions de responsabilité civile ainsi que des sanctions pénales ([4]).

Ordonnances judiciaires de surveillance conformément à la loi fédérale relative aux écoutes téléphoniques: les autorités répressives peuvent également intercepter en temps réel les communications filaires, orales ou électroniques pour les besoins d'une enquête pénale conformément à la loi fédérale relative aux écoutes téléphoniques. Voir 18 U.S.C. §§ 2510 à 2523. Ce pouvoir est soumis à l'octroi d'une ordonnance judiciaire par un juge estimant notamment qu'il existe un motif sérieux de croire que la mise sur écoute ou l'interception électronique permettra d'obtenir des preuves d'une infraction grave au droit fédéral ou des renseignements sur la localisation d'un fugitif cherchant à échapper à des poursuites. La législation prévoit des sanctions pénales et en responsabilité civile en cas de violation des dispositions relatives aux écoutes téléphoniques.

Mandat de perquisition – Fed. R. Crim. P. Règle 41: les autorités répressives peuvent procéder à des fouilles physiques de locaux aux États-Unis sur autorisation du juge. Elles doivent pour cela démontrer au juge qu'il existe un motif sérieux de penser qu'une infraction grave a été ou va être commise et que des éléments en rapport avec cette infraction pourraient se trouver à l'endroit spécifié dans le mandat. Ce pouvoir est souvent utilisé lorsque la fouille physique d'un local par la police est nécessaire compte tenu du risque que la société ne détruise les preuves si elle reçoit une injonction ou une autre ordonnance de production d'informations. 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. Voir Mapp v. Ohio, 367 U.S. 643 (1961). Lorsqu'un détenteur de données est tenu de divulguer des données en vertu d'un mandat, la partie obligée peut notamment contester l'obligation de divulgation au motif qu'elle est indûment contraignante. Voir In re Application of United States, 610 F.2d 1148, 1157 (3d Cir. 1979) (estimant que «la procédure régulière exige une audition sur la question de la lourdeur avant d'obliger une compagnie de téléphone à fournir» une assistance pour un mandat de perquisition); In re Application of United States, 616 F.2d 1122 (9th Cir. 1980) (parvenant à la même conclusion sur la base de l'autorité de contrôle du tribunal).

Lignes directrices et politiques du DOJ: outre ces limitations constitutionnelles, législatives et réglementaires de l'accès des pouvoirs publics aux données, le procureur général a également publié des lignes directrices limitant davantage l'accès des autorités répressives aux données, qui contiennent également des protections concernant la vie privée et les libertés civiles. Par exemple, les lignes directrices du procureur général destinées aux activités intérieures du FBI (septembre 2008) (Attorney General's Guidelines for Domestic Federal Bureau of Investigation Operations, ci-après les «AG FBI Guidelines»), disponibles à l'adresse http://www.justice.gov/archive/opa/docs/guidelines.pdf, limitent l'utilisation de moyens d'enquête pour l'obtention d'informations relatives à des enquêtes sur des infractions fédérales graves. Ces lignes directrices exigent du FBI qu'il utilise les méthodes d'enquête les moins intrusives possible, en tenant compte de leur incidence sur la vie privée et les libertés civiles et du préjudice potentiel à la réputation des personnes concernées. Elles indiquent par ailleurs que «le FBI doit de toute évidence effectuer ses enquêtes et autres activités d'une manière licite et raisonnable, qui respecte la liberté et la vie privée et évite toute intrusion inutile dans la vie des personnes respectueuses de la loi». Voir AG FBI Guidelines, p. 5. Le FBI a mis en œuvre ces lignes directrices au moyen du guide sur les enquêtes et activités intérieures du FBI (Domestic Investigations and Operations Guide, DIOG), disponible à l'adresse https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29. Il s'agit d'un manuel complet qui inclut des limitations détaillées de l'utilisation des outils d'enquête, ainsi que des orientations visant à garantir la protection des libertés civiles et de la vie privée dans toutes les enquêtes. D'autres règles et politiques limitant les activités d'enquête des procureurs fédéraux sont incluses dans le manuel de la justice, également disponible en ligne à l'adresse https://www.justice.gov/jm/justice-manual.

Compétences civiles et réglementaires (intérêt public):

([4]) En outre, la section 2705(b) de la SCA autorise le gouvernement à obtenir une ordonnance du tribunal, sur la base d'un besoin démontré de protection contre la divulgation, interdisant à un fournisseur de services de communications d'informer volontairement ses utilisateurs de la réception d'une procédure judiciaire de la SCA. En octobre 2017, le procureur général adjoint Rod Rosenstein a publié un mémorandum à l'intention des avocats et des agents du ministère de la justice, énonçant des orientations visant à garantir que les demandes de telles ordonnances de protection soient adaptées aux faits et préoccupations spécifiques d'une enquête et fixant une limite maximale d'un an à la durée pendant laquelle une demande peut chercher à retarder la notification. En mai 2022, la procureure générale adjointe Lisa Monaco a publié des orientations supplémentaires sur le sujet qui, entre autres, établissent des exigences d'agrément interne du ministère de la justice pour les demandes de prorogation d'une ordonnance de protection au-delà de la période initiale d'un an et exigent la résiliation des ordonnances de protection à la fin d'une enquête.

Il existe également des limitations importantes d'ordre civil ou réglementaire (autrement dit d'«intérêt public») à l'accès aux données détenues par des sociétés aux États-Unis. Les agences investies de responsabilités civiles et réglementaires peuvent adresser des injonctions aux sociétés afin d'accéder à des documents professionnels, à des informations électroniques ou à d'autres éléments tangibles. L'exercice, par ces agences, de leurs pouvoirs d'injonction administrative ou civile est limité non seulement par leur statut interne, mais aussi par un contrôle judiciaire indépendant des injonctions préalable à leur éventuelle application judiciaire. Voir, par exemple, Fed. R. Civ. P. 45. Les agences ne peuvent demander l'accès qu'aux données concernées par les domaines relevant de leur compétence. Par ailleurs, le destinataire d'une injonction administrative peut contester l'exécution de celle-ci devant un tribunal en démontrant que l'agence n'a pas respecté le principe fondamental du caractère raisonnable présenté ci-dessus.

Il existe d'autres bases juridiques permettant aux sociétés de contester des demandes de données émanant d'agences administratives, en fonction de leur secteur d'activité et du type de données en leur possession. Par exemple, les institutions financières peuvent contester les injonctions administratives réclamant certains types d'informations au motif d'une violation de la loi sur le secret bancaire et de ses modalités d'exécution. Voir 31 U.S.C. § 5318; 31 C.F.R. chapitre X. Les autres sociétés peuvent invoquer le FAIR Credit Reporting Act (voir 15 U.S.C, § 1681b) ou d'autres dispositions législatives sectorielles. L'utilisation abusive par une agence de son pouvoir d'injonction peut entraîner la responsabilité de l'agence ou la responsabilité personnelle de ses employés. Voir, par exemple, loi sur le droit à la confidentialité financière (Right to Financial Privacy Act), 12 U.S.C. §§ 3401 à 3423. Les tribunaux des États-Unis servent donc de remparts aux demandes réglementaires abusives et assurent une surveillance indépendante des activités des agences fédérales.

Enfin, tout pouvoir accordé par la loi aux autorités administratives pour saisir physiquement des documents d'une société aux États-Unis en vertu d'un mandat de perquisition doit respecter les exigences fondées sur le quatrième amendement. Voir See v. City of Seattle, 387 U.S. 541 (1967).

Conclusion:

Toutes les activités réglementaires et répressives effectuées aux États-Unis doivent respecter le droit applicable, y compris la Constitution américaine, les actes législatifs, les règles et les règlements. Ces activités doivent également se conformer aux politiques applicables, notamment les lignes directrices du procureur général régissant les activités répressives des autorités fédérales. Le cadre juridique décrit ci-dessus limite la capacité des agences répressives et réglementaires américaines d'obtenir des informations de la part de sociétés aux États-Unis – qu'elles concernent des ressortissants américains ou des ressortissants de pays tiers – tout en permettant le contrôle judiciaire de toute demande de données adressée par les pouvoirs publics en vertu de ces compétences.

Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANNEXE VII

BUREAU DU DIRECTEUR DES AFFAIRES JURIDIQUES AUPRÈS DU BUREAU DU DIRECTEUR DU RENSEIGNEMENT NATIONAL

WASHINGTON, DC 20511

9 décembre 2022

Leslie B.
Kiernan, Directrice des affaires juridiques
Ministère du
commerce des États-Unis, 1401 Constitution
Ave., NW Washington, DC 20230

Madame,

Le 7 octobre 2022, le président Biden a signé le décret présidentiel 14086 intitulé «Enhancing Safeguards for United States Signals Intelligence Activities», qui renforce le solide faisceau de garanties en matière de protection de la vie privée et des libertés civiles qui s'applique aux activités de renseignement d'origine électromagnétique des États-Unis. Ces garanties sont notamment les suivantes: exiger que les activités de renseignement d'origine électromagnétique répondent à des objectifs légitimes énumérés; interdire de manière explicite ces activités dans le but d'atteindre des objectifs spécifiques interdits; mettre en place de nouvelles procédures pour garantir que les activités de renseignement d'origine électromagnétique servent ces objectifs légitimes et ne servent pas des objectifs interdits; exiger que les activités de renseignement d'origine électromagnétique ne soient menées qu'après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, que ces activités sont nécessaires pour faire progresser une priorité validée en matière de renseignement, et uniquement dans une mesure et d'une manière proportionnées à la priorité validée en matière de renseignement pour laquelle elles ont été autorisées; et demander aux composantes de la communauté du renseignement de mettre à jour leurs politiques et procédures afin de tenir compte des garanties imposées par le décret présidentiel en matière de renseignement d'origine électromagnétique. Plus important encore, le décret présidentiel met également en place un mécanisme indépendant et contraignant permettant aux particuliers des «États admissibles», désignés conformément au décret, de demander réparation s'ils estiment avoir fait l'objet d'activités illégales de renseignement d'origine électromagnétique aux États-Unis, notamment d'activités violant les protections prévues par le décret.

La publication du décret présidentiel 14086 par le président Biden marque l'aboutissement de plus d'un an de négociations pointues entre les représentants de la Commission européenne et des États-Unis et indique les mesures que les États-Unis prendront pour mettre en œuvre leurs engagements en vertu du cadre de protection des données UE — États-Unis. Conformément à l'esprit de coopération qui a présidé à l'élaboration du cadre, je crois comprendre que vous avez reçu deux séries de questions de la part de la Commission sur la manière dont la communauté du renseignement mettra en œuvre le décret. J'ai le plaisir de répondre à ces questions par la présente lettre.

Article 702 de la loi sur la surveillance et le renseignement extérieur de 1978 (article 702 du FISA)

La première série de questions concerne l'article 702 du FISA, qui autorise la collecte d'informations de renseignement extérieur via le ciblage de personnes non américaines dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis, avec l'assistance obligatoire des fournisseurs de services de communications électroniques. Plus précisément, les questions portent sur l'interaction entre cette disposition et le décret présidentiel 14086, ainsi que sur les autres garanties qui s'appliquent aux activités menées en vertu de l'article 702 du FISA.

Pour commencer, nous pouvons confirmer que la communauté du renseignement appliquera les garanties énoncées dans le décret présidentiel 14086 aux activités menées en vertu de l'article 702 du FISA.

En outre, de nombreuses autres garanties s'appliquent à l'utilisation par le gouvernement de l'article 702 du FISA. Toutes les certifications de l'article 702 du FISA doivent, par exemple, être signées par le procureur général et le directeur du renseignement national, et le gouvernement doit soumettre toutes ces certifications à l'approbation du tribunal de surveillance du renseignement extérieur (Foreign Intelligence Surveillance Court ou «FISC»), qui est composé de juges indépendants, nommés à vie et dont le mandat est de sept ans non renouvelable. Les certifications définissent les catégories d'informations de renseignement extérieur à collecter, qui doivent répondre à la définition légale des informations de renseignement extérieur, en ciblant des personnes non américaines dont il est raisonnable de penser qu'elles se trouvent en dehors des États-Unis. Les certifications ont inclus des informations concernant le terrorisme international et d'autres sujets, tels que l'acquisition d'informations sur les armes de destruction massive. Chaque certification annuelle doit être soumise à l'approbation du FISC dans un dossier de demande de certification comprenant les certifications du procureur général et du directeur du renseignement national, les déclarations sous serment de certains chefs d'agences de renseignement, ainsi que les procédures de ciblage, de minimisation et d'interrogation qui sont contraignantes pour le gouvernement. Les procédures de ciblage exigent, entre autres, que la communauté du renseignement évalue raisonnablement, sur la base de l'ensemble des circonstances, que le ciblage est susceptible de donner lieu à la collecte d'informations de renseignement extérieur indiquées dans une certification au titre de l'article 702 du FISA.

En outre, lorsqu'elle collecte des informations en vertu de l'article 702 du FISA, la communauté du renseignement doit: expliquer par écrit la base sur laquelle elle a évalué, au moment du ciblage, que la cible est susceptible de détenir, de recevoir ou de communiquer des informations de renseignement extérieur indiquées dans une certification au titre de l'article 702 du FISA; confirmer que le critère de ciblage défini dans les procédures de ciblage de l'article 702 du FISA est toujours respecté; et cesser la collecte si le critère n'est plus respecté. *Voir* observations du gouvernement américain au tribunal de surveillance du renseignement extérieur, *2015 Summary of Notable Section 702 Requirements*, aux pages 2 et 3 (15 juillet 2015).

Le fait d'exiger que la communauté du renseignement consigne par écrit et confirme régulièrement la validité de son évaluation selon laquelle les cibles de l'article 702 du FISA répondent aux normes de ciblage applicables facilite la supervision par le FISC des activités de ciblage de la communauté du renseignement. L'enregistrement de chaque évaluation et justification de ciblage est vérifié tous les deux mois par les avocats du ministère de la justice (Department of Justice ou «DOJ») chargés du contrôle des renseignements, qui exercent cette fonction de contrôle indépendamment des opérations de renseignement extérieur. Le département du DOJ chargé de cette fonction est alors responsable, en vertu d'une règle établie de longue date par le FISC, de lui signaler toute violation des procédures applicables. Cette obligation de rapport, ainsi que les réunions régulières entre le FISC et ce département du DOJ concernant le contrôle du ciblage au titre de l'article 702 du FISA, permettent au FISC de faire respecter les procédures de ciblage et autres de l'article 702 du FISA et de garantir que les activités du gouvernement sont conformes à la loi. Plus précisément, le FISC peut le faire de plusieurs manières, notamment en rendant des décisions correctives contraignantes pour mettre fin au pouvoir du gouvernement de collecter des données contre une cible particulière, ou pour modifier ou retarder la collecte de données en vertu de l'article 702 du FISA. Le FISC peut également demander au gouvernement de fournir des rapports ou des informations supplémentaires sur le respect des procédures de ciblage et autres, ou exiger des modifications de ces procédures.

La collecte «en vrac» de renseignement d'origine électromagnétique

La deuxième série de questions concerne la collecte «en vrac» de renseignement d'origine électromagnétique, définie par le décret présidentiel 14086 comme étant «la collecte autorisée de grandes quantités de données de renseignement d'origine électromagnétique qui, en raison de considérations techniques ou opérationnelles, sont acquises sans l'utilisation de discriminants (par exemple, sans l'utilisation d'indicatifs spécifiques ou de critères de sélection)».

En ce qui concerne ces questions, nous tenons tout d'abord à souligner que ni le FISA ni les lettres de sécurité nationale n'autorisent la collecte en vrac. Pour ce qui est du FISA:

— les titres I et III du FISA, qui autorisent respectivement la surveillance électronique et les fouilles corporelles, nécessitent une ordonnance judiciaire (sauf exceptions limitées, comme en cas d'urgence) et, dans tous les cas, un motif raisonnable de croire que la cible est une puissance étrangère ou un agent d'une puissance étrangère. *Voir* 50 U.S.C. §§ 1805, 1824.

— Le USA FREEDOM Act de 2015 a modifié le titre IV du FISA, qui autorise l'utilisation d'enregistreurs graphiques et de dispositifs de traçage, en vertu d'une ordonnance judiciaire (sauf en cas d'urgence), afin d'obliger le gouvernement à fonder ses demandes sur un «critère de sélection spécifique». *Voir* 50 U.S.C. § 1842(c)(3).

— Le titre V du FISA, qui permet au Federal Bureau of Investigation (FBI) d'obtenir certains types de documents commerciaux, requiert une ordonnance du tribunal sur la base d'une demande précisant «qu'il existe des faits spécifiques et clairs donnant des raisons de croire que la personne à laquelle les données se rapportent est une puissance étrangère ou un agent d'une puissance étrangère». *Voir* 50 U.S.C. § 1862(b)(2)(B) ([1]).

— Enfin, l'article 702 du FISA permet le «ciblage de personnes dont il est raisonnable de penser qu'elles se trouvent hors des États-Unis pour se procurer des informations de renseignement extérieur». *Voir* 50 U.S.C. § 188la(a). Ainsi, comme l'a noté le Conseil de surveillance de la vie privée et des libertés civiles, la collecte de données par le gouvernement au titre de l'article 702 du FISA «consiste exclusivement dans le fait de cibler des personnes et de se procurer des communications liées à ces personnes, dont le gouvernement a des raisons de penser qu'il obtiendra certains types de renseignements étrangers», de sorte que le «programme ne fonctionne pas en collectant des communications en vrac». Conseil de surveillance de la vie privée et des libertés civiles, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, p. 103 (2 juillet 2014) ([2]).

En ce qui concerne les lettres de sécurité nationale, le USA FREEDOM Act de 2015 impose un «critère de sélection spécifique» pour l'utilisation de ces lettres. *Voir* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

En outre, le décret présidentiel 14086 prévoit qu'«il convient de donner la priorité à une collecte ciblée» et que, lorsque la communauté du renseignement procède à une collecte en vrac, «la collecte en vrac de renseignements d'origine électromagnétique ne doit être autorisée que s'il est déterminé […] que les informations nécessaires pour faire progresser une priorité validée en matière de renseignement ne peuvent raisonnablement pas être obtenues par une collecte ciblée». *Voir* décret présidentiel 14086, § 2(c)(ii)(A).

En outre, lorsque la communauté du renseignement détermine que la collecte en vrac répond à ces normes, le décret présidentiel 14086 prévoit des garanties supplémentaires. Plus précisément, le décret exige que la communauté du renseignement, lorsqu'elle procède à une collecte en vrac, «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». *Voir ibidem*. Le décret précise également que les «activités de renseignement d'origine électromagnétique», qui comprennent l'interrogation de renseignements d'origine électromagnétique obtenus par une collecte en vrac, «ne sont menées qu'après avoir déterminé, sur la base d'une évaluation raisonnable de tous les facteurs pertinents, que ces activités sont nécessaires pour faire progresser une priorité validée en matière de renseignement». *Voir ibidem* § 2(a)(ii)(A). Le décret met en œuvre ce principe en indiquant que la communauté du renseignement ne peut interroger que les renseignements d'origine électromagnétique non réduits au minimum obtenus en vrac dans le cadre de six objectifs autorisés, et que ces interrogations doivent être effectuées conformément à des politiques et procédures qui «tiennent dûment compte de l'incidence [des interrogations] sur la vie privée et les libertés civiles de toutes les personnes, indépendamment de leur nationalité ou de leur lieu de résidence». *Voir ibidem* § 2(c)(iii)(D). Enfin, le décret prévoit des contrôles du traitement et de la sécurité des données collectées ainsi que de l'accès à celles-ci. *Voir ibidem* § 2(c)(iii)(A) et § 2(c)(iii)(B).

Nous espérons que ces éclaircissements vous seront utiles. Nous restons à votre disposition pour toute question supplémentaire sur la manière dont la communauté du renseignement des États-Unis prévoit de mettre en œuvre le décret présidentiel 14086.

Je vous prie, Madame, d'agréer l'expression de ma haute considération

([1]) De 2001 à 2020, le titre V du FISA permettait au FBI de demander l'autorisation au FISC de recueillir des «objets tangibles» pertinents pour certaines enquêtes autorisées. *Voir* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). Cette disposition, qui a été supprimée et n'a donc plus force de loi, a permis au gouvernement de collecter à un moment donné des métadonnées téléphoniques en vrac. Toutefois, avant même que cette disposition ne devienne caduque, le USA FREEDOM Act l'avait modifiée pour obliger le gouvernement à fonder une demande auprès du FISC sur un «critère de sélection spécifique». *Voir* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

([2]) Les articles 703 et 704, qui autorisent la communauté du renseignement à cibler des personnes américaines situées à l'étranger, requièrent une ordonnance judiciaire (sauf en cas d'urgence) et exigent, dans tous les cas, un motif raisonnable de croire que la cible est une puissance étrangère, un agent d'une puissance étrangère ou un fonctionnaire ou employé d'une puissance étrangère. *See* 50 U.S.C. §§ 1881b, 1881c.

Sincerely,

Christopher C. FONZONE,
directeur des affaires juridiques

ANNEXE VIII

Liste des abréviations

Les abréviations suivantes figurent dans la présente décision:

AAA	American Arbitration Association
AGG-DOM	Attorney General Guidelines for Domestic FBI Operations (Lignes directrices du procureur général pour les opérations intérieures du FBI)
APA	Administrative Procedure Act (Loi sur la procédure administrative)
APD	Autorité chargée de la protection des données
CIA	Central Intelligence Agency (Agence centrale de renseignements)
CNSS	Committee on National Security Systems (Comité des systèmes de sécurité nationaux)
Cour de justice	Cour de justice de l'Union européenne
CPD UE - États-Unis ou CPD	Cadre de protection des données UE - États-Unis
Décision	Décision d'exécution de la Commission constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE - États-Unis
DNI	Director of National Intelligence (Directeur du renseignement national)
DPRC	Data Protection Review Court (Cour de contrôle de la protection des données)
ECOA	Equal Credit Opportunity Act (Loi sur l'égalité des chances en matière de crédit)
ECPA	Electronic Communications Privacy Act (Loi sur la confidentialité des communications électroniques)
EEE	Espace économique européen
EO 14086	Décret présidentiel n° 14086 sur le renforcement des garanties pour les activités de renseignement d'origine électromagnétique menées par les États-Unis
EO 12333	Décret présidentiel n° 12333 sur les activités de renseignement des États-Unis
FBI	Federal Bureau of Investigation (Bureau fédéral d'enquête)
FCRA	Fair Credit Reporting Act (Loi sur la publication d'informations en matière de crédit équitable)
FISA	Foreign Intelligence Surveillance Act (Loi sur la surveillance du renseignement étranger)
FISC	(Foreign Intelligence Surveillance Court (Cour de surveillance du renseignement étranger)
FISCR	Foreign Intelligence Surveillance Court of Review (Cour de contrôle de la surveillance du renseignement étranger)
FOIA	Freedom of Information Act (Loi sur la liberté d'information)
FRA	Federal Records Act (Loi fédérale sur les registres)
FTC	U.S. Federal Trade Commission (Commission fédérale américaine du commerce)
HIPAA	Health Insurance Portability and Accountability Act (Loi sur la portabilité et la responsabilité de l'assurance maladie)
ICDR	International Centre for Dispute Resolution
IOB	Intelligence Oversight Board (Comité de surveillance du renseignement)
Les principes	Les principes du cadre de protection des données UE - États-Unis
Liste du CPD	Liste du cadre de protection des données UE - États-Unis
NIST	National Institute of Standards and Technology (Institut national des normes et des technologies)

NSA	National Security Agency (Agence nationale de sécurité)
NSL	National Security Letter(s) (Lettre(s) nationale(s) de sécurité)
ODNI	Office of the Director of National Intelligence (Bureau du directeur du renseignement national)
ODNI CLPO, CLPO	Civil Liberties Protection Officer of the Director of National Intelligence (Responsable de la protection des libertés civiles du directeur du renseignement national)
OMB	Office of Management and Budget (Bureau de la gestion et du budget des États-Unis)
OPCL	Office of Privacy and Civil Liberties of the Department of Justice (Bureau chargé de la protection de la vie privée et des libertés civiles du ministère de la justice)
Panel du CPD UE - États-Unis	Panel du cadre de protection des données UE - États-Unis
PCLOB	Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles)
PIAB	President's Intelligence Advisory Board (Conseil consultatif du renseignement du président)
PPD 28	Presidential Policy Directive 28 (Directive présidentielle n° 28)
Règlement (UE) 2016/679	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 AG	Règlement du procureur général relatif à la Cour de contrôle de la protection des données
Union	Union européenne