II

(Actes non législatifs)

DÉCISIONS

DÉCISION D'EXÉCUTION (UE) 2016/1250 DE LA COMMISSION

du 12 juillet 2016

conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis

[notifiée sous le numéro C(2016) 4176]

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

LA COMMISSION EUROPÉENNE,

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

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ([1]), et notamment son article 25, paragraphe 6,

après consultation du Contrôleur européen de la protection des données ([2]),

1. INTRODUCTION

(1) La directive 95/46/CE fixe les règles applicables au transfert de données à caractère personnel des États membres vers des pays tiers, dans la mesure où ces transferts relèvent de son champ d'application.

(2) L'article 1er et les considérants 2 et 10 de la directive 95/46/CE visent à garantir non seulement une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit fondamental au respect de la vie privée à l'égard du traitement des données à caractère personnel, mais également un niveau élevé de protection de ces libertés et droits fondamentaux ([3]).

(3) L'importance tant du droit fondamental au respect de la vie privée, garanti par l'article 7 de la charte des droits fondamentaux de l'Union européenne, que du droit fondamental à la protection des données à caractère personnel, garanti par l'article 8 de celle-ci, a été soulignée dans la jurisprudence de la Cour de justice ([4]).

(4) Conformément à l'article 25, paragraphe 1, de la directive 95/46/CE, les États membres sont tenus de veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays en question assure un niveau de protection adéquat et si les lois des États membres qui mettent en œuvre d'autres dispositions de la directive sont respectées avant le transfert. La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat en raison de sa législation interne ou des engagements internationaux auxquels il a souscrit pour protéger les droits des personnes. Dans ce cas, et sans préjudice du respect des dispositions nationales prises en application d'autres dispositions de la directive, des données à caractère personnel peuvent être transférées à partir des États membres sans que des garanties supplémentaires soient nécessaires.

([1]) JO L 281 du 23.11.1995, p. 31.
([2]) Voir l'avis 4/2016 concernant le «Bouclier vie privée UE-États-Unis — Projet de décision d'adéquation, publié le 30 mai 2016.
([3]) Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems»), EU:C:2015:650, point 39.
([4]) Affaire C-553/07, Rijkeboer, EU:C:2009:293, point 47; affaires jointes C-293/12 et C-594/12, Digital Rights Ireland e.a., EU: C:2014:238, point 53, et affaire C-131/12, Google Spain et Google, EU:C:2014:317, points 53, 66 et 74.

(5) Conformément à l'article 25, paragraphe 2, de la directive 95/46/CE, il y a lieu d'apprécier le niveau de protection offert par un pays tiers au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données, notamment des règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause.

(6) Dans la décision 2000/520/CE de la Commission ([5]), il était considéré, aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, que les «principes de la sphère de sécurité relatifs à la protection de la vie privée», appliqués conformément aux orientations fournies par les «questions souvent posées» publiées par le ministère du commerce des États-Unis, assuraient un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis.

(7) Dans ses communications COM(2013) 846 final ([6]) et COM(2013) 847 final ([7]) du 27 novembre 2013, la Commission a considéré que les fondements du régime de la sphère de sécurité devaient être réexaminés et renforcés au vu d'un certain nombre de facteurs, dont la croissance exponentielle des flux de données et l'importance cruciale de ceux-ci pour l'économie transatlantique, l'augmentation rapide du nombre d'entreprises américaines souscrivant audit régime, ainsi que les nouvelles informations sur l'ampleur et la portée de certains programmes de renseignement américains qui ont soulevé des questions quant au niveau de protection que ledit régime pouvait garantir. La Commission a en outre relevé un certain nombre d'insuffisances et de lacunes dans le régime de la sphère de sécurité.

(8) Sur la base des éléments qu'elle a recueillis, notamment des données tirées des travaux du groupe de contact UE/États-Unis sur la protection de la vie privée ([8]) et des informations sur les programmes de renseignement américains reçues dans le cadre du groupe de travail ad hoc UE/États-Unis ([9]), la Commission a formulé 13 recommandations en vue d'un réexamen du régime de la sphère de sécurité. Ces recommandations portaient principalement sur le renforcement des principes de fond protégeant la vie privée et une plus grande transparence des politiques de confidentialité des entreprises américaines autocertifiées, sur un contrôle, un suivi et une mise en œuvre améliorés, par les autorités américaines, du respect de ces principes, sur la mise en place de mécanismes de règlement des litiges abordables et sur la nécessité de limiter le recours à la dérogation pour raison de sécurité nationale, prévue par la décision 2000/520/CE, à ce qui est strictement nécessaire et proportionné.

(9) Dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner ([10]), la Cour de justice de l'Union européenne a déclaré invalide la décision 2000/520/CE. Sans examiner le contenu des principes de la sphère de sécurité, la Cour a considéré que Commission n'avait pas fait état, dans cette décision, de ce que les États-Unis «assuraient» effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux ([11]).

(10) À cet égard, la Cour de justice a expliqué que, même si l'expression «niveau de protection adéquat» figurant à l'article 25, paragraphe 6, de la directive 95/46/CE ne signifie pas un niveau de protection identique à celui qui est garanti dans l'ordre juridique de l'Union, elle doit être comprise comme exigeant que le pays tiers assure un niveau de protection des libertés et droits fondamentaux «substantiellement équivalent» à celui qui est garanti au sein de l'Union en vertu de la directive 95/46/CE lue à la lumière de la charte des droits fondamentaux. Même si les moyens auxquels ce pays tiers a recours, à cet égard, peuvent être différents de ceux mis en œuvre au sein de l'Union, ils doivent néanmoins s'avérer, en pratique, effectifs ([12]).

(11) La Cour de justice a critiqué le fait que la décision 2000/520/CE ne comportait pas de constatations suffisantes quant à, d'une part, l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale, et, d'autre part, l'existence d'une protection juridique efficace contre des ingérences de cette nature ([13]).

([5]) Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO L 215 du 28.8.2000, p. 7).

([6]) Communication de la Commission au Parlement européen et au Conseil intitulée «Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique» [COM(2013) 846 final du 27 novembre 2013].

([7]) Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, [COM(2013) 847 final du 27 novembre 2013].

([8]) Voir, par exemple, le document du Conseil de l'Union européenne — Rapport final du groupe de contact à haut niveau UE/États-Unis sur l'échange d'informations, le respect de la vie privée et la protection des données à caractère personnel, note 9831/08 du 28 mai 2008, disponible sur l'internet à l'adresse suivante: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf.

([9]) Rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail ad hoc UE/États-Unis sur la protection des données du 27 novembre 2013, disponible sur l'internet à l'adresse suivante: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

([10]) Voir la note 3.

([11]) Arrêt Schrems, point 97.

([12]) Arrêt Schrems, points 73 et 74.

([13]) Arrêt Schrems, points 88 et 89.

(12) En 2014, la Commission avait entamé des pourparlers avec les autorités américaines en vue de discuter du renforcement du régime de la sphère de sécurité sur la base des 13 recommandations formulées dans la communication COM(2013) 847 final. À la suite de l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire Schrems, ces pourparlers se sont intensifiés en vue d'adopter une éventuelle nouvelle décision constatant l'adéquation du niveau de protection qui respecterait les exigences de l'article 25 de la directive 95/46/CE telles qu'elles ont été interprétées par la Cour de justice. Les documents annexés à la présente décision, qui seront également publiés au *Federal Register* (le Journal officiel américain), sont le fruit de ces discussions. Les principes de protection de la vie privée (annexe II) et les observations et engagements officiels de diverses autorités américaines figurant dans les documents joints en tant qu'annexes I et III à VII constituent le «bouclier de protection des données UE-États-Unis».

(13) La Commission a soigneusement analysé la législation et les pratiques des États-Unis, y compris ces observations et engagements officiels. Sur la base des constatations exposées aux considérants 136 à 140, elle conclut que les États-Unis assurent un niveau de protection adéquat des données à caractère personnel transférées, dans le cadre du bouclier de protection des données UE-États-Unis, de l'Union vers des organisations autocertifiées aux États-Unis.

2. LE «BOUCLIER DE PROTECTION DES DONNÉES UE-ÉTATS-UNIS»

(14) Le bouclier de protection des données UE-États-Unis repose sur un système d'autocertification en vertu duquel les organisations américaines s'engagent à respecter une série de principes de protection de la vie privée, constitués de principes-cadres et de principes complémentaires (ci-après, conjointement, les «principes»), qui sont publiés par le ministère américain du commerce et qui figurent à l'annexe II de la présente décision. Ce bouclier s'applique à la fois aux responsables du traitement et aux sous-traitants (mandataires), avec ceci de spécifique que les sous-traitants doivent être 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 ([14]).

(15) Sans préjudice du respect des dispositions nationales adoptées en application de la directive 95/46/CE, la présente décision a pour effet d'autoriser les transferts d'un responsable du traitement ou d'un sous-traitant de l'Union vers des organisations américaines qui ont autocertifié leur adhésion aux principes auprès du ministère du commerce et qui se sont engagées à les respecter. Les principes ne s'appliquent au traitement de données à caractère personnel par l'organisation américaine que dans la mesure où ce traitement ne relève pas du champ d'application de la législation de l'Union ([15]). Le bouclier de protection des données ne porte pas atteinte à l'application de la législation de l'Union régissant le traitement des données à caractère personnel dans les États membres ([16]).

([14]) Voir la section III.10.a. de l'annexe II. Conformément à la définition donnée à la section I.8.c., le responsable européen du traitement déterminera la finalité et les moyens du traitement des données à caractère personnel. De plus, le contrat conclu avec le mandataire doit indiquer clairement si les transferts ultérieurs sont autorisés (voir la section III.10.a.ii.2.).

([15]) Cela vaut aussi pour les données relatives aux ressources humaines transférées à partir de l'Union européenne dans le cadre d'une relation de travail. Alors que les principes soulignent la «responsabilité première» de l'employeur de l'Union européenne (voir la section III.9.d.i. de l'annexe II), ils indiquent clairement que les agissements de ce dernier sont régis par les règles applicables dans l'Union et/ou l'État membre concerné et pas par les principes. Voir les sections III.9.a.i., b.ii., c.i. et d.i. de l'annexe II.

([16]) Cela vaut également pour les traitements qui sont effectués par une organisation établie en dehors de l'Union, mais en recourant à des moyens situés sur le territoire de l'Union [voir l'article 4, paragraphe 1, point c), de la directive 95/46/CE]. À partir du 25 mai 2018, le règlement général sur la protection des données s'appliquera i) au traitement des données à caractère personnel dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union (même lorsque le traitement a lieu aux États-Unis) ou ii) au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées a) à l'offre de biens ou de services à ces personnes concernées, qu'un paiement soit exigé ou non desdites personnes, ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. Voir l'article 3, paragraphes 1 et 2, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

(16) La protection offerte aux données à caractère personnel par le bouclier de protection des données s'applique à toute personne concernée de l'Union européenne ([17]) dont les données à caractère personnel ont été transférées à partir de l'Union européenne à des organisations situées aux États-Unis qui ont autocertifié leur adhésion aux principes auprès du ministère du commerce.

(17) Les principes s'appliquent dès la certification. La seule exception concerne le principe «Responsabilité en cas de transfert ultérieur», lorsque l'organisation qui autocertifie son adhésion au bouclier de protection des données entretient déjà des relations commerciales avec des tiers. Étant donné qu'il faudra sans doute un peu de temps pour mettre ces relations commerciales en conformité avec les règles applicables en vertu de ce principe, l'organisation sera tenue de les adapter dès que possible et, en tout état de cause, dans un délai de neuf mois à compter de l'autocertification (pour autant que cette dernière intervienne dans les deux mois suivant le jour de l'entrée en vigueur du bouclier de protection des données). Pendant cette période transitoire, l'organisation devra appliquer les principes «Notification» et «Choix» (et permettre ainsi à la personne concernée de l'Union européenne de s'opposer au traitement) et, lorsque des données à caractère personnel seront transférées à un tiers agissant en qualité de mandataire, elle devra veiller à ce que ce dernier offre au moins le niveau de protection requis par les principes ([18]). Cette période transitoire constitue un compromis raisonnable et approprié entre le respect du droit fondamental à la protection des données et le besoin légitime des entreprises de disposer d'un délai suffisant pour s'adapter au nouveau cadre, lorsque cette adaptation dépend aussi de leurs relations commerciales avec des tiers.

(18) Le système sera géré et contrôlé par le ministère du commerce conformément aux engagements qu'il a pris et qui sont énoncés dans les observations du secrétaire d'État américain au commerce (annexe I de la présente décision). S'agissant de l'application effective des principes, les observations de la Commission fédérale du commerce (Federal Trade Commission — FTC) et du ministère du transport figurent aux annexes IV et V de la présente décision.

2.1. *Principes de protection de la vie privée*

(19) Lorsqu'elles autocertifient leur adhésion au bouclier de protection des données UE-États-Unis, les organisations doivent s'engager à respecter les principes ([19]).

(20) En vertu du *principe «Notification»*, les organisations ont l'obligation de fournir aux personnes concernées des informations sur un certain nombre d'éléments essentiels en rapport avec le traitement de leurs données à caractère personnel (tels que le type de données recueillies, la finalité du traitement, le droit d'accès et de choix, les conditions applicables aux transferts ultérieurs et la responsabilité du traitement). D'autres garanties s'appliquent, en particulier l'obligation, pour les organisations, de rendre publiques leurs politiques en matière de protection de la vie privée (qui tiennent compte des principes) et de fournir des liens dirigeant vers le site web du ministère du commerce (qui donne davantage de détails sur l'autocertification, les droits des personnes concernées et les mécanismes de recours disponibles), vers la liste du bouclier de protection des données mentionnée au considérant 30 et vers le site web d'un organe approprié de règlement extrajudiciaire des litiges.

(21) En vertu du *principe «Intégrité des données et limitation des finalités»*, les données à caractère personnel doivent se limiter à ce qui est pertinent aux fins du traitement et êtres fiables par rapport à l'utilisation prévue, exactes, exhaustives et actuelles. 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. Les organisations doivent veiller à ce que les données à caractère personnel soient fiables par rapport à l'utilisation prévue, exactes, exhaustives et actuelles.

([17]) La présente décision présente un intérêt pour l'EEE. L'accord sur l'Espace économique européen (ci-après l'«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 législation de l'Union en matière de protection des données, y compris la directive 95/46/CE, est couverte par l'accord EEE et a été intégrée dans l'annexe XI de celui-ci. Le Comité mixte de l'EEE doit décider de l'intégration de la présente décision dans l'accord EEE. Dès que la présente décision s'appliquera à l'Islande, au Liechtenstein et à la Norvège, ceux-ci seront également couverts par le bouclier de protection des données UE-États-Unis et les références à l'Union européenne et à ses États membres figurant dans le paquet «bouclier de protection des données» s'entendront comme incluant ces trois pays.

([18]) Voir la section III.6.e de l'annexe II.

([19]) Des règles particulières fournissant des garanties supplémentaires s'appliquent aux données relatives aux ressources humaines recueillies dans le contexte d'une relation de travail, ainsi que le prévoit le principe complémentaire «Données relatives aux ressources humaines» (voir la section III.9 de l'annexe II). Par exemple, les employeurs devraient tenir 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. Plus important encore, lorsqu'il est question de telles données, les organisations sont tenues de coopérer avec les autorités de protection des données de l'Union et à respecter l'avis de celles-ci.

(22) Lorsqu'une nouvelle finalité (modifiée) est sensiblement différente de la finalité initiale, mais qu'elle reste compatible avec celle-ci, le *principe «Choix»* donne aux personnes concernées le droit de s'opposer au traitement (refus). Le *principe «Choix»* ne se substitue pas à l'interdiction expresse de procéder à des traitements incompatibles ([20]). Des règles particulières permettant, de manière générale, de refuser «à tout moment» l'utilisation de données à caractère personnel s'appliquent au marketing direct ([21]). En cas de données sensibles, les organisations doivent normalement obtenir le consentement exprès de la personne concernée («consentement»).

(23) Toujours en vertu du *principe «Intégrité des données et limitation des finalités»*, 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) 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. Cette obligation n'empêche pas les organisations participant au bouclier 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 ci-après: l'archivage dans l'intérêt public, le journalisme, l'art et la littérature, ainsi que la recherche historique et l'analyse statistique. La conservation de données à caractère personnel pendant une période plus longue à l'une de ces fins sera soumise aux garanties prévues par les principes.

(24) En vertu du *principe «Sécurité»*, les organisations qui créent, gèrent, utilisent ou diffusent des données à caractère personnel doivent prendre des mesures de sécurité raisonnables et adéquates, qui tiennent compte des risques inhérents au traitement et à la nature des données. En cas de sous-traitance, les organisations doivent conclure avec le sous-traitant 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.

(25) En vertu du *principe «Accès»* ([22]), les personnes concernées ont le droit, sans justification et sans redevance excessive, d'obtenir d'une organisation qu'elle leur confirme le traitement de données à caractère personnel les concernant et qu'elle leur communique ces données dans un délai raisonnable. Ce droit ne peut être restreint que dans des circonstances exceptionnelles. 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. Les personnes concernées doivent pouvoir corriger, modifier ou supprimer les informations à caractère personnel lorsque celles-ci sont inexactes ou qu'elles ont été traitées en violation des principes. 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), le droit américain offre des protections spécifiques contre les décisions négatives ([23]). 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. Ces règles offrent une protection dans les cas probablement assez peu nombreux dans lesquels des décisions automatisées seraient prises par l'organisation participant au bouclier de protection des données elle-même ([24]). Néanmoins, compte tenu du recours accru au traitement automatisé (y compris au profilage) pour fonder des décisions concernant les personnes dans l'économie numérique moderne, ce domaine doit faire l'objet d'une étroite surveillance. Afin de faciliter cette surveillance, il a été convenu avec les autorités américaines qu'un dialogue sur la prise de décision automatisée, comportant un échange de vues sur les similitudes et les différences des approches adoptées par l'Union européenne et les États-Unis en la matière, sera prévu dans le cadre du premier examen annuel et, s'il y a lieu, des examens ultérieurs.

([20]) Cela vaut pour tous les transferts de données effectués dans le cadre du bouclier de protection des données, y compris lorsqu'ils concernent des données recueillies dans le contexte d'une relation de travail. Si une organisation américaine autocertifiée peut, 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. 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.

([21]) Voir la section III.12 de l'annexe II.

([22]) Voir également le principe complémentaire «Accès» (section III.8 de l'annexe II).

([23]) Voir, par exemple, l'Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 et suivants), le FAIR Credit Reporting Act (FRCA, 15 U.S.C. § 1681 et suivants) ou le FAIR Housing Act (FHA, 42 U.S.C. 3601 et suivants).

([24]) Dans la plupart des cas, lors d'un transfert de données à caractère personnel recueillies dans l'Union européenne, c'est avec le responsable européen du traitement, tenu de respecter les règles de l'Union européenne en matière de protection des données, que la personne (le client) entretiendra une relation contractuelle et c'est généralement ce responsable européen du traitement qui prendra une décision sur la base d'un traitement automatisé. Cela englobe les cas de figure dans lesquels le traitement est effectué par une organisation participant au bouclier de protection des données qui agit en tant que mandataire pour le compte du responsable européen du traitement.

(26) En vertu du *principe «Voies de recours, application et responsabilité»* ([25]), les organisations participantes doivent prévoir des mécanismes solides destinés à garantir le respect des autres principes, ainsi que des possibilités de recours, y compris en vue d'obtenir une réparation effective, pour les personnes concernées de l'Union européenne dont les données à caractère personnel ont été traitées en violation des principes. Une fois qu'une organisation a pris volontairement la décision d'autocertifier ([26]) son adhésion au bouclier de protection des données UE-États-Unis, elle doit obligatoirement respecter les principes. Afin de pouvoir continuer à se prévaloir du bouclier de protection des données pour recevoir des données à caractère personnel de l'Union, cette organisation doit recertifier chaque année sa participation au bouclier. Les organisations doivent également prendre des mesures pour vérifier ([27]) que les politiques en matière de protection de la vie privée qu'elles ont rendues publiques 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 ou des vérifications aléatoires. En outre, l'organisation doit mettre en place un mécanisme de recours effectif pour traiter les réclamations éventuelles (voir également à cet égard le considérant 43) et est soumise aux pouvoirs d'enquête et d'exécution de la FTC, du ministère du transport ou de tout autre organisme officiel américain qui veillera au respect effectif des principes.

(27) Des règles particulières s'appliquent aux transferts dits «ultérieurs», c'est-à-dire aux transferts de données à caractère personnel d'une organisation 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). Ces règles visent à faire en sorte que la protection garantie des données à caractère personnel des personnes concernées de l'Union européenne ne sera pas compromise, et ne pourra pas être contournée, lorsque ces données seront transférées à des tiers. Elles sont particulièrement importantes en cas de chaînes de traitement plus complexes, caractéristiques de l'économie numérique actuelle.

(28) En vertu du principe *«Responsabilité en cas de transfert ultérieur»* ([28]), tout transfert ultérieur ne peut avoir lieu: i) qu'à des fins limitées et spécifiques; ii) que sur la base d'un contrat [ou d'un dispositif comparable en cas de transfert intragroupe ([29])] et iii) que si ce contrat prévoit le même niveau de protection que celui qui est garanti par les principes, ce qui implique notamment que l'application de ces derniers ne peut être limitée que dans la mesure nécessaire à la sécurité nationale, au respect de la loi ou à d'autres intérêts publics ([30]). Ces règles doivent être lues en liaison avec le *principe «Notification»* et, en cas de transfert ultérieur à un responsable du traitement dans un pays tiers ([31]), 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). Au vu du *principe «Intégrité des données et limitation des finalités»*, l'obligation d'offrir le même niveau de protection que celui qui est garanti par les principes présuppose 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 initialement collectées ou qui ont été approuvées ultérieurement par la personne concernée.

(29) 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. En tout état de cause, le contrat avec le destinataire tiers doit prévoir que ce dernier prévient l'organisation participant au bouclier de protection des données s'il constate qu'il n'est plus en mesure de respecter cette obligation. Dans ce cas, il y a lieu de mettre

([25]) Voir également le principe complémentaire «Résolution des litiges et application des décisions» (section III.11 de l'annexe II).
([26]) Voir également le principe complémentaire «Autocertification» (section III.6 de l'annexe II).
([27]) Voir également le principe complémentaire «Vérification» (section III.7 de l'annexe II).
([28]) Voir également le principe complémentaire «Contrats obligatoires pour les transferts ultérieurs» (section III.10 de l'annexe II).
([29]) Voir le principe complémentaire «Contrats obligatoires pour les transferts ultérieurs» (section III.10.b de l'annexe II). 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 autocertifiée restera responsable du respect des principes, elle aura tout intérêt à utiliser des instruments réellement efficaces dans la pratique.
([30]) Voir la section I.5 de l'annexe II.
([31]) 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.

fin au traitement ou de prendre d'autres mesures raisonnables et appropriées pour remédier à la situation ([32]). Si des problèmes de respect des principes se posent dans la chaîne de (sous-)traitance, l'organisation participant au bouclier de protection des données qui agit en tant que responsable du traitement des données à caractère personnel devra prouver que le fait générateur du dommage ne lui est pas imputable. Dans le cas contraire, il devra en assumer la responsabilité, conformément au *principe «Voies de recours, application et responsabilité»*. Des protections supplémentaires sont prévues en cas de transfert ultérieur à un mandataire tiers ([33]).

2.2. *Transparence, gestion et contrôle du bouclier de protection des données UE-États-Unis*

(30) Le bouclier de protection des données UE-États-Unis prévoit des mécanismes de contrôle et d'application destinés à vérifier et à garantir que les entreprises américaines autocertifiées respectent les principes et qu'il sera remédié à tout manquement à cet égard. Ces mécanismes sont définis dans les principes (annexe II) et dans les engagements pris par le ministère américain du commerce (annexe I), la FTC (annexe IV) et le ministère des transports (annexe V).

(31) Pour que le bouclier de protection des données 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. À cet effet, le ministère américain du commerce s'est engagé à tenir et à rendre publique une liste des organisations qui ont autocertifié leur adhésion aux principes et qui relèvent de la compétence d'au moins une des autorités chargées de l'application du bouclier mentionnées aux annexes I et II de la présente décision («liste du bouclier de protection des données») ([34]). Le ministère du commerce actualisera la liste en fonction des recertifications annuelles et chaque fois qu'une organisation se retire ou est radiée du bouclier de protection des données. Il 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. Enfin, il fournira un lien dirigeant vers la liste des affaires en rapport avec l'application du bouclier de protection des données dont la FTC est saisie (cette liste figure sur le site web de cette dernière).

(32) Le ministère du commerce publiera la liste du bouclier de protection des données et les recertifications sur un site web dédié. Les organisations autocertifiées devront pour leur part fournir l'adresse web de la liste du bouclier de protection des données gérée par le ministère. En outre, si elle est disponible en ligne, la politique de l'organisation en matière de protection de la vie privée doit inclure un lien dirigeant vers le site web du bouclier de protection des données, ainsi qu'un lien dirigeant vers le site web ou le formulaire d'introduction des réclamations du mécanisme de recours indépendant chargé d'instruire les réclamations non résolues. Le ministère du commerce vérifiera systématiquement, dans le contexte de la certification et de la recertification d'une organisation, si la politique de cette dernière en matière de protection de la vie privée est conforme aux principes.

(33) Les organisations qui persistent à ne pas respecter les principes seront radiées de la liste du bouclier de protection des données et devront renvoyer ou supprimer les données à caractère personnel reçues dans le cadre de ce dernier. Les organisations qui sont rayées de la liste pour d'autres raisons, telles que le retrait volontaire ou la non-recertification, peuvent conserver ces données 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). Dans ce cas, l'organisation doit identifier en son sein un point de contact pour toutes les questions liées au bouclier de protection des données UE-États-Unis.

(34) Le ministère du commerce surveillera les organisations qui ne participent plus au bouclier de protection des données, parce qu'elles s'en sont volontairement retirées ou que leur certification a expiré, afin de vérifier si elles restituent, suppriment ou conservent ([35]) les données à caractère personnel reçues antérieurement dans le cadre

([32]) 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 bouclier de protection des données — en tant qu'organisation responsable du traitement sur les instructions de laquelle le mandataire agit — de prendre ces mesures.

([33]) En pareil cas, l'organisation américaine doit également 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.

([34]) Pour de plus amples informations sur la gestion de la liste du bouclier de protection des données, voir les annexes I et II (sections I.3, I.4, III.6.d, et III.11.g).

([35]) Voir les sections I.3., III.6.f. et III.11.g.i. de l'annexe II.

du bouclier. Si elles conservent ces données, les organisations sont tenues de continuer à leur appliquer les principes. Lorsque le ministère du commerce a radié des organisations en raison d'un non-respect persistant des principes, il veille à ce que ces organisations restituent ou suppriment les données à caractère personnel qu'elles ont reçues dans le cadre du bouclier.

(35) Lorsqu'une organisation se retire du bouclier de protection des données UE-États-Unis, quelle qu'en soit la raison, elle doit supprimer toute déclaration publique laissant croire qu'elle continue à participer au bouclier ou qu'elle peut prétendre au bénéfice de celui-ci. Elle doit notamment supprimer toute référence au bouclier dans la politique de protection de la vie privée qu'elle rend publique. Le ministère du commerce recherchera les fausses déclarations de participation au bouclier, y compris par d'anciens participants ([36]), et s'emploiera à y remédier. 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 du transport ou toute autre autorité américaine chargée de l'application du bouclier. 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) ([37]).

(36) Le ministère du commerce surveillera d'office toutes les fausses déclarations de participation au bouclier de protection des données ou les usages abusifs de la marque de certification, et les APD peuvent renvoyer les organisations à un point de contact spécialisé au sein du ministère en vue d'un contrôle. Lorsqu'une organisation s'est retirée du bouclier de protection des données, ne recertifie pas son engagement à respecter les principes ou est radiée de la liste du bouclier, le ministère du commerce vérifiera, de manière suivie, qu'elle a supprimé de la politique en matière de protection de la vie privée qu'elle a rendue publique toute référence au bouclier de protection des données laissant croire qu'elle continue d'y participer et, si les fausses déclarations persistent, il saisira la FTC, le ministère du transport ou toute autre autorité compétente en vue de l'adoption d'éventuelles mesures d'exécution. Le ministère du commerce adressera des questionnaires aux organisations dont l'autocertification a expiré ou qui se sont volontairement retirées du bouclier de protection des données afin de vérifier si elles ont l'intention de restituer ou de supprimer les données à caractère personnel qu'elles ont reçues lorsqu'elles participaient au bouclier ou si elles comptent continuer à leur appliquer les critères, auquel cas, il devra vérifier qui, au sein de l'organisation, servira de point de contact permanent pour les questions liées au bouclier.

(37) Sur une base continue, le ministère du commerce procédera d'office à des contrôles visant à déterminer si les organisations autocertifiées respectent les principes ([38]), notamment en leur envoyant des questionnaires détaillés. Il procédera aussi à un contrôle systématique chaque fois qu'il recevra une réclamation spécifique (sérieuse), qu'une organisation ne répondra pas de manière satisfaisante à ses demandes d'information ou que des indices crédibles donneront à penser qu'une organisation ne respecte par les principes. S'il y a lieu, le ministère du commerce consultera aussi les APD au sujet de ces contrôles.

2.3. *Mécanismes de recours, traitement des réclamations et application effective*

(38) Par le *principe «Voies de recours, application et responsabilité»*, le bouclier de protection des données 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 européenne, d'introduire une réclamation en cas de non-respect des principes par des entreprises américaines certifiées, ainsi que de voir ces réclamations tranchées et aboutir si nécessaire à une décision prévoyant une réparation effective.

(39) Dans le cadre de leur autocertification, les organisations doivent satisfaire aux exigences découlant du principe «Voies de recours, application et responsabilité», en prévoyant des mécanismes de recours indépendants facilement accessibles et efficaces qui permettent d'examiner et de trancher rapidement toute réclamation et tout litige sans frais pour les personnes concernées.

(40) Les organisations peuvent opter pour des mécanismes de recours indépendants, soit dans l'Union, soit aux États-Unis, dont la possibilité de s'engager, sur une base volontaire, à coopérer avec les APD de l'Union européenne.

([36]) Voir la section «Détecter et traiter les fausses déclarations de participation» à l'annexe I.
([37]) Voir les sections III.6.h et III.11.f de l'annexe II.
([38]) Voir l'annexe I.

Cependant, un tel choix n'existe pas lorsque les organisations traitent des données relatives aux ressources humaines, auquel cas la coopération avec les APD 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». Les organisations sont tenues de remédier aux problèmes de non-respect. Elles doivent aussi préciser qu'elles sont soumises aux pouvoirs d'enquête et d'application de la FTC, du ministère du transport ou de tout autre organisme officiel américain.

(41) Par conséquent, le cadre du bouclier de protection des données 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 américaines autocertifiées 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 ou de la FTC.

(42) 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 du mécanisme de règlement des litiges offert par le comité du bouclier de protection des données (Privacy Shield Panel) (annexe 1 de l'annexe II 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. Toutefois, comme indiqué ci-dessous, il existe un certain ordre logique qu'il est conseillé de suivre.

(43) Premièrement, les personnes concernées de l'Union peuvent introduire une réclamation en cas de non-conformité aux principes de protection de la vie privée en prenant directement contact avec l'*entreprise américaine autocertifiée*. 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 des instances indépendantes de traitement des réclamations.

(44) 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 européenne dans un délai de 45 jours. Cette réponse doit contenir une appréciation du bien-fondé de la réclamation et des informations sur la manière dont l'organisation remédiera au problème. 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 ([39]) (lorsque l'organisation s'est engagée à coopérer avec l'APD). Les organisations doivent conserver des archives sur la mise en œuvre de leurs politiques en matière de protection de la vie privée et les remettre sur demande à une instance de recours indépendante ou à la FTC (ou à une autre autorité américaine compétente en matière de pratiques déloyales et frauduleuses) dans le cadre d'une enquête ou d'une réclamation pour non-conformité.

(45) 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. 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. 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 bouclier de protection des données UE—États-Unis et aux services qu'ils fournissent à ce titre. Ils doivent publier chaque année un rapport annuel fournissant des statistiques agrégées concernant ces services ([40]).

([39]) Il s'agit de l'autorité responsable du traitement désignée par le panel d'APD établi dans le principe additionnel sur le «Rôle des autorités chargées de la protection des données» (annexe II, section III.5).

([40]) Le rapport annuel comprend: 1) le nombre total de réclamations relatives au bouclier de protection des données 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.

(46) Dans le cadre de ses procédures de contrôle de la conformité, le ministère du commerce s'assurera que les entreprises américaines autocertifiées sont effectivement enregistrées auprès des instances de recours indépendantes auprès desquelles elles affirment être enregistrées. Tant les organisations que les instances de recours indépendantes compétentes sont tenues de répondre rapidement aux questions et aux demandes formulées par le ministère du commerce pour les informations qui ont trait au bouclier de protection des données.

(47) 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 pratiques déloyales et frauduleuses), ou à un tribunal compétent ([41]). 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 sera considéré comme une non-conformité persistante et, en conséquence, le ministère du commerce retira de la liste 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 ([42]). Si une organisation continue à affirmer qu'elle est certifiée au regard du bouclier de protection des données après avoir été retirée de la liste, le ministère en réfèrera à la FTC ou à un autre service répressif ([43]).

(48) Troisièmement, les personnes peuvent également introduire leurs réclamations auprès d'une *APD* nationale. 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. 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.

(49) Les avis des APD seront communiqués par l'intermédiaire d'un panel informel d'APD établi au niveau de l'Union ([44]), qui aidera notamment à garantir qu'une réclamation donnée est traitée selon une approche harmonisée et cohérente. Un avis ne sera émis que lorsque l'on aura 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 donnera 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. 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 notifiera 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). 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 bouclier de protection des données.

(50) 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 concerné.

(51) 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 bouclier de protection des données 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 ([45]). De même, la FTC s'est engagée à mettre en place un point de contact ad hoc ([46]) et à assister les APD dans les enquêtes en vertu du SAFE WEB Act américain ([47]).

([41]) Voir la section III.11.e de l'annexe II.
([42]) Voir la section III.11.g de l'annexe II et, en particulier, les points ii) et iii).
([43]) Voir la section intitulée «Détecter et traiter les fausses déclarations de participation» de l'annexe I.
([44]) Il convient que les APD établissent le règlement intérieur du panel informel d'APD, étant donné qu'elles sont compétentes pour organiser leurs travaux et coopérer entre elles.
([45]) Voir les sections intitulées «Renforcer la coopération avec les APD» et «Faciliter le traitement définitif des réclamations pour non-conformité» de l'annexe I et la section II.7.e de l'annexe II.
([46]) Voir l'annexe IV, p. 6.
([47]) Idem.

(52) 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. 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 entreprises, pour faciliter le règlement des litiges. Afin d'accélérer le traitement des réclamations individuelles, le point de contact sera en contact direct avec l'APD concernée en ce qui concerne les problèmes de conformité et, en particulier, tiendra celle-ci informée de l'état des réclamations dans un délai maximal de 90 jours à compter de la saisine. Cela permet aux personnes concernées d'introduire des réclamations pour non-conformité d'entreprises américaines autocertifées directement auprès de leur APD nationale, ces réclamations étant ensuite canalisées vers le ministère du commerce, qui est l'autorité américaine chargée de gérer le bouclier de protection des données UE —États-Unis. Le ministère du commerce a également promis de fournir, dans le cadre de l'examen annuel du fonctionnement du bouclier de protection des données UE—États-Unis, un rapport contenant une analyse agrégée des réclamations qu'il reçoit chaque année ([48]).

(53) 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 bouclier de protection des données. 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.

(54) Cinquièmement, une organisation participant au bouclier de protection des données doit être soumise aux pouvoirs d'enquête et au pouvoir coercitif des autorités américaines, notamment la FTC ([49]), qui veillera au respect effectif des principes. Cette dernière examinera en priorité les saisines pour non-conformité aux principes de protection de la vie privée 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 ([50]). 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 acceptera les réclamations qui lui seront directement adressées par des personnes physiques et ouvrira des enquêtes sur le bouclier de protection des données de sa propre initiative, notamment dans le cadre de ses enquêtes générales sur les aspects relatifs à la protection de la vie privée.

(55) La FTC peut exiger la mise en conformité par des injonctions administratives (*consent order*) et elle contrôle systématiquement si ces directives sont respectées. Lorsque les organisations ne se conforment pas à ces injonctions, la FTC peut porter l'affaire devant le tribunal compétent afin de requérir des amendes administratives et d'autres sanctions, y compris pour tout préjudice causé par le comportement illégal. La FTC peut également requérir directement auprès d'un tribunal fédéral une injonction préliminaire ou permanente ou d'autres mesures visant à remédier à la situation de non-conformité. Chaque *consent order* adressée à une organisation participant au bouclier de protection des données contiendra des dispositions en matière de notification spontanée ([51]) et les organisations seront tenues de publier toute section du bouclier de protection des données 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 bouclier de protection des données.

(56) 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 européenne, celle-ci peut recourir à un arbitrage contraignant par le «panel du bouclier de protection des données». Les organisations doivent informer les personnes qu'elles ont la possibilité de faire appel à un arbitrage contraignant sous certaines conditions et, lorsqu'une personne a notifié à une organisation qu'elle recourait à cette possibilité, l'organisation en question est tenue de donner suite ([52]).

([48]) Voir la section intitulée «Faciliter le traitement définitif des réclamations pour non-conformité» de l'annexe I.

([49]) Une organisation participant au bouclier de protection des données de l'organisation doit déclarer publiquement qu'elle s'engage à respecter les principes, divulguer publiquement ses politiques en matière de protection de la vie privée, qui doivent être conformes aux principes, et mettre pleinement en œuvre ces politiques. 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.

([50]) 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 l'article 20 du FTC Act) et peut utiliser le système judiciaire pour faire exécuter ces injonctions en cas de non-conformité.

([51]) 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.

([52]) Voir les sections II.1.xi et III.7.c de l'annexe II.

(57) Ce panel d'arbitrage sera composé d'un groupe d'au moins 20 arbitres 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 sélectionneront dans ce groupe un panel constitué d'un, de deux ou de trois arbitres ([53]). La procédure sera régie par des règles d'arbitrage standard à convenir entre le ministère du commerce et la Commission. Ces règles compléteront le cadre qui a déjà été arrêté et qui contient plusieurs éléments facilitant l'accès des personnes concernées de l'Union européenne 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 normalement ([54]) 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 bouclier de protection des données, 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.

(58) Le panel du bouclier de protection des données aura le pouvoir d'imposer les «mesures d'équité personnalisées et non pécuniaires» ([55]) 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 bouclier de protection des données, mais les personnes peuvent toujours recourir à l'arbitrage si elles estiment que ces mesures sont insuffisantes. Cela permettra 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 autorités compétentes américaines (par exemple la FTC), 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'entreprise américaine autocertifiée, 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.

(59) 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 les législations des États américains, qui prévoient des voies de recours au titre de la responsabilité délictuelle et dans les cas de dol, d'actes et de pratiques déloyales ou frauduleuses ou de rupture de contrat.

(60) En outre, lorsqu'une APD, après avoir reçu une réclamation d'une personne concernée de l'Union européenne, considère que le transfert des données concernant une personne à une organisation aux États-Unis est effectué en violation de la législation de l'Union européenne en matière de protection des données, notamment lorsque l'exportateur de données a des raisons de croire que l'organisation ne respecte pas les principes, cette APD peut également exercer ses pouvoirs à l'égard dudit exportateur de données et, si nécessaire, ordonner la suspension du transfert de données.

(61) À la lumière des informations figurant dans cette section, la Commission considère que les principes publiés par le ministère du commerce des États-Unis garantissent en tant que tels un niveau de protection des données à caractère personnel essentiellement équivalent à celui qui est garanti par les principes matériels de base énoncés dans la directive 95/46/CE.

(62) En outre, l'application effective des principes est garantie par les obligations de transparence et par le fait que le ministère du commerce gère le bouclier de protection des données et assure le contrôle de la conformité en ce qui concerne ce bouclier.

(63) De plus, la Commission considère que, pris dans leur ensemble, les mécanismes de surveillance, de recours et de coercition prévus par le bouclier de protection des données permettent de détecter et de sanctionner, en pratique, les infractions aux principes commises par des organisations participant au bouclier 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.

([53]) Le nombre d'arbitres dans chaque panel devra faire l'objet d'un accord entre les parties.

([54]) Le panel peut toutefois considérer que cette mise à disposition entraînerait des coûts injustifiés ou disproportionnés, eu égard aux circonstances de l'arbitrage en question.

([55]) Si les personnes ne peuvent pas réclamer de dommages-intérêts dans le cadre de l'arbitrage, le fait de recourir à l'arbitrage n'empêchera en revanche pas de réclamer par ailleurs des dommages et intérêts devant les tribunaux américains ordinaires.

3. ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DANS LE CADRE DU BOUCLIER DE PROTECTION DES DONNÉES UE—ÉTATS-UNIS ET UTILISATION DE CES DONNÉES PAR LES AUTORITÉS PUBLIQUES AMÉRICAINES

(64) Comme il découle de la section I.5 de l'annexe II, l'adhésion aux principes est limitée à ce qui est nécessaire pour satisfaire aux obligations ayant trait à la sécurité nationale, à l'intérêt public ou au respect de la loi.

(65) La Commission a évalué les limitations et garanties prévues dans la législation des États-Unis en ce qui concerne l'accès aux données à caractère personnel transférées dans le cadre du bouclier de protection des données UE—États-Unis et l'utilisation de ces données par les autorités publiques américaines à des fins de sécurité nationale, de respect de la loi ou d'intérêt public. En outre, le gouvernement américain, par l'intermédiaire de son bureau du directeur du renseignement national (Office of the Director of National Intelligence, ODNI) ([56]), a transmis à la Commission des observations et des engagements détaillés qui figurent à l'annexe VI de la présente décision. Par lettre signée par le secrétaire d'État américain, qui figure à l'annexe III de la présente décision, le gouvernement des États-Unis s'est également engagé à créer un nouveau mécanisme de surveillance pour les ingérences de la sécurité nationale, à savoir le médiateur du bouclier de protection des données, qui est indépendant de la communauté du renseignement. Enfin, une série d'observations du ministère de la justice américain, figurant à l'annexe VII de la présente décision, décrivent les limitations et garanties applicables à l'accès aux données et à l'utilisation de ces données par les autorités publiques aux fins de garantir le respect de la loi et à d'autres fins d'intérêt général. Afin d'accroître la transparence et de manifester la nature juridique de ces engagements, chacun des documents mentionnés et annexés à la présente décision sera publié au Journal officiel des États-Unis (*U.S. Federal Register*).

(66) Les conclusions de la Commission concernant les limitations de l'accès aux données à caractère personnel transférées de l'Union européenne vers les États-Unis et de l'utilisation de ces données par les autorités publiques américaines et concernant l'existence d'une protection juridique effective sont détaillées ci-dessous.

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

(67) Il ressort de l'analyse effectuée par la Commission que le droit américain prévoit plusieurs limitations de l'accès aux données à caractère personnel transférées dans le cadre du bouclier de protection des données UE—États-Unis et de l'utilisation de ces données à des fins de sécurité nationale, ainsi qu'une surveillance et des mécanismes de recours qui offrent des garanties suffisantes pour que lesdites données soient protégées de manière efficace contre les interventions illicites et le risque d'abus ([57]). Depuis 2013, l'année au cours de laquelle la Commission a publié ses deux communications (voir le considérant 7), ce cadre juridique a été considérablement renforcé, comme décrit ci-dessous.

3.1.1. Limitations

(68) En vertu de la Constitution des États-Unis, il appartient au président, en tant que commandant en chef des forces armées et chef de l'exécutif, de garantir la sécurité nationale, et, en ce qui concerne le renseignement extérieur, de conduire les affaires étrangères des États-Unis ([58]). Même si le Congrès a le pouvoir d'imposer certaines limitations et a déjà fait usage de ce pouvoir à divers égards, le président peut, à l'intérieur de ces limites, diriger les activités de la communauté américaine du renseignement, notamment par des décrets présidentiels ou des directives présidentielles. Cela vaut évidemment aussi dans les domaines où il n'existe aucune orientation de la part du Congrès. Actuellement les deux instruments juridiques essentiels à cet égard sont le décret présidentiel n° 12333 (*Executive Order 12333*, ci-après l'«E.O. 12333») ([59]) et la directive stratégique présidentielle n° 28 (*Presidential Policy directive 28*, ci-après la «PPD-28»).

([56]) Le directeur du renseignement national (*Director of National Intelligence*, DNI) exerce les fonctions de chef de la communauté du renseignement et de conseiller principal auprès du président et du Conseil national de sécurité. Voir l'Intelligence Reform and Terrorism Prevention Act de 2004, publié sous la référence *Pub. L. 108-458* du 17.12.2004. L'ODNI est notamment chargé de réglementer, gérer et diriger les activités de commande, de collecte, d'analyse, de production et de diffusion de renseignements nationaux exercées par la communauté du renseignement, y compris en élaborant des orientations sur la manière d'accéder aux informations ou aux renseignements et d'utiliser et de partager ces informations ou renseignements. Voir l'article 1.3 (a), (b) de l'E.O. 12333 (décret présidentiel n° 12333).

([57]) Voir l'arrêt Schrems, point 91.

([58]) Constitution des États-Unis, article II. Voir aussi l'introduction de la PPD-28.

([59]) *E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No. 235* (8 décembre 1981). Dans la mesure où il est accessible au public, le décret présidentiel définit 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 (en particulier, la nécessité de promulguer des règles procédurales propres). Conformément à l'article 3.2 de l'E.O. 12333, le président, assisté par le Conseil national de sécurité, et le DNI publient les directives, procédures et orientations appropriées qui sont nécessaires à la mise en œuvre du décret.

(69) La PPD-28, qui a été publiée le 17 janvier 2014, impose un certain nombre de limitations pour les opérations de «renseignement d'origine électromagnétique» ([60]). Cette directive présidentielle a force obligatoire pour les autorités américaines de renseignement ([61]) et continue de produire ses effets après un changement de gouvernement américain ([62]). La PPD-28 revêt une importance particulière pour les personnes qui ne sont pas américaines, y compris les personnes concernées de l'Union. Elle dispose notamment ce qui suit:

a) la collecte de renseignements d'origine électromagnétique doit être fondée sur une loi ou une autorisation présidentielle et doit être effectuée conformément à la Constitution des États-Unis (en particulier, son quatrième amendement) et au droit des États-Unis;

b) toute personne doit être traitée avec respect et dignité, quels que soient sa nationalité et son lieu de résidence;

c) toute personne a des intérêts légitimes de protection de sa vie privée dans le cadre du traitement de ses données à caractère personnel;

d) il est pleinement tenu compte de la protection de la vie privée et des libertés fondamentales dans la planification des activités de renseignement d'origine électromagnétique des États-Unis;

e) les activités de renseignement d'origine électromagnétique des États-Unis doivent, dès lors, comporter des garanties appropriées pour les données à caractère personnel de toute personne, quels que soient sa nationalité et son lieu de résidence.

(70) La PPD-28 dispose que les renseignements d'origine électromagnétique peuvent être collectés uniquement s'il existe une finalité de renseignement extérieur ou de contre-espionnage, pour soutenir des missions nationales et ministérielles, et jamais à d'autres fins (par exemple, pour offrir un avantage concurrentiel aux entreprises américaines). À cet égard, l'ODNI explique que les composantes de la communauté du renseignement «devraient, à chaque fois que cela est faisable, exiger que la collecte soit focalisée sur des cibles ou aspects spécifiques du renseignement extérieur par l'utilisation de discriminants (par exemple, des dispositifs spécifiques, des règles de sélection et des identifiants)» ([63]). En outre, les observations donnent des assurances que les décisions en matière de collecte de renseignements ne sont pas laissées à la discrétion de l'un ou l'autre agent de renseignement, mais obéissent à des politiques et des procédures que les différentes composantes (les services) de la communauté américaine du renseignement sont tenues de mettre en place pour mettre en œuvre la PPD-28 ([64]). En conséquence, l'élaboration et le choix des sélecteurs appropriés sont effectués au sein du cadre des priorités de contrôle du renseignement national (*National Intelligence Priorities Framework*, NIPF); ce cadre général garantit que les priorités en matière de renseignement sont fixées par des décideurs politiques de haut niveau et sont régulièrement réexaminées afin de rester adaptées aux menaces réelles pour la sécurité nationale et en tenant compte des risques potentiels, y compris les risques d'atteinte à la vie privée ([65]). Sur cette base, les agents des différents services élaborent et établissent des règles spécifiques de sélection qui doivent collecter des renseignements extérieurs répondant aux priorités ([66]). Les règles de sélection, aussi appelées «sélecteurs», doivent être régulièrement réexaminées afin de voir si elles continuent de fournir des renseignements pertinents au regard des priorités ([67]).

([60]) Conformément à l'E.O. 12333, le directeur de l'Agence de sécurité nationale (National Security Agency, NSA) est le directeur fonctionnel pour le renseignement d'origine électromagnétique, qui gère une organisation unifiée pour les activités de renseignement d'origine électromagnétique.

([61]) Pour la définition de l'expression «*Intelligence Community*» (communauté du renseignement), voir l'article 3.5 (h) de l'E.O. 12333 et la note 1 de bas de page de la PPD-28.

([62]) Voir le document *Memorandum by the Office of Legal Counsel, Department of Justice (DOJ), to President Clinton* du 29 janvier 2000. Selon cet avis juridique, les directives présidentielles ont le «même effet juridique matériel qu'un décret présidentiel».

([63]) Observations de l'ODNI (annexe VI), p. 3.

([64]) Voir section 4(b),(c) de la PPD-28. Selon des informations publiques, l'examen de 2015 a confirmé les six finalités existantes. Voir le document *ODNI, Signals Intelligence Reform, 2016 Progress Report*.

([65]) Observations de l'ODNI (annexe VI), p. 6 (en ce qui concerne l'*Intelligence Community directive 204*). Voir aussi la section 3 de la PPD-28.

([66]) Observations de l'ODNI (annexe VI), p. 6. Voir par exemple le document *NSA Civil Liberties and Privacy Office (NSA CLPO), NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333* du 7 octobre 2014. Voir également le document *ODNI Status Report 2014*. Pour les demandes d'accès relevant de l'article 702 du Foreign Intelligence Surveillance Act (FISA), les requêtes sont soumises aux procédures de minimisation approuvées par le tribunal de surveillance du renseignement extérieur (FISC). Voir le document *NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* du 16 avril 2014.

([67]) Voir le document *Signals Intelligence Reform, 2015 Anniversary Report*. Voir également les observations de l'ODNI (annexe VI), p. 6, 8, 9 et 11.

(71) En outre, les exigences fixées dans la PPD-28 selon lesquelles la collecte de renseignements doit toujours ([68]) être «aussi ciblée que possible» et la communauté du renseignement doit accorder une priorité élevée à la disponibilité d'autres informations et d'autres solutions appropriées et faisables ([69]), sont conformes à la règle générale selon laquelle la collecte ciblée est prioritaire par rapport à la collecte en vrac. Selon les assurances données par l'ODNI, ces exigences garantissent en particulier que la collecte en vrac n'est pas «massive» ni effectuée «à l'aveugle», et que l'exception ne se substitue pas à la règle ([70]).

(72) Si la PPD-28 explique que les composantes de la communauté du renseignement doivent parfois collecter des renseignements d'origine électromagnétique en vrac dans certaines circonstances, par exemple pour détecter et évaluer les nouvelles menaces ou les menaces émergentes, elle n'en impose pas moins à ces composantes de donner la priorité à des solutions de substitution qui permettraient de mettre en œuvre un renseignement d'origine électromagnétique ciblé ([71]). Il s'ensuit que la collecte en vrac n'aura lieu que lorsque la collecte ciblée au moyen de discriminants — c'est-à-dire un identifiant associé à une cible spécifique (tel que l'adresse électronique ou le numéro de téléphone de la cible) — n'est pas possible «pour des raisons techniques ou opérationnelles» ([72]). Cela vaut tant pour la manière dont les renseignements d'origine électromagnétique sont collectés que pour les renseignements qui sont effectivement collectés ([72]).

(73) D'après les observations de l'ODNI, même lorsque la communauté du renseignement ne peut pas utiliser des identifiants spécifiques pour cibler la collecte, elle s'efforcera de réduire «autant que possible» le champ de la collecte. Afin de respecter ce principe, elle «applique des filtres et d'autres moyens techniques pour focaliser la collecte sur les dispositifs qui sont les plus susceptibles de contenir des informations présentant un intérêt pour le renseignement extérieur» [et elle répondra donc aux exigences élaborées par les décideurs politiques américains conformément au processus décrit ci-dessus, au considérant 70]. En conséquence, la collecte en vrac sera ciblée au moins de deux façons, comme indiqué ci-après. Premièrement, cette collecte portera toujours sur des objectifs liés au renseignement extérieur (par exemple, pour acquérir des renseignements d'origine électromagnétique sur les activités d'un groupe terroriste opérant dans une région donnée) et sera toujours focalisée sur les communications qui présentent un tel lien. Selon les assurances données par l'ODNI, cela est illustré par le fait que les «activités de renseignement d'origine électromagnétique menées par les États-Unis ne touchent qu'une faible partie des communications transitant sur internet» ([73]). Deuxièmement, les observations de l'ODNI expliquent que les filtres et autres moyens techniques utilisés seront conçus de manière à cibler la collecte «aussi précisément que possible» de façon à garantir que le volume de «données non pertinentes» soit réduit au minimum.

(74) Enfin, même dans les cas où les États-Unis jugent nécessaire de recueillir des renseignements d'origine électromagnétique en vrac, dans les conditions fixées aux considérants 70 à 73, la PPD-28 restreint l'utilisation de ces renseignements à une liste spécifique de six motifs de protection de la sécurité nationale, en vue de défendre la vie privée et les libertés civiles de toutes les personnes, quels que soient leur nationalité et leur lieu de résidence ([74]). Ces motifs autorisés comprennent des mesures visant à détecter et à neutraliser les menaces liées à

([68]) Voir note 63.

([69]) Il convient également de relever que, conformément à l'article 2.4 de l'E.O. 12333, les composantes de la communauté du renseignement «utilisent les techniques de collecte les moins intrusives possible parmi celles qui peuvent être mises en œuvre aux États-Unis». En ce qui concerne les limitations qui existent pour le remplacement de toutes les collectes en vrac par des collectes ciblées, voir les résultats d'une évaluation effectuée par le Conseil national de sécurité, rapportés par l'Agence des droits fondamentaux de l'Union européenne dans le document *Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU (2015)*, p. 18.

([70]) Observations de l'ODNI (annexe VI), p. 4.

([71]) Voir également la section 5(d) de la PPD-28, qui impose au DNI de fournir au président, en coordination avec les chefs des composantes compétentes de la communauté du renseignement et du bureau des politiques scientifiques et technologiques (*Office of Science and Technology Policy*), un «rapport évaluant la faisabilité de la création d'un logiciel qui permettrait à la communauté du renseignement de mettre en œuvre une acquisition de données ciblée plutôt qu'une collecte en vrac». Selon des informations publiques, ce rapport a conclu qu'«il n'existe pas de solution logicielle qui pourrait se substituer entièrement à la collecte en vrac pour détecter certaines menaces pour la sécurité nationale». Voir le document *Signals Intelligence Reform, 2015 Anniversary Report*.

([72]) Voir note 63.

([73]) Observations de l'ODNI (annexe VI). Cela répond spécifiquement à la préoccupation exprimée par les APD nationales dans leur avis sur le projet de décision d'adéquation. Voir l'avis n° 1/2016 du groupe de travail «article 29» sur la protection des données intitulé «*Avis 01/2016 concernant le "Bouclier vie privée UE-États-Unis" (Privacy Shield) Projet de décision d'adéquation*» (adopté le 13 avril 2016), p. 38 et la note 47 de bas de page.

([74]) Voir article 2 de la PPD-28.

l'espionnage, au terrorisme et aux armes de destruction massive, les menaces pour la cybersécurité, ainsi que les menaces contre les forces armées ou le personnel de l'armée et les menaces criminelles transnationales liées aux cinq autres motifs; ils seront réexaminés au moins une fois par an. Selon les observations des autorités américaines, les acteurs de la communauté du renseignement ont renforcé leurs pratiques et normes analytiques en matière d'interrogation de données de renseignement d'origine électromagnétique non évaluées de façon à se conformer à ces exigences; l'utilisation de questions ciblées garantit que seules les informations dont on estime qu'elles présentent un intérêt potentiel du point de vue du renseignement sont soumises pour examen aux analystes ([75]).

(75) Ces restrictions sont particulièrement appropriées pour les données à caractère personnel transférées dans le cadre du bouclier de protection des données UE-États-Unis, en particulier dans le cas où la collecte de données à caractère personnel devrait intervenir à l'extérieur des États-Unis, notamment lors de leur transit sur les câbles transatlantiques de l'Union vers les États-Unis. Comme l'ont confirmé les autorités américaines dans les observations de l'ODNI, les limitations et garanties prévues par ce bouclier, y compris celles énoncées dans la PPD-28, s'appliquent à ce type de collecte ([76]).

(76) Même si les principes considérés ne sont pas formulés dans un langage juridique, ils rendent l'essence des principes de nécessité et de proportionnalité. La priorité est clairement donnée à une collecte ciblée, tandis que la collecte en vrac est limitée aux situations (exceptionnelles) dans lesquelles une collecte ciblée n'est pas possible pour des raisons techniques ou opérationnelles. Même lorsque la *collecte de données en vrac* ne peut être évitée, l'«utilisation» ultérieure de ces données du fait de l'accès accordé est *strictement limitée* à des fins spécifiques et légitimes tenant à la sécurité nationale ([77]).

(77) Les exigences considérées, se présentant sous la forme d'une directive adoptée par le président en sa qualité de premier magistrat, sont contraignantes pour l'ensemble des services de renseignement et ont été mises en œuvre plus avant au moyen de règles et de procédures des agences qui transposent les principes généraux en orientations spécifiques pour les opérations quotidiennes. En outre, si le Congrès n'est pas lui-même lié par la PPD-28, il a également pris des mesures pour veiller à ce que, aux États-Unis, la collecte des données à caractère personnel et l'accès à ces données s'effectuent de manière ciblée et non généralisée.

(78) Il ressort des informations disponibles, notamment des observations reçues de la part des autorités américaines, qu'une fois que les données ont été transférées à des organismes établis aux États-Unis et autocertifiés, dans le cadre du bouclier de protection des données UE-États-Unis, les agences américaines de renseignement ne pourront chercher ([78]) à avoir accès à des données à caractère personnel que si leur demande est conforme à la loi sur la surveillance et le renseignement étranger (FISA) ou qu'elle émane du Bureau fédéral d'enquête (FBI) agissant sur le fondement d'une lettre dite de sécurité nationale ([79]). Plusieurs bases juridiques existent dans le cadre du FISA, qui peuvent être utilisées pour collecter (et par la suite traiter) les données à caractère personnel de citoyens

([75]) Observations de l'ODNI (annexe VI), p. 4. Voir également la directive 203 des services de renseignements.

([76]) Observations de l'ODNI (annexe VI), p. 2. De même, les limitations prévues dans l'E.O. 12333 (par exemple, la nécessité que les informations collectées répondent aux priorités en matière de renseignement fixées par le président) s'appliquent.

([77]) Voir l'arrêt Schrems, point 93.

([78]) En outre, la collecte de données par le FBI peut également se fonder sur des autorisations en matière d'application de la législation (voir section 3.2 de la présente décision).

([79]) Pour de plus amples explications sur l'utilisation des lettres de sécurité nationale, voir les observations de l'ODNI (annexe VI), p. 13 à 14, et n. 38. Comme cela est indiqué dans ce document, le FBI ne peut recourir à ces lettres que pour demander des informations ne se rapportant pas au contenu qui 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. En ce qui concerne les transferts de données effectués en vertu du bouclier de protection des données UE-États-Unis, la base juridique la plus pertinente paraît être la loi sur la protection des communications électroniques [Electronic Communications Privacy Act (18 U.S.C., § 2709)], qui exige que toute demande d'informations ou d'enregistrement de transactions concernant les abonnés utilise un terme qui identifie spécifiquement une personne, une entité, un numéro de téléphone ou un compte.

européens transférées en vertu du bouclier de protection des données UE-États-Unis. En dehors de l'article 104 du FISA ([80]) qui porte sur la surveillance électronique classique des individus et de l'article 402 du FISA ([81]) relatif à l'installation de dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications, les deux principaux instruments sont l'article 501 du FISA [ex-article 215 du «PATRIOT ACT» américain (loi antiterroriste)] et l'article 702 du FISA ([82]).

(79) À cet égard, l'USA FREEDOM Act, qui a été adopté le 2 juin 2015, interdit la collecte en vrac d'enregistrements sur la base de l'article 402 du FISA (dispositifs d'écoute téléphonique et de suivi et d'enregistrement des communications), de l'article 501 du FISA (ex-article 215 du PATRIOT ACT) américain ([83]) et par le recours aux lettres de sécurité nationale, et demande à la place l'utilisation de «critères de sélection» spécifiques ([84]).

(80) Si le FISA contient d'autres bases juridiques permettant de mener des activités de renseignement nationales, notamment en matière de renseignements d'origine électromagnétique, l'évaluation de la Commission a montré qu'en ce qui concerne le transfert de données à caractère personnel dans le cadre du bouclier de protection des données UE-États-Unis, ces autorisations limitent de la même manière l'ingérence des autorités publiques à une collecte et un accès ciblés.

(81) C'est clairement le cas en ce qui concerne la surveillance électronique classique des personnes effectuée en application de l'article 104 du FISA ([85]). Pour ce qui est de l'article 702 du FISA, qui fournit la base pour deux importants programmes de renseignement menés par les agences américaines de renseignement (PRISM, UPSTREAM), des recherches sont effectuées de manière ciblée par le recours à différents critères de sélection qui identifient des moyens de communication spécifiques, comme l'adresse électronique ou le numéro de téléphone d'une cible, mais non des mots clés ni même les noms des personnes ciblées ([86]). Par conséquent, comme l'a fait

([80]) 50 U.S.C, § 1804. Si cette base juridique nécessite un exposé des faits et circonstances invoqués par le requérant à l'appui de sa conviction que (A) l'objet de la surveillance électronique est une puissance étrangère ou un agent d'une puissance étrangère, ce dernier 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)]. Il n'existe toutefois qu'un lien théorique avec les données à caractère personnel transférées en vertu du bouclier de protection des données UE-États-Unis, étant donné que l'exposé des faits doit également justifier la conviction que «chacune des installations ou chacun des lieux faisant l'objet de la surveillance électronique est utilisé ou sur le point d'être utilisé par une puissance étrangère ou un agent d'une puissance étrangère». En tout état de cause, pour faire appel à cette base juridique, il convient de recourir au tribunal de surveillance du renseignement extérieur qui appréciera, entre autres, si sur la base des faits soumis, il existe une cause probable qui fait que c'est en effet le cas.

([81]) 50 U.S.C. § 1842 avec § 1841(2) et sec. 3127 du titre 18. 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). Elle requiert une demande d'injonction du tribunal de surveillance du renseignement extérieur (ou d'un juge magistrat américain) et l'utilisation d'un terme de recherche spécifique au sens du § 1841(4), à savoir un terme 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.

([82]) Si l'article 501 du FISA (ex-article 215 du PATRIOT ACT américain) autorise le FBI à demander une ordonnance du tribunal en vue de la présentation de «faits tangibles» (en particulier des métadonnées de communications téléphoniques ainsi que des fichiers de sociétés) à des fins de renseignement extérieur, l'article 702 du FISA autorise des entités des services américains de renseignement à demander l'accès à des informations, notamment au contenu de communications sur internet, émanant du territoire des États-Unis mais ciblant certaines personnes non américaines à l'extérieur du territoire des États-Unis.

([83]) Sur la base de cette disposition, le FBI peut demander des «éléments tangibles» (par exemple des enregistrements, des pièces et des documents) après avoir démontré au tribunal de surveillance du renseignement extérieur qu'il a des motifs valables de penser qu'ils présentent un intérêt pour une enquête spécifique du FBI. Lorsqu'il procède à sa recherche, le FBI doit utiliser des critères spécifiques approuvés par le tribunal précité, qui permettent de déterminer s'il existe «une suspicion raisonnable claire» d'un lien avec une ou plusieurs puissances étrangères ou leurs agents impliqués dans le terrorisme international ou dans des actes de préparation dans ce domaine. Voir le rapport du Conseil de surveillance de la vie privée et des libertés civiles au titre de l'article 215, p. 59; CLPO/NSA, Rapport sur la transparence (The USA Freedom Act Business Records FISA Implementation) du 15 janvier 2016, p. 4 à 6.

([84]) Observations de l'ODNI (annexe VI), p. 13 (n. 38).

([85]) Voir note 81.

([86]) PCLOB; rapport sur l'article 702, p. 32 à 33 et autres références. Comme le prévoit son bureau chargé de la protection de la vie privée, l'autorité de sécurité nationale 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 l'Autorité nationale de sécurité; 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).

observer le conseil de surveillance de la vie privée et des libertés civiles (PCLOB), la surveillance effectuée 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 ([87]). En vertu d'une «clause de caducité», l'article 702 du FISA devra être réexaminé en 2017, date à laquelle la Commission devra réévaluer les garanties dont disposent les personnes concernées de l'Union.

(82) En outre, dans les observations qu'elles ont présentées, les autorités américaines ont donné à la Commission européenne des garanties expresses sur le fait que leurs services de renseignements ne se livraient pas à une surveillance systématique généralisée, y compris des citoyens européens ordinaires ([88]). En ce qui concerne les données à caractère personnel collectées à l'intérieur des États-Unis, cette déclaration est étayée par des données empiriques qui montrent que les *demandes d'accès* au moyen des lettres de sécurité nationale et dans le cadre du FISA, que ce soit sur le fondement d'une seule de ces bases ou des deux, ne concernent qu'un nombre relativement faible de cibles par rapport à l'ensemble des flux de données sur l'internet ([89]).

(83) En ce qui concerne *l'accès* aux données collectées et la *sécurité de ces données*, la PPD-28 prévoit que l'accès doit être limité au personnel habilité ayant besoin de connaître les informations en cause pour mener à bien sa mission et que les informations à caractère personnel doivent être traitées et stockées dans des conditions qui garantissent une protection adéquate et empêchent l'accès des personnes non habilitées, conformément aux garanties applicables en matière d'informations sensibles. Le personnel des services de renseignement reçoit une formation appropriée et adéquate en ce qui concerne les principes énoncés dans la PPD-28 ([90]).

(84) Enfin, en ce qui concerne le *stockage* et la *diffusion* ultérieure des données à caractère personnel concernant des personnes de l'Union collectées par les autorités américaines de renseignement, la PPD-28 prévoit que toute personne (y compris les personnes non américaines) doit être traitée avec respect et dignité, que toute personne possède des intérêts légitimes en matière de vie privée dans le cadre du traitement de ses informations personnelles et que les entités des services de renseignements doivent donc mettre en place des politiques offrant des garanties appropriées pour ce type de données, qui soient raisonnablement conçues afin de limiter le plus possible la diffusion et la conservation de ces données ([91]).

([87]) PLCOB; rapport sur l'article 702, p. 111. Voir également les observations de l'ODNI (annexe VI), p. 9 («La collecte effectuée en application de l'article 702 du [FISA] n'est pas massive et systématique; elle est étroitement axée sur le recueil de renseignements extérieurs provenant de cibles légitimes identifiées individuellement») et p. 13, n. 36 (avec référence à un avis de 2014 du tribunal de surveillance du renseignement extérieur). Voir CLPO/NSA (NSA's Implementation of Foreign Intelligence Act Section 702 du 16 avril 2014). Même dans le cas d'UPSTREAM, l'autorité nationale de sécurité ne peut demander que l'interception de communications électroniques en direction, à partir de ou concernant des sélecteurs.

([88]) Voir les observations de l'ODNI (annexe VI, p. 18; voir également p. 6), selon lesquelles les procédures applicables mettent en évidence une volonté claire d'empêcher une collecte arbitraire et systématique de renseignements d'origine électromagnétique et d'appliquer, au plus haut niveau de l'administration, le principe du caractère raisonnable.

([89]) Voir le rapport du 22 avril 2015 sur la transparence en matière statistique en ce qui concerne le recours aux autorités chargées de la sécurité nationale. Pour ce qui est du flux global de données sur l'internet, voir, par exemple, Agence des droits fondamentaux, Surveillance par les services de renseignement: garanties et moyens de recours dans l'Union européenne (2015), p. 15 et 16. En ce qui concerne le programme UPSTREAM, selon un avis de 2011 déclassifié du tribunal de surveillance du renseignement extérieur, plus de 90 % des communications électroniques obtenues dans le cadre de l'article 702 du FISA provenaient du programme PRISM et moins de 10 % d'UPSTREAM. Voir l'avis du tribunal de surveillance du renseignement extérieur de 2011[Memorandum Opinion 2011 WL 10945618 (FISA CT.du 3 octobre 2011)], n. 21 disponible à l'adresse suivante: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

([90]) Voir article 4(a)(ii) de la PPD-28. Voir également le document de l'ODNI de juillet 2014, p. 5, intitulé «Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy directive 28» (Garantir à toutes les personnes la protection des informations à caractère personnel les concernant: rapport d'avancement sur l'élaboration et la mise en œuvre des procédures dans le cadre de la directive présidentielle nº 28), selon lequel les politiques menées par les différentes entités des services de renseignement devraient renforcer les pratiques et normes analytiques actuelles par lesquelles les analystes doivent chercher à structurer les demandes ou d'autres termes et techniques d'interrogation en vue d'identifier les informations en matière de renseignement pertinentes pour une mission valable dans le domaine du renseignement ou de l'application de la loi; axer les requêtes concernant des personnes sur les catégories d'informations relevant d'un besoin de renseignement extérieur ou d'application de la loi; et réduire au maximum l'examen des informations à caractère personnel sans pertinence pour le renseignement extérieur ou l'application de la loi. Voir par exemple CIA, Activités de renseignement d'origine électromagnétique, p. 5; FBI, Politiques et procédures dans le cadre de la PPD-28, p. 3. Selon le rapport d'avancement de 2016 sur la réforme des activités de renseignement d'origine électromagnétique, les entités des services de renseignement (dont le FBI, la CIA et la NSA) ont pris des mesures pour sensibiliser leur personnel aux exigences de la PPD-28 en mettant en place de nouvelles politiques de formation ou en modifiant les politiques existantes en la matière.

([91]) D'après les observations de l'ODNI, ces restrictions s'appliquent indépendamment de la question de savoir si les informations ont été recueillies en vrac ou au moyen d'une collecte ciblée, et quelle que soit la nationalité de la personne concernée.

(85) Les autorités américaines ont expliqué que cette exigence concernant le caractère raisonnable implique que les entités des services de renseignement ne seront pas tenues d'adopter «toute mesure théoriquement envisageable» mais devront trouver un équilibre entre leurs efforts visant à protéger les intérêts légitimes relatifs au respect de la vie privée et des libertés civiles et les nécessités pratiques liées aux activités de renseignement électromagnétique ([92]). À cet égard, les personnes non américaines seront traitées de la même façon que les personnes américaines, sur la base des procédures approuvées par le procureur général ([93]).

(86) D'après ces règles, la conservation des données est généralement limitée à une période maximale de cinq ans, à moins qu'il ne soit établi spécifiquement par la législation ou décidé expressément par le directeur de l'Agence nationale du renseignement après évaluation minutieuse des problèmes de protection de la vie privée, en tenant compte de l'avis du délégué à la protection des libertés civiles de l'ODNI ainsi que des responsables chargés de la protection de la vie privée et des libertés civiles au sein des agences, que leur conservation prolongée répond aux intérêts de sécurité nationale des États-Unis ([94]). La diffusion est limitée aux cas dans lesquels ces informations présentent un intérêt pour l'objectif fondamental poursuivi par la collecte et, partant, répondent à un besoin autorisé de renseignement extérieur ou d'application de la législation ([95]).

(87) Selon les assurances données par le gouvernement américain, les informations à caractère personnel ne peuvent être diffusées au seul motif qu'il s'agit d'une personne non américaine et que les renseignements d'origine électromagnétique sur les activités habituelles d'un étranger ne peuvent être considérés comme des renseignements extérieurs susceptibles d'être diffusés ou conservés durablement en vertu de ce seul fait, à moins qu'ils ne répondent par ailleurs à des exigences admises en matière de renseignement extérieur ([96]).

(88) Sur la base de toutes les considérations qui précèdent, la Commission conclut que des règles sont en place aux États-Unis, qui visent à limiter toute ingérence, pour les besoins de la sécurité nationale, dans l'exercice des droits fondamentaux des personnes dont les données à caractère personnel sont transférées de l'Union européenne vers les États-Unis dans le cadre du bouclier de protection des données UE-États-Unis à ce qui est strictement nécessaire pour atteindre l'objectif légitime recherché.

(89) Comme l'a montré l'analyse ci-dessus, le droit américain garantit que les mesures de surveillance serviront uniquement à l'obtention de renseignements extérieurs, ce qui constitue un objectif stratégique légitime ([97]), et

([92]) Voir les observations de l'ODNI (annexe VI).

([93]) Voir l'article 4(a)(i) de la PPD-28 et la section 2.3 de l'E.O. 12333.

([94]) Voir article 4(a)(i) de la PPD-28. Observations de l'ODNI (annexe VI), p. 7. Par exemple, pour les informations à caractère personnel collectées dans le cadre de l'article 702 du FISA, les procédures de minimisation de la NSA approuvées par le FISC prévoient, en règle générale, que les métadonnées et le contenu non évalué de PRISM seront conservés pendant une période maximale de cinq ans, tandis que les données UPSTREAM seront conservées pendant deux ans maximum. La NSA se conforme à ces limites en matière de stockage au moyen d'un processus automatisé qui supprime les données collectées à la fin de la période de conservation respective. Voir procédures de minimisation de la NSA dans le cadre de l'article 702 de la FISA; article 7 et article 6(a)(1); document NSA CLPO «NSA's Implementation of Foreign Intelligence Surveillance Act Section 702» du 16 avril 2014. De même, la conservation dans le cadre de l'article 501 de la FISA (ex article 215 du PATRIOT ACT américain) est limitée à cinq ans, sauf si les données à caractère personnel font partie des informations en matière de renseignement extérieur dont la diffusion a été préalablement approuvée ou si le DOJ informe la NSA par écrit de ce que les archives doivent être conservées dans le cadre de litiges en cours ou attendus. Voir CLPO/NSA, Rapport sur la transparence (The USA Freedom Act Business Records FISA Implementation) du 15 janvier 2016.

([95]) En particulier, dans le cas de l'article 501 du FISA (ex-article 215 du PATRIOT ACT), la diffusion des informations à caractère personnel ne peut intervenir que pour des motifs liés à la lutte contre le terrorisme ou pour la présentation d'éléments de preuve dans un crime; dans le cas de l'article 702 du FISA, elle ne peut intervenir que pour un objectif valable de renseignement extérieur ou d'application de la loi. Voir le document NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 du 16 avril 2014; rapport sur la transparence (The USA Freedom Act Business Records FISA Implementation) du 15 janvier 2016. Voir également le document NSA Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333 du 7 octobre 2014.

([96]) Observations de l'ODNI (annexe VI), p. 7 (et référence à la directive 203 des services de renseignement).

([97]) La Cour de justice a précisé que la sécurité nationale constitue un but légitime. Voir l'arrêt Schrems, point 88. Voir également l'arrêt de la Cour dans l'affaire Digital Rights Ireland e.a., points 42 à 44 et 51, dans lequel la Cour de justice a considéré que la lutte contre les formes graves de criminalité, en particulier la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. En outre, contrairement à ce qui se passe dans le cas des enquêtes pénales qui concernent le plus souvent l'établissement de manière rétroactive des responsabilités et de la culpabilité pour des actes passés, les activités de renseignement sont souvent axées sur la prévention des menaces contre la sécurité nationale avant la survenue d'un événement néfaste. Par conséquent, les enquêtes menées dans le cadre de ces activités peuvent souvent être amenées à couvrir un éventail plus large d'acteurs éventuels («cibles») et une zone géographique plus étendue. Voir CEDH, arrêt Weber et Saravia c. Allemagne; décision du 29 juin 2006, requête n° 54934/00, points 105 à 118 (concernant la «surveillance à but stratégique»).

seront le plus spécifiques possible. En particulier, la collecte en vrac ne sera autorisée qu'à titre exceptionnel lorsqu'une collecte ciblée n'est pas réalisable, et sera assortie de garanties supplémentaires en vue de limiter au maximum la quantité de données collectées et l'accès ultérieur (qui devra être ciblé et autorisé uniquement à des fins spécifiques).

(90) Selon l'appréciation de la Commission, cette pratique est conforme à la norme fixée par la Cour de justice dans l'arrêt Schrems, selon lequel une réglementation comportant une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la charte doit imposer «un minimum d'exigences» ([98]) et «n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données» ([99]). Il n'y aura pas non plus collecte ou stockage illimité de données de toutes les personnes sans restrictions ni accès illimité. En outre, les observations présentées à la Commission, y compris l'assurance que les activités de renseignement d'origine électromagnétique des États-Unis ne concernent qu'une faible partie des communications transitant sur internet, excluent qu'il puisse y avoir accès «sur une base généralisée» ([100]) au contenu des communications électroniques.

3.1.2. Protection juridictionnelle effective

(91) La Commission a évalué à la fois les mécanismes de surveillance qui existent aux États-Unis en ce qui concerne toute ingérence des autorités américaines de renseignement dans les données à caractère personnel transférées vers les États-Unis et les voies de recours dont peuvent disposer les personnes concernées de l'Union pour obtenir réparation à titre individuel.

Surveillance

(92) L'ensemble des entités des services de renseignement des États-Unis est soumis à divers mécanismes de contrôle et de surveillance qui relèvent des trois pouvoirs de l'État. Il s'agit ainsi notamment d'organes internes et externes au sein du pouvoir exécutif, d'un certain nombre de commissions du Congrès et d'entités chargées d'une surveillance judiciaire portant spécifiquement sur les activités menées dans le cadre de la loi sur la surveillance et le renseignement étranger.

(93) Premièrement, les activités de renseignement des autorités américaines font l'objet d'une surveillance approfondie de la part du pouvoir exécutif.

(94) Selon la section 4(a)(iv) de la PPD-28, les politiques et les procédures appliquées par les acteurs des services de renseignement comprennent des mesures adéquates visant à faciliter la surveillance de la mise en œuvre des garanties protégeant les informations à caractère personnel; ces mesures doivent englober un audit périodique ([101]).

([98]) Arrêt Schrems, point 91, avec d'autres références.
([99]) Arrêt Schrems, point 93.
([100]) Voir l'arrêt Schrems, point 94.
([101]) Voir le document de l'ODNI intitulé «Safeguarding the Personal Information of all People: Status Report on the Development and Implementation of Procedures under Presidential Policy directive 28» (Garantir à toutes les personnes la protection des informations à caractère personnel les concernant: rapport d'avancement sur l'élaboration et la mise en œuvre des procédures dans le cadre de la directive présidentielle n° 28), p. 7. Voir par exemple CIA, Activités de renseignement d'origine électromagnétique, p. 6 (Contrôle concernant le respect des principes); FBI, Politiques et procédures dans le cadre de la PPD-28, section III (A)(4), (B)(4); NSA, PPD-28 Section 4 Procedures, 12 janvier 2015, Sections 8.1, 8.6(c).

(95) De multiples niveaux de supervision ont été instaurés à cet égard, notamment des délégués à la protection des libertés civiles ou de la vie privée, des inspecteurs généraux, le bureau de l'ODNI chargé des libertés civiles et de la vie privée, le conseil de surveillance de la vie privée et des libertés civiles (PCLOB) et le conseil de surveillance du renseignement du président (PIOB). Le personnel de toutes les agences chargé du respect de la conformité participe au bon déroulement de ces fonctions de surveillance ([102]).

(96) Comme l'ont expliqué les autorités américaines ([103]), des *délégués à la protection des libertés civiles ou de la vie privée* investis de responsabilités en matière de surveillance sont en place dans différents services et agences de renseignement ([104]). 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 [et, dans certains cas, à l'instar de l'ODNI, ces délégués peuvent eux-mêmes avoir le pouvoir d'enquêter sur des réclamations ([105])]. Le chef du service/de l'agence doit quant à lui veiller à ce que le délégué reçoive toutes les informations et se voie accorder l'accès à tous les documents nécessaires pour pouvoir s'acquitter de ses fonctions. 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 ([106]). Selon l'appréciation des autorités nationales de protection des données, le contrôle interne exercé par les délégués à la protection des libertés civiles ou de la vie privée peut être considéré comme «assez solide», bien que, de leur point de vue, ces délégués ne jouissent pas du degré d'indépendance requis ([107]).

(97) En outre, chaque entité du secteur du renseignement compte son propre *inspecteur général* chargé, entre autres, de contrôler les activités de renseignement extérieur ([108]). Se trouve ainsi, au sein de l'ODNI, un bureau de l'inspecteur général doté de vastes attributions en ce qui concerne l'ensemble des services de renseignement et 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 ([109]). Les inspecteurs généraux sont des entités dont l'indépendance est inscrite dans la loi ([110]); 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 ([111]). Ils sont autorisés à avoir 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

([102]) À titre d'exemple, la NSA emploie plus de 300 agents chargés de vérifier le respect des principes au sein de la direction responsable de la conformité. Voir les observations de l'ODNI (annexe VI), p. 7.

([103]) Voir mécanisme de médiation (annexe III), section 6(b) (i) à (iii).

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

([105]) Selon les autorités américaines, si le bureau de l'ODNI chargé de la protection des libertés civiles et de la vie privée est saisi d'une réclamation, il se coordonnera également avec d'autres acteurs des services de renseignement pour réfléchir au traitement à réserver à cette réclamation au sein de ces services. Voir mécanisme de médiation (annexe III), section 6(b) (ii).

([106]) Voir 42 U.S.C. § 2000ee-1. (f)(1),(2).

([107]) Avis nº 1/2016 du groupe de travail «article 29» sur la protection des données intitulé «*Avis 01/2016 concernant le "Bouclier vie privée UE-États-Unis" — Projet de décision d'adéquation*» (adopté le 13 avril 2016), p. 41.

([108]) Observations de l'ODNI (annexe VI), p. 7. Voir par exemple NSA, PPD-28 Section 4 Procedures, 12 janvier 2015, Section 8.1; CIA, Activités de renseignement d'origine électromagnétique, p. 7 (Responsabilités).

([109]) Cet inspecteur général (IG) (la fonction a été créée en octobre 2010) est nommé par le président, et sa nomination est entérinée par le Sénat; il ne peut être révoqué que par le président et non par le directeur du renseignement national.

([110]) Ces 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 exemple loi sur l'inspecteur général de 1978, § 8 (IG du ministère de la défense); § 8E (IG du DOJ); § 8G (d)(2)(A),(B) (IG de la NSA); 50. U.S.C. § 403 q (b) (IG pour la CIA); Intelligence Authorization Act For Fiscal Year 2010, Section 405(f) (IG pour le secteur du renseignement). Selon l'appréciation des autorités nationales chargées de la protection des données, les inspecteurs généraux «rempliront vraisemblablement le critère relatif à l'indépendance organisationnelle telle que définie par la CJUE et la Cour européenne des droits de l'homme (CEDH), au moins à partir du moment où le nouveau processus de nomination s'applique à tous». Voir l'avis nº 1/2016 du groupe de travail «article 29» sur la protection des données intitulé «*Avis 01/2016 concernant le "Bouclier vie privée UE-États-Unis" — Projet de décision d'adéquation*» (adopté le 13 avril 2016), p. 40.

([111]) Voir les observations de l'ODNI (annexe VI), p. 7. Voir également la loi sur l'inspecteur général (Inspector General Act) de 1978, telle que modifiée, pub. L. 113-126 du 7 juillet 2014.

peuvent recueillir des témoignages ([112]). Si les inspecteurs généraux ne peuvent que formuler des recommandations non contraignantes sur l'adoption de mesures correctives, leurs rapports, notamment sur les mesures de suivi (ou leur absence) sont rendus publics et de surcroît transmis au Congrès qui peut, sur cette base, exercer sa fonction de contrôle ([113]).

(98) En outre, le *conseil de surveillance du droit au respect de la vie privée et des libertés civiles*, organe indépendant ([114]), relevant du pouvoir exécutif, composé d'un conseil de cinq membres ([115]) issus des deux grands partis et nommés par le président pour un mandat de six ans avec l'approbation du Sénat, 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 de l'action des services 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. Il reçoit des rapports des délégués à la protection des libertés civiles et de la vie privée de plusieurs agences/organes fédéraux ([116]); il peut leur adresser des recommandations et fait régulièrement rapport aux commissions du Congrès et au président ([117]). Le PCLOB est également chargé, dans les limites de son mandat, de préparer un rapport évaluant la mise en œuvre de la PPD-28.

(99) Enfin, les mécanismes de surveillance précités sont complétés par le *conseil de surveillance du renseignement* (Intelligence Oversight Board) créé au sein du conseil consultatif en matière de renseignement relevant du président, qui supervise le respect par les autorités américaines de renseignement de la Constitution et de toutes les règles applicables.

(100) Pour faciliter la surveillance, les entités des services de renseignement sont invitées à concevoir des systèmes d'information pour permettre le suivi, l'enregistrement et l'examen des demandes ou d'autres recherches d'informations à caractère personnel ([118]). Les organismes chargés des contrôles et du respect de la conformité contrôleront régulièrement les pratiques mises en place par les entités des services de renseignement en vue de protéger les informations à caractère personnel figurant dans les renseignements d'origine électromagnétique et le respect de ces procédures ([119]).

(101) Ces fonctions de contrôle sont en outre complétées par des exigences importantes en matière de rapport sur le non-respect de la conformité. En particulier, les procédures appliquées par les agences doivent garantir que lors de la survenue d'un problème notable de conformité concernant des données à caractère personnel d'une personne quelconque, quelle que soit sa nationalité, collectées au moyen de renseignements d'origine électromagnétique, ce problème sera rapidement signalé au responsable de l'entité du service de renseignement qui, à son tour, en informera le directeur du renseignement national qui, en vertu de la PPD-28, appréciera si des mesures correctives sont nécessaires ([120]). En outre, conformément à l'E.O. 12333, toutes les entités des services de renseignement sont tenues de faire rapport au conseil de surveillance du renseignement sur les incidents en matière de non-respect de la conformité ([121]). Ces mécanismes garantissent que le problème sera traité au plus haut niveau au

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

([113]) Voir les observations de l'ODNI (annexe VI), p. 7. Voir également la loi sur l'inspecteur général de 1978 (Inspector General Act), §§ 4(5), 5. Selon l'article 405(b)(3) et (4) de la loi «Intelligence Authorization Act For Fiscal Year 2010», Pub. L. 111-259 du 7 octobre 2010, l'inspecteur général pour le secteur du renseignement tiendra le directeur du renseignement national ainsi que le Congrès informés de la nécessité de mesures correctives et de l'avancement en la matière.

([114]) Selon l'évaluation des autorités nationales chargées de la protection des données, le PCLOB a, par le passé, fait la preuve qu'il jouissait de pouvoirs de décision indépendants. Voir l'avis n° 1/2016 du groupe de travail «article 29» sur la protection des données intitulé «*Avis 01/2016 concernant le "Bouclier vie privée UE-États-Unis" — Projet de décision d'adéquation*» (adopté le 13 avril 2016), p. 42.

([115]) En outre, le PCLOB emploie quelque 20 agents statutaires. Voir https://www.pclob.gov/about-us/staff.html.

([116]) 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.

([117]) Voir 42 U.S.C. § 2000ee. Voir également mécanisme de médiation (annexe III), section 6(b) (iv). Entre autres, le PCLOB est tenu de faire rapport lorsqu'une agence relevant du pouvoir exécutif refuse de suivre ses conseils.

([118]) Voir le document de l'ODNI intitulé «Safeguarding the Personal Information of all People: Status Report on the Development and Implementation of Procedures under Presidential Policy directive 28» (Garantir à toutes les personnes la protection des informations à caractère personnel les concernant: rapport d'avancement sur l'élaboration et la mise en œuvre des procédures dans le cadre de la directive présidentielle n° 28), p. 7 et 8.

([119]) Ibidem, p. 8. Voir également les observations de l'ODNI (annexe VI), p. 9.

([120]) Voir le document de l'ODNI intitulé «Safeguarding the Personal Information of all People: Status Report on the Development and Implementation of Procedures under Presidential Policy directive 28» (Garantir à toutes les personnes la protection des informations à caractère personnel les concernant: rapport d'avancement sur l'élaboration et la mise en œuvre des procédures dans le cadre de la directive présidentielle n° 28), p. 7. Voir, par exemple, NSA, PPD-28 Section 4 Procedures, 12 janvier 2015, sections 7.3, 8.7(c),(d); FBI, Politiques et procédures dans le cadre de la PPD-28, section III.(A)(4), (B)(4); document de la CIA, p. 6: Signals Intelligence Activities (Activités des services de renseignement d'origine électromagnétique), p. 6 (Contrôle concernant le respect des principes) et p. 8 (Responsabilités).

([121]) Voir l'article 1.6(c) de l'E.O. 12333.

sein des services de renseignement. Lorsque le problème concerne un ressortissant non américain, le directeur du renseignement national, en concertation avec le secrétaire d'État et le chef du service ou de l'agence notifiante, décide s'il convient de prendre des mesures pour informer le gouvernement étranger concerné, dans le respect de la protection des sources, des méthodes et du personnel des États-Unis ([122]).

(102) Deuxièmement, outre ces mécanismes de contrôle au sein du pouvoir exécutif, le Congrès américain, en particulier les *commissions du renseignement et judiciaires de la Chambre des représentants et du Sénat*, exerce des responsabilités de surveillance à l'égard de toutes les activités du renseignement extérieur américain, y compris le renseignement d'origine électromagnétique. 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» ([123]). 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» ([124]). Les membres de ces commissions ont accès à des informations classifiées et aux méthodes et programmes de renseignement ([125]).

(103) Des lois ultérieures ont étendu et précisé les obligations de rendre compte, tant pour les composantes des services de renseignement que pour les inspecteurs généraux et le procureur général (*Attorney General*). Par exemple, le FISA exige que le ce dernier «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 ([126]). Elle impose en outre au gouvernement d'adresser aux commissions du Congrès «un exemplaire de chaque décision, ordonnance ou avis émis par le tribunal de la surveillance du renseignement extérieur (FISC) ou la cour révisant les décisions en matière de surveillance du renseignement extérieur (FISCR), contenant une interprétation ou une explication du sens ou de l'intention» des dispositions du FISA. En particulier, en ce qui concerne le contrôle visé à l'article 702 du FISA, la surveillance 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 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 ([127]), 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, y compris des procédures conçues pour veiller à ce que cette collecte serve un objectif valable de renseignement extérieur ([128]). Le Congrès reçoit également des rapports établis par les inspecteurs généraux qui sont autorisés à évaluer dans quelle mesure les agences respectent les procédures de ciblage et de «minimisation» et les orientations du procureur général.

(104) Selon l'USA FREEDOM Act de 2015, le gouvernement américain est tenu de communiquer 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 ([129]). Cet acte législatif exige également par ailleurs la communication publique d'informations sur le

([122]) Article 4(a)(iv) de la PPD-28.
([123]) Voir article 501(a)(1) [50 U.S.C. § 413(a)(1)]. Cette disposition contient les exigences générales concernant la surveillance incombant au Congrès en matière de sécurité nationale.
([124]) Voir article 501(b) [50 U.S.C. § 413(b)].
([125]) Voir article 501(c) [50 U.S.C. § 413(d)].
([126]) Voir 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Voir 50 U.S.C. § 1881f.
([128]) Voir 50 U.S.C. § 1881a(l)(1).
([129]) Voir l'USA FREEDOM Act de 2015, Pub. L. No. 114-23, article 602(a). 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 «terme sélectionné 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».

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) ([130]).

(105) Troisièmement, les activités de renseignement menées par les autorités américaines sur la base du FISA permettent la révision, et dans certains cas une autorisation préalable des mesures, par le *tribunal FISA* (FISC) ([131]), un tribunal indépendant ([132]) dont les décisions peuvent être contestées devant la cour révisant les décisions en matière de surveillance du renseignement extérieur (FISCR) ([133]) et, en dernier recours, devant la Cour suprême des États-Unis ([134]). En cas d'autorisation préalable, les autorités qui en font la demande (FBI, NSA, CIA, etc.) devront présenter un projet de demande aux avocats du *National Security Department* du ministère de la justice, qui l'examineront et, le cas échéant, demanderont des informations supplémentaires ([135]). Une fois la demande finalisée, elle doit être approuvée par le procureur général, le procureur général adjoint ou l'assistant du procureur général pour la sécurité nationale ([136]). Le ministère de la justice présentera ensuite la demande au FISC, qui évaluera cette dernière et adoptera un premier avis sur la marche à suivre ([137]). Lorsqu'une audience a lieu, le FISC a la capacité de recueillir des témoignages pouvant inclure des conseils d'experts ([138]).

(106) Le FISC (de même que la FISCR) reçoit l'appui d'un panel permanent de cinq personnes qui ont une expertise en matière de sécurité nationale et de libertés civiles ([139]). Le tribunal désignera 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 ([140]). Cette possibilité garantira 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* ([141]).

([130]) USA FREEDOM Act, articles 602(a), 603(a).

([131]) Pour certains types de surveillance, il est possible qu'un juge magistrat américain désigné publiquement par le juge en chef des États-Unis (*Chief Justice*) ait le pouvoir d'entendre les demandes et d'émettre des ordonnances.

([132]) Le FISC se compose de 11 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 article 103 du FISA [50 U.S.C. § 1803 (a)]; PCLOB, rapport sur l'article 215, p. 174 à 187. Les juges sont assistés de référendaires expérimentés qui constituent le personnel juridique du tribunal et préparent les analyses juridiques des demandes de collecte. Voir PCLOB, rapport sur l'article 215, p. 178; 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 et 3.

([133]) La FISCR est composée de trois juges nommés par le juge en chef des États-Unis et recrutés dans les tribunaux de district ou courts d'appel américains, en service pour un mandat de sept ans échelonné. Voir article 103 du FISA [50 U.S.C. § 1803 (b)].

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

([135]) Par exemple, des informations factuelles complémentaires concernant l'objet de la surveillance, des informations techniques relatives à la méthode de surveillance ou des garanties sur le mode d'obtention des informations seront utilisées et divulguées. Voir PCLOB, rapport sur l'article 215, p. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) Le FISC peut approuver la demande, vouloir des informations supplémentaires, constater la nécessité d'une audience ou communiquer un rejet éventuel de la demande. Sur la base de cette position préliminaire, le gouvernement présentera sa demande finale. Celle-ci peut être sensiblement modifiée par rapport à la demande initiale, eu égard aux commentaires préliminaires formulés par le juge. Bien qu'un pourcentage élevé de demandes finales soient approuvées par le FISC, une grande partie d'entre elle contient des modifications notables par rapport à la demande initiale, par exemple 24 % des demandes approuvées pour la période comprise entre juillet et septembre 2013. Voir PCLOB, rapport sur l'article 215, p. 179; lettre Walton, p. 3.

([138]) Voir PCLOB, rapport sur l'article 215, p. 179, n. 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Cette nouvelle législation a mis en œuvre des recommandations émises par le PCLOB visant à créer un pool d'experts en matière de protection de la vie privée et des libertés civiles, pouvant agir en tant qu'*amicus curiae* et fournir au tribunal des arguments juridiques visant à promouvoir la protection de la vie privée et des libertés civiles. Voir PCLOB, rapport sur l'article 215, p. 183 à 187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Selon les informations fournies par l'ODNI, ces nominations ont déjà eu lieu. Voir «*Signals Intelligence Reform*», *Progress Report* de 2016.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) En ce qui concerne les deux autorisations légales de surveillance au titre du FISA qui ont une importance majeure pour les transferts de données dans le cadre du bouclier de protection des données UE-États-Unis, la surveillance exercée par le FISC n'est pas la même.

(108) À l'article 501 du FISA ([142]), qui permet la collecte de «tout élément matériel (y compris des livres, des enregistrements, des documents papier, ou d'autres articles)», la demande du FISC doit contenir une déclaration des faits montrant qu'il existe des motifs raisonnables de considérer que les éléments matériels demandés sont pertinents aux fins d'une enquête autorisée (autre qu'une évaluation de menace), menée pour obtenir des informations sur le renseignement extérieur ne se rapportant pas à une personne américaine ou pour se protéger du terrorisme international ou des activités clandestines de renseignement. De plus, la demande doit contenir une liste des procédures de minimisation adoptées par le procureur général pour la rétention et la diffusion des renseignements collectés ([143]).

(109) Inversement, selon l'article 702 du FISA ([144]), le FISC n'autorise pas de mesures de surveillance individuelle, mais plutôt des programmes de surveillance (comme PRISM ou UPSTREAM) sur la base de certifications annuelles préparées par le procureur général et le directeur du renseignement national (DNI). 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 en matière de renseignement extérieur ([145]). Ce ciblage est effectué par la NSA en deux étapes. Premièrement, les analystes de la NSA recenseront 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. Deuxièmement, 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 ([146]), 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) ([147]). Comme indiqué, les certifications qui doivent être approuvées par le FISC ne contiennent pas d'informations sur les personnes à cibler individuellement mais déterminent plutôt des catégories d'informations en matière de renseignement extérieur ([148]). Même si le FISC n'évalue pas, à l'aune d'une cause ou de tout autre critère, si les personnes sont correctement ciblées pour se procurer des informations en matière de renseignement extérieur ([149]), son contrôle s'étend à la condition qu'«un objectif important de l'acquisition soit d'obtenir des informations en matière de renseignement extérieur» ([150]). En effet, selon l'article 702 du FISA, la NSA n'est autorisée à collecter des communications de personnes non américaines hors des États-Unis que s'il existe des motifs raisonnables de penser qu'un moyen de communication spécifique est utilisé pour communiquer des informations en matière de renseignement extérieur (par exemple liées au terrorisme international, à la prolifération nucléaire ou à des cyberactivités nuisibles). Les décisions prises en la matière sont susceptibles d'un recours juridictionnel ([151]). Les certifications doivent également prévoir des procédures de ciblage et de minimisation ([152]). Le procureur général et le directeur de l'Agence nationale du

([142]) 50 U.S.C. § 1861.
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) Voir PCLOB, rapport sur l'article 702, p. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Selon le PCLOB, ces catégories ont concerné jusqu'à présent essentiellement le terrorisme international et des thèmes comme l'acquisition d'armes de destruction massive. Voir PCLOB, rapport sur l'article 702, p. 25.
([149]) Voir PCLOB, rapport sur l'article 702, p. 27.
([150]) 50 U.S.C. § 1881a.
([151]) «Liberty and Security in a Changing World», Rapport et recommandations du groupe de révision du Président sur le renseignement et les technologies de communication, 12 décembre 2013, p. 152.
([152]) 50 U.S.C. § 1881a (i).

renseignement vérifient le respect des normes et les agences ont l'obligation de rapporter tout cas de non-respect au FISC ([153]) (ainsi qu'au Congrès et au PIOB), qui peut modifier l'autorisation sur cette base ([154]).

(110) De plus, pour augmenter l'efficacité de la surveillance exercée par le FISC, l'administration américaine a convenu de mettre en œuvre une recommandation du PCLOB visant à fournir au FISC les documents relatifs aux décisions de ciblage relevant de l'article 702, y compris un échantillon aléatoire de feuillets d'assignation, de manière que le FISC soit en mesure d'évaluer comment l'obligation en matière de renseignement extérieur est remplie en pratique ([155]). Parallèlement, l'administration américaine a accepté et pris des mesures pour réviser les procédures de ciblage de la NSA, afin qu'une meilleure justification documentaire soit fournie concernant les motifs des décisions de ciblage sur le renseignement extérieur ([156]).

Recours individuels

(111) Plusieurs voies de recours sont disponibles en droit américain pour les personnes de l'Union européenne concernées par les données à caractère personnel, lorsqu'elles craignent que ces données aient été traitées (collectées, évaluées, etc.) par des entités américaines du secteur du renseignement et, si tel est le cas, lorsqu'elles veulent s'assurer que les limitations en vigueur en droit américain ont été respectées. Ces limitations portent essentiellement sur trois domaines: ingérences au titre de la FISA, accès illégal intentionnel à des données à caractère personnel par des fonctionnaires de l'État, et accès à des informations au titre de la loi sur la liberté de l'information (FOIA) ([157]).

(112) Premièrement, le FISA prévoit un certain nombre de recours, également accessibles aux personnes non américaines, pour contester la surveillance électronique illégale ([158]). Les personnes concernées peuvent notamment: 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 ([159]); poursuivre des fonctionnaires de l'État américain à titre personnel («sous l'apparence du droit») pour obtenir des dommages et intérêts ([160]); et 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 ([161]).

(113) Deuxièmement, le gouvernement américain a communiqué à la Commission un certain nombre de voies de recours que les personnes de l'Union européenne concernées par les données à caractère personnel pourraient utiliser pour former un recours en justice contre des fonctionnaires de l'État en raison d'un accès ou d'un usage

([153]) La disposition 13, point b), du règlement de procédure du FISC impose au gouvernement de présenter une note écrite au tribunal dès qu'il découvre qu'une autorisation ou une approbation accordée par le tribunal a été appliquée de manière non conforme à cette autorisation ou approbation, ou au droit en vigueur. Elle exige en outre que le gouvernement notifie au tribunal par écrit les faits et circonstances concernant ce non-respect. Généralement, le gouvernement présentera une note finale au titre de cette disposition, point a), lorsque les faits concernés seront connus et lorsque toute collecte non autorisée aura été détruite. Voir lettre Walton, p. 10.

([154]) 50 U.S.C. § 1881 (l). Voir également PCLOB, rapport sur l'article 702, p. 66 à 76; document NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act, article 702, du 16 avril 2014. La collecte de données personnelles à des fins de renseignement au titre de l'article 702 du FISA fait l'objet d'une surveillance tant interne qu'externe au sein du pouvoir exécutif. Entre autres, la surveillance interne inclut des programmes internes sur le respect des normes, visant à évaluer et à surveiller le respect des procédures de ciblage et de minimisation, à rapporter les cas de non-respect, internes ou externes, à l'ODNI, au ministère de la justice, au Congrès et au FISC; et à adresser des réexamens annuels à ces mêmes organes. En ce qui concerne la surveillance externe, elle consiste principalement en des examens de ciblage et de minimisation menés par l'ODNI, le DOJ et les inspecteurs généraux, qui à leur tour font rapport au Congrès et au FISC, y compris sur les cas de non-respect. Les cas de non-respect importants doivent être signalés au FISC immédiatement, les autres doivent l'être dans un rapport trimestriel. Voir PCLOB, rapport sur l'article 702, p. 66 à 77.

([155]) PCLOB, «*Recommendations Assessment Report*» du 29 janvier 2015, p. 20.

([156]) Ibidem, p. 16.

([157]) En outre, l'article 10 du Classified Information Procedures Act (loi sur les procédures relatives aux informations classifiées) dispose que, dans toute procédure au cours de laquelle les États-Unis doivent démontrer que les pièces constituent des informations classifiées (par exemple parce qu'elles nécessitent une protection contre la divulgation non autorisée pour des raisons de sécurité nationale), les États-Unis informent la partie défenderesse des éléments des pièces sur lesquels ils peuvent raisonnablement s'appuyer pour démontrer le caractère classifié d'un élément lié à l'infraction.

([158]) Voir à ce sujet les observations de l'ODNI (annexe VI), p. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

illégal de données à caractère personnel, y compris à des fins prétendues de sécurité nationale [à savoir le Computer Fraud and Abuse Act ([162]); le Electronic Communications Privacy Act ([163]); et le Right to Financial Privacy Act ([164])]. Tous ces motifs de recours 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) ([165]). Une possibilité plus générale de recours est contenue dans l'Administrative Procedure Act (5 U.S.C. § 702), 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. 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 ([166]).

(114) Enfin, le gouvernement américain a décrit le FOIA comme un moyen pour les personnes non américaines de demander l'accès aux archives des organismes fédéraux, notamment lorsqu'elles contiennent les données à caractère personnel de la personne concernée ([167]). Eu égard à son orientation, le FOIA ne prévoit pas de voie de recours pour des actions individuelles contre les ingérences proprement dites en matière de données à caractère personnel, même s'il pourrait en principe permettre aux personnes d'avoir accès aux informations pertinentes détenues par les agences nationales du renseignement. Même à cet égard, les possibilités semblent limitées, car les agences peuvent retenir des informations qui relèvent d'une liste d'exceptions, notamment l'accès aux informations classifiées de sécurité nationale et aux informations concernant les enquêtes menées par les services répressifs ([168]). Toutefois, le recours à ces exceptions par les agences nationales de renseignement peut être contesté par des personnes physiques, qui sont en mesure de former un recours à la fois administratif et juridictionnel.

(115) Alors que les personnes physiques, notamment les personnes concernées de l'Union européenne, disposent donc d'un certain nombre de voies de recours lorsqu'elles ont fait l'objet d'une surveillance (électronique) illégale à des fins de sécurité nationale, il est également clair qu'au moins quelques bases juridiques pouvant être utilisées par les services de renseignement américains (comme l'E.O. 12333) ne sont pas couvertes. De plus, même lorsque des possibilités de recours juridictionnel existent en principe pour des personnes non américaines, comme par exemple pour la surveillance FISA, les moyens d'action sont limités ([169]) et les réclamations introduites par des personnes physiques (même américaines) seront déclarées irrecevables lorsqu'elles ne peuvent démontrer leur qualité pour agir ([170]), ce qui restreint l'accès aux juridictions ordinaires ([171]).

(116) Afin de fournir des voies de recours supplémentaires à toutes les personnes de l'Union européenne concernées, le gouvernement a décidé de créer un nouveau mécanisme de médiation tel que décrit dans la lettre adressée à la Commission par le secrétaire d'État américain, qui figure à l'annexe III de la présente décision. Ce mécanisme repose sur la désignation, au titre de la PPD-28, d'un coordinateur chevronné (niveau de sous-secrétaire) au département d'État en tant que point de contact permettant aux gouvernements étrangers d'exprimer leurs préoccupations à propos des activités américaines de renseignement d'origine électromagnétique, mais la portée de ce mécanisme est beaucoup plus vaste que le concept initial.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) Observations de l'ODNI (annexe VI), p. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Il existe des législations analogues au niveau des États.
([168]) 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 l'affaire ACLU v. CIA, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Voir les observations de l'ODNI (annexe VI), p. 16. Selon les explications fournies, les procédures disponibles nécessitent soit l'existence d'un *dommage* (18 U.S.C. § 2712; 50 U.S.C. § 1810), soit la preuve que le *gouvernement envisage d'utiliser ou de divulguer à l'encontre d'une personne des informations* obtenues sur celle-ci par surveillance électronique ou par l'effet de cette surveillance, *dans une procédure judiciaire ou administrative* aux États-Unis (50 U.S.C. § 1806). Cependant, comme la Cour de justice l'a indiqué à diverses reprises, pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence. Voir l'arrêt Schrems, point 89, avec d'autres références.
([170]) Ce critère de recevabilité résulte de l'exigence *«case or controversy»* (une affaire ou un différend) figurant à l'article III de la Constitution américaine.
([171]) Voir l'affaire Clapper v. Amnesty International USA, 133 S.Ct. 1138, 1144 (2013). En ce qui concerne l'utilisation des LSN, la loi USA FREEDOM [articles 502(f)-503] dispose que les exigences de non-divulgation doivent être révisées à intervalles réguliers et que les *destinataires* des LSN doivent être informés lorsque l'obligation de non-divulgation cesse de s'appliquer aux faits [voir les observations de l'ODNI (annexe VI), p. 13]. Cependant, il n'est pas garanti ainsi que les personnes de l'Union européenne concernées sauront qu'elles ont fait l'objet d'une enquête.

(117) En particulier, selon les engagements pris par le gouvernement américain, le mécanisme du médiateur garantira que les réclamations individuelles sont traitées et analysées correctement, et que les personnes concernées se verront confirmer de manière indépendante que les lois américaines ont été respectées ou, en cas de violation desdites lois, que le manquement a été corrigé ([172]). Le mécanisme inclut le «médiateur du bouclier de protection des données», à savoir le sous-secrétaire et d'autres membres du personnel ainsi que d'autres organismes de surveillance pour contrôler les diverses entités du secteur du renseignement, sur la collaboration desquelles le médiateur s'appuiera pour traiter les réclamations. En particulier, lorsque la demande d'une personne porte sur la compatibilité de la surveillance avec le droit américain, le médiateur du bouclier de protection des données pourra s'appuyer sur des organismes de surveillance indépendants détenant des pouvoirs d'enquête (comme les inspecteurs généraux ou le PCLOB). Dans chaque cas, le secrétaire d'État veillera à ce que le médiateur ait les moyens de vérifier que sa réponse aux demandes individuelles est fondée sur toutes les informations requises.

(118) À l'aide de cette structure «composite», le mécanisme de médiation garantit une surveillance indépendante et un recours individuel. De plus, la coopération avec d'autres organismes de surveillance garantit un accès à l'expertise nécessaire. Enfin, en imposant au médiateur du bouclier de protection des données l'obligation de confirmer le respect du droit ou la correction d'un manquement au droit, le mécanisme reflète l'engagement pris globalement par le gouvernement américain de traiter les réclamations introduites par des personnes de l'Union européenne et d'y apporter une réponse.

(119) Premièrement, à la différence d'un mécanisme simple de gouvernement à gouvernement, le médiateur du bouclier de protection des données recevra des réclamations individuelles et répondra à ces dernières. Ces réclamations peuvent être adressées aux autorités de contrôle chargées, dans les États membres, de la surveillance des services de sécurité nationale et/ou du traitement des données à caractère personnel par les autorités publiques, lesquelles présenteront ces réclamations à un organisme européen centralisé à partir duquel ils seront réorientés vers le médiateur du bouclier de protection des données ([173]). Le bénéfice sera en réalité pour les personnes de l'Union européenne qui peuvent s'adresser à une autorité nationale géographiquement proche et communiquant dans leur langue. Il incombera à l'autorité en question de soutenir la personne concernée dans la présentation de sa demande au médiateur du bouclier de protection des données, de manière que la demande contienne les informations essentielles et puisse donc être considérée comme «complète». La personne n'est pas tenue de démontrer que ses données à caractère personnel ont été consultées dans les faits par le gouvernement américain au moyen d'activités de renseignement d'origine électromagnétique.

(120) Deuxièmement, le gouvernement américain s'engage à faire en sorte que, dans l'exercice de ses fonctions, le médiateur du bouclier de protection des données soit en mesure de s'appuyer sur la coopération avec d'autres mécanismes de surveillance et de contrôle de respect du droit existant dans la législation américaine. Cette situation concernera parfois les autorités nationales du renseignement, notamment lorsque la demande doit être interprétée comme relevant de l'accès aux documents au titre du Freedom of Information Act. Dans d'autres cas, en particulier lorsque les demandes portent sur la compatibilité de la surveillance avec le droit américain, ce type de coopération fera intervenir des organismes de surveillance indépendants (comme les inspecteurs généraux), ayant la responsabilité et le pouvoir de procéder à une enquête approfondie (notamment grâce à un accès à tous les documents utiles et à la possibilité de demander des informations et des déclarations), et mettra un terme au manquement ([174]). De plus, le médiateur du bouclier de la protection des données aura la possibilité de transmettre les cas au PCLOB afin qu'il les examine ([175]). Lorsqu'un non-respect des normes est détecté par l'un de ces organismes de surveillance, la composante concernée des services de renseignement sera tenue de corriger ce manquement, car seule cette démarche permettra au médiateur de fournir une réponse «positive» (indiquant que

([172]) Si le réclamant cherche à accéder à des documents détenus par les autorités publiques américaines, les règles et les procédures décrites dans le Freedom of Information Act s'appliquent. Il est notamment possible de former un recours juridictionnel (au lieu d'une surveillance indépendante) en cas de rejet de la demande, dans les conditions fixées par la FOIA.

([173]) Selon le mécanisme du médiateur (annexe III), section 4(f), le médiateur du bouclier de protection des données communiquera directement avec l'organe européen chargé du traitement de la réclamation individuelle, lequel sera à son tour chargé de communiquer avec la personne intéressée qui présente la demande. Même si les communications directes font partie du «processus sous-jacent» susceptible d'apporter la solution demandée (par exemple à une demande d'accès au titre du FOIA, voir section 5), ces communications auront lieu conformément aux procédures en vigueur applicables.

([174]) Voir mécanisme du médiateur (annexe III), section 2(a). Voir également les considérants 0-0.

([175]) Voir mécanisme du médiateur (annexe III), section 2(c). Selon les explications fournies par le gouvernement américain, le PCLOB révisera en permanence les politiques et les procédures des autorités américaines responsables de la lutte contre le terrorisme, ainsi que la mise en œuvre, afin de déterminer si leurs actions «assurent une protection adéquate de la vie privée et des libertés civiles et sont cohérentes par rapport aux lois, réglementations et politiques en vigueur concernant la vie privée et les libertés civiles». Cet organisme recevra et révisera également des rapports et d'autres informations transmises par des délégués à la protection des libertés civiles et de la vie privée et, le cas échéant, formulera des recommandations à leur égard concernant leurs activités.

tout manquement est donc corrigé) à la personne concernée, le gouvernement américain s'étant engagé à procéder de la sorte. Dans le cadre de la coopération, par ailleurs, le médiateur du bouclier de protection des données sera informé des résultats de l'enquête et sera en mesure de veiller à recevoir toutes les informations utiles à la préparation de sa réponse.

(121) Enfin, le médiateur du bouclier de protection des données sera indépendant des services américains de renseignement et ne recevra donc aucune instruction de leur part ([176]). Cet élément revêt une importance notable, car le médiateur devra «confirmer» que: i) la plainte été correctement analysée; et que ii) le droit américain pertinent, y compris les limites et les protections prévues à l'annexe VI, a été respecté ou, dans la négative, que le manquement a été corrigé. Afin de pouvoir fournir cette confirmation indépendante, le médiateur du bouclier de protection des données devra recevoir les informations nécessaires concernant l'enquête pour évaluer la précision de la réponse à la plainte. En outre, le secrétaire d'État s'est engagé à faire en sorte que le sous-secrétaire exerce la fonction de médiateur du bouclier de protection des données de manière objective et libre de toute influence susceptible d'avoir un effet sur la réponse fournie.

(122) Globalement, ce mécanisme est conçu pour que les réclamations individuelles soient examinées de manière approfondie et traitées, et que, dans le domaine de la surveillance au moins, il soit fait appel à des organes de surveillance indépendants ayant l'expertise et les pouvoirs d'enquête nécessaires, ainsi qu'à un médiateur qui sera en mesure d'exercer ses fonctions sans subir d'influence inappropriée, en particulier sur le plan politique. De plus, les personnes pourront introduire des réclamations sans devoir démontrer ni même fournir des éléments indiquant qu'elles ont fait l'objet d'une surveillance ([177]). Eu égard à cette situation, la Commission se félicite de voir qu'il existe des garanties adaptées et efficaces contre les abus.

(123) Sur la base de ce qui précède, la Commission conclut que les États-Unis garantissent une protection juridique effective contre les ingérences de la part de leurs services de renseignement dans les droits fondamentaux des personnes dont les données sont transférées de l'Union européenne vers les États-Unis au titre du bouclier de protection des données UE-États-Unis.

(124) À cet égard, la Commission prend note de l'arrêt de la Cour de justice dans l'affaire Schrems, selon lequel «une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte» ([178]). L'évaluation de la Commission a confirmé que de telles voies de droit sont prévues aux États-Unis, y compris par le biais de l'introduction du mécanisme de médiation. Le mécanisme du médiateur assure une surveillance indépendante fondée sur des pouvoirs d'enquête. Dans le cadre du suivi continu du bouclier de protection de la vie privée assuré par la Commission, notamment à l'aide du réexamen annuel conjoint auquel le médiateur prendra part également, l'efficacité de ce mécanisme sera réévaluée.

3.2. *Accès aux données et utilisation de celles-ci par les autorités publiques américaines aux fins de garantir l'application de la loi et à d'autres fins d'intérêt général*

(125) En ce qui concerne les ingérences dans les données à caractère personnel transférées au titre du bouclier de protection des données UE-États-Unis aux fins de garantir l'application de la loi, le gouvernement américain (par l'intermédiaire du ministère de la justice) a donné des garanties concernant les limitations et les protections en vigueur qui contiennent, selon l'évaluation de la Commission, un niveau de protection adéquat.

([176]) Voir l'affaire Roman Zakharov c. Russie, arrêt du 4 décembre 2015 (Grande Chambre), requête n° 47143/06, point 275 («s'il est en principe souhaitable que la fonction de contrôle soit confiée à un juge, le contrôle par un organe non judiciaire peut passer pour compatible avec la Convention dès lors que cet organe est indépendant des autorités qui procèdent à la surveillance et est investi de pouvoirs et attributions suffisants»).

([177]) Voir l'affaire Kennedy c. Royaume-Uni, arrêt du 18 mai 2010, requête n° 26839/05, point 167.

([178]) Arrêt Schrems, point 95. Comme le montrent clairement les points 91 et 96 de l'arrêt, le point 95 concerne le niveau de protection garanti dans l'ordre juridique de l'Union, auquel le niveau de protection assuré dans le pays tiers doit être «substantiellement équivalent». Selon les points 73 et 74 de l'arrêt, cela ne signifie pas que le niveau de protection ou les moyens auxquels le pays tiers a recours doivent être identiques, même si les moyens employés doivent s'avérer, en pratique, effectifs.

(126) Selon ces informations, en vertu du quatrième amendement à la Constitution américaine ([179]), les perquisitions et saisies effectuées par les autorités répressives nécessitent essentiellement ([180]) un mandat délivré par un tribunal sur une «présomption sérieuse». Dans les quelques cas exceptionnels et spécifiquement constatés où l'exigence de mandat ne s'applique pas ([181]), l'application de la législation est soumise à une mesure du «caractère raisonnable» ([182]). Le caractère raisonnable d'une perquisition ou saisie est «déterminé en évaluant, d'une part, la mesure dans laquelle elle fait intrusion dans la vie privée d'une personne et, de l'autre, la mesure dans laquelle elle est nécessaire pour mettre en avant les intérêts légitimes du gouvernement» ([183]). Plus généralement, le quatrième amendement garantit le droit à une vie privée et à une dignité, et protège contre des actes arbitraires et intrusifs de la part de fonctionnaires de l'État ([184]). Ces notions couvrent l'idée de la nécessité et de la proportionnalité dans le droit de l'Union. Lorsque l'autorité répressive n'a plus besoin d'utiliser les éléments saisis en tant que preuves, elle a l'obligation de les restituer ([185]).

(127) Le quatrième amendement ne s'applique pas aux personnes non américaines qui ne résident pas aux États-Unis, mais ces personnes bénéficient quand même indirectement de ses protections, étant donné que les données à caractère personnel sont détenues par des entreprises américaines, ce qui a pour effet que les autorités répressives sont en tout état de cause tenues de demander une autorisation judiciaire (ou au moins de respecter l'exigence du caractère raisonnable) ([186]). Certains actes législatifs ou réglementaires spéciaux et les lignes directrices du ministère de la justice (*Department of Justice Guidelines*) fournissent des protections supplémentaires, qui autorisent l'accès aux données aux fins de garantir le respect de la loi uniquement pour des motifs équivalents à la nécessité et à la proportionnalité (par exemple, en exigeant que le FBI utilise les méthodes d'enquête les moins intrusives pouvant être mises en œuvre, en tenant compte des incidences sur la protection de la vie privée et les libertés fondamentales) ([187]). Selon les observations du gouvernement américain, des protections identiques ou plus élevées 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) ([188]).

(128) Bien qu'une autorisation judiciaire préalable d'un tribunal ou d'un *grand jury* (jury institué par un juge ou un magistrat afin de mener l'instruction dans une affaire criminelle) ne soit pas requise dans tous les cas ([189]), le recours à des injonctions administratives est limité à des cas spécifiques et est soumis à un contrôle juridictionnel indépendant, tout du moins lorsque le gouvernement cherche à faire exécuter ces injonctions par la voie judiciaire ([190]).

([179]) Aux termes du quatrième amendement, «[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 enfreint, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans décrire spécifiquement le lieu à perquisitionner et les personnes ou objets à saisir». Seuls les juges (magistrats) sont habilités à délivrer des mandats de perquisition. Les mandats fédéraux relatifs à la reproduction d'informations stockées sur support électronique sont en outre régis par le point 41 du code fédéral de procédure pénale.

([180]) La Cour suprême a qualifié à plusieurs reprises d'exceptionnelles certaines perquisitions sans mandat. Voir par exemple les affaires Johnson v. United States, 333 U.S. 10, 14 (1948); McDonald v. United States, 335 U.S. 451, 453 (1948); Camara v. Municipal Court, 387 U.S. 523, 528-29 (1967); G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 355 (1977). De même, la Cour suprême rappelle régulièrement que «la règle constitutionnelle la plus élémentaire dans ce domaine veut que les perquisitions effectuées en dehors d'une procédure judiciaire, sans approbation préalable d'un juge ou d'un magistrat, ont *en soi* un caractère déraisonnable en vertu du quatrième amendement, qui prévoit uniquement quelques exceptions bien définies et spécifiquement constatées». Voir par exemple les affaires Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971); G.M. Leasing Corp. v. United States, 429 U.S. 338, 352-53, 358 (1977).

([181]) City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010).

([182]) Voir PCLOB, rapport sur l'article 215, p. 107, qui renvoie à l'affaire Maryland v. King, 133 S. Ct. 1958, 1970 (2013).

([183]) Voir PCLOB, rapport sur l'article 215, p. 107, qui renvoie à l'affaire Samson v. California, 547 U.S. 843, 848 (2006).

([184]) City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Voir par exemple l'affaire United States v Wilson, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Voir l'affaire Roman Zakharov c. Russie, arrêt du 4 décembre 2015 (grande chambre), requête n° 47143/06, point 269, selon lequel «l'obligation de présenter une autorisation d'interception au prestataire de services de communication avant d'obtenir l'accès aux communications d'une personne constitue l'une des protections importantes contre les abus des autorités répressives, puisqu'elle garantit qu'une autorisation en bonne et due forme est obtenue dans tous les cas d'interception».

([187]) Observations du ministère de la justice (annexe VII), p. 4, et les références qui y sont citées.

([188]) Observations du ministère de la justice (annexe VII), note 2 de bas de page.

([189]) Selon les informations reçues par la Commission, mis à part certains domaines qui ne sont sans doute pas pertinents pour les transferts de données au titre du bouclier de protection des données UE—États-Unis (par exemple, les enquêtes sur les fraudes dans le domaine des soins de santé, la maltraitance des enfants ou les affaires de substances contrôlées), cela concerne essentiellement un certain nombre d'autorités visées par l'*Electronic Communications Privacy Act* (ECPA), et plus précisément les demandes d'informations de base sur les abonnés, les sessions et la facturation [18 U.S.C. § 2703(c)(1), (2)] et les demandes d'accès au contenu des courriers électroniques datant de plus de 180 jours [18 U.S.C. § 2703(a), (b)]. Toutefois, dans ce dernier cas, l'intéressé doit en être informé et a donc la possibilité de contester la demande en justice. Voir aussi le résumé dans le document *DOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Ch. 3: The Stored Communications Act*, p. 115 à 138.

([190]) D'après les observations du gouvernement américain, 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. Voir les observations du ministère de la justice (annexe VII), p. 2.

(129) Il en va de même pour l'utilisation des injonctions administratives à des fins d'intérêt public. En outre, selon les observations reçues des autorités américaines, des limitations de fond similaires s'appliquent en ce sens que les agences ne peuvent demander à accéder qu'aux données se rapportant aux matières relevant de leur compétence et doivent respecter la norme du raisonnable.

(130) 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. Ces voies de recours, parmi lesquelles figurent notamment l'Administrative Procedure Act (loi de procédure administrative, 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.

(131) De manière générale, en vertu des dispositions relatives au contrôle juridictionnel de l'APA ([191]), 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 ([192]). 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» ([193]).

(132) Plus spécifiquement, le titre II de l'ECPA ([194]) 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 électronique stockées par des prestataires de services tiers ([195]). 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.

(133) Par ailleurs, en vertu du Freedom of Information Act (loi sur la liberté de l'information, FOIA, 5 U.S.C. § 552), toute personne a le droit d'obtenir l'accès aux documents des agences fédérales et, une fois épuisés tous les recours administratifs, de requérir l'application de ce droit devant un tribunal, sauf si ces documents échappent à la divulgation en vertu d'une dérogation ou d'exclusions spéciales de l'application de la loi ([196]).

([191]) 5 U.S.C. § 702.

([192]) 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.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701 à 2712.

([195]) 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.

([196]) 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)].

(134) 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) ([197]), le Computer Fraud and Abuse Act (loi relative à la fraude et aux abus informatiques) ([198]), le Federal Torts Claim Act (loi fédérale sur les actions pour cause d'infraction) ([199]), le Right to Financial Privacy Act (loi sur le droit à la protection des données personnelles à caractère financier) ([200]), et le FAIR Credit Reporting Act ([201]).

(135) La Commission conclut dès lors que les États-Unis disposent de règles visant à limiter toute entrave, à des fins répressives ([202]) ou à d'autres fins d'intérêt public, aux droits fondamentaux des personnes dont des données personnelles sont transférées de l'Union vers les États-Unis au titre du «bouclier vie privée» UE-U.S. à ce qui est strictement nécessaire pour atteindre l'objectif légitime en question, et garantissant une protection juridique efficace contre des ingérences de cette nature.

4. NIVEAU ADÉQUAT DE PROTECTION DANS LE CADRE DU BOUCLIER DE PROTECTION DES DONNÉES UE-ÉTATS-UNIS

(136) À la lumière de ces constatations, la Commission considère que les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées de l'Union européenne vers des organisations autocertifiées aux États-Unis dans le cadre du bouclier de protection des données UE-États-Unis.

(137) La Commission considère en particulier que les principes publiés par le ministère américain du commerce dans leur ensemble assurent un niveau de protection des données à caractère personnel qui est fondamentalement équivalent à celui garanti par les principes de base énoncés dans la directive 95/46/CE.

(138) En outre, l'application effective des principes est garantie par les obligations de transparence et l'administration du bouclier de protection des données par le ministère du commerce.

(139) De plus, la Commission considère que, pris dans leur ensemble, les mécanismes de surveillance et de recours prévus par le bouclier de protection des données permettent d'identifier et de sanctionner en pratique les infractions aux principes commises par des organisations figurant sur la liste des organisations adhérant au bouclier de protection des données et offrent aux personnes concernées des voies de droit afin d'avoir accès à des données à caractère personnel les concernant et, in fine, d'obtenir leur rectification ou leur suppression.

(140) Enfin, sur la base des informations disponibles concernant l'ordre juridique des États-Unis, y compris les observations et les engagements du gouvernement américain, la Commission considère que toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes dont les données sont transférées de l'Union européenne vers les États-Unis dans le cadre du bouclier de protection des données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérences de cette nature.

([197]) 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 le 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).

([198]) 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.

([199]) 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.

([200]) 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.

([201]) 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.

([202]) La Cour de justice a reconnu que l'application des lois constituait un objectif stratégique légitime. Voir l'arrêt dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland e.a., EU:C:2014:238, point 42. Voir aussi l'article 8, paragraphe 2, de la CEDH et l'arrêt de la Cour européenne des droits de l'homme dans l'affaire Weber et Saravia c. Allemagne, requête n° 54934/00, point 104.

(141) La Commission conclut que la situation est conforme aux exigences de l'article 25 de la directive 95/46/CE interprété à la lumière de la charte des droits fondamentaux de l'Union européenne, comme l'a expliqué la Cour de justice en particulier dans l'arrêt Schrems.

5. ACTION DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES ET INFORMATION DE LA COMMISSION

(142) Dans l'arrêt Schrems, la Cour de justice a précisé que la Commission n'est pas compétente pour restreindre les pouvoirs que les APD tirent de l'article 28 de la directive 95/46/CE (y compris le pouvoir de suspendre des transferts de données), dans le cas où une personne remet en cause, à l'occasion d'une demande au titre de cette disposition, la compatibilité d'une décision de la Commission constatant un niveau de protection adéquat avec le droit fondamental à la protection de la vie privée et à la protection des données personnelles ([203]).

(143) Pour contrôler efficacement le fonctionnement du bouclier de protection des données, la Commission devrait être informée par les États membres des mesures pertinentes prises par les APD.

(144) La Cour de justice a par ailleurs considéré que, conformément à l'article 25, paragraphe 6, second alinéa, de la directive 95/46/CE, les États membres et leurs organes doivent prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent, en principe, d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés dans le cadre d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité. En conséquence, une décision d'adéquation de la Commission adoptée conformément à l'article 25, paragraphe 6, de la directive 95/46/CE a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de surveillance indépendantes ([204]). Lorsqu'une telle autorité a été saisie d'une plainte concernant 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 et qu'elle estime que les griefs avancés sont fondés, 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 ([205]).

6. RÉEXAMEN PÉRIODIQUE DE LA CONSTATATION CONCERNANT LE NIVEAU ADÉQUAT DE LA PROTECTION

(145) Au regard du fait que le niveau de protection assuré par l'ordre juridique des États-Unis est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, vérifiera de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par le bouclier de protection des données UE-États-Unis sont toujours justifiées en fait et en droit. Une telle vérification s'impose, en tout état de cause, lorsque la Commission a connaissance d'informations faisant naître un doute justifié à cet égard ([206]).

(146) En conséquence, la Commission procédera à un suivi constant du cadre global pour le transfert de données à caractère personnel que constitue le bouclier de protection des données UE-États-Unis, ainsi que du respect, par les autorités américaines, des observations et des engagements contenus dans les documents joints à la présente décision. Pour faciliter ce processus, les États-Unis se sont engagés à informer la Commission de toute évolution importante de la législation américaine présentant un intérêt pour le bouclier de protection des données et concernant la protection des données et les limitations et garanties applicables à l'accès des autorités publiques aux données à caractère personnel. De plus, la présente décision sera soumise à un réexamen annuel conjoint, qui couvrira tous les aspects du fonctionnement du bouclier de protection des données UE-États-Unis, notamment l'usage fait des exceptions aux principes pour des raisons ayant trait à la sécurité nationale ou au respect de la législation. En outre, étant donné que la décision d'adéquation pourrait aussi être influencée par des évolutions juridiques dans le droit de l'Union, la Commission évaluera le niveau de protection assuré par le bouclier de protection des données après l'entrée en application du règlement général sur la protection des données.

(147) Pour l'exécution du réexamen annuel conjoint visé aux annexes I, II et VI, la Commission rencontrera le ministère du commerce et la FTC, accompagnés, s'il y a lieu, d'autres services et agences participant à la mise en œuvre des dispositions du bouclier de protection des données, ainsi que, pour les questions ayant trait à la sécurité nationale, des représentants de l'ODNI, d'autres composantes des services de renseignement et le médiateur. La participation à cette réunion sera ouverte aux APD de l'Union européenne et à des représentants du groupe de travail «article 29».

([203]) Arrêt Schrems, points 40 et suivants et points 101 à 103.
([204]) Arrêt Schrems, points 51, 52 et 62.
([205]) Arrêt Schrems, point 65.
([206]) Arrêt Schrems, point 76.

(148) Dans le cadre du réexamen annuel conjoint, la Commission demandera que le ministère américain du commerce fournisse des informations complètes sur tous les aspects utiles du fonctionnement du bouclier de protection des données UE-États-Unis, notamment les dossiers déférés au ministère du commerce par les APD et les résultats des contrôles de la conformité exécutés d'office. La Commission demandera également des explications sur toute question ou tout sujet concernant le bouclier de protection des données UE-États-Unis et son fonctionnement découlant de toute information disponible, notamment les rapports de transparence autorisés par l'USA FREEDOM Act, les rapports publics des services de renseignement nationaux américains, des APD ou de groupes privés, les reportages dans les médias ou toute autre source possible. De plus, afin de faciliter la tâche de la Commission à cet égard, les États membres devraient informer la Commission des cas dans lesquels les organismes chargés de faire respecter les principes aux États-Unis ne parviennent pas à s'acquitter de leur tâche et de tout élément indiquant que les actions des autorités publiques américaines responsables de la sécurité nationale ou de la prévention, de la détection, des enquêtes et des poursuites en matière d'infractions pénales n'assurent pas le niveau de protection requis.

(149) Sur la base du réexamen annuel conjoint, la Commission élaborera un rapport public qui sera présenté au Parlement européen et au Conseil.

7. SUSPENSION DE LA DÉCISION D'ADÉQUATION

(150) Lorsque, sur la base des vérifications ou de toute autre information disponible, la Commission parvient à la conclusion que le niveau de protection assuré par le bouclier de protection des données ne peut plus être considéré comme fondamentalement équivalent à celui qui est garanti dans l'Union européenne ou lorsque des éléments indiquent clairement que le respect effectif des principes aux États-Unis pourrait ne plus être assuré ou que les actions des autorités publiques américaines responsables de la sécurité nationale ou de la prévention, de la détection, des enquêtes et des poursuites en matière d'infractions pénales n'assurent pas le niveau de protection requis, elle en informe le ministère du commerce et demande que des mesures appropriées soient prises pour corriger rapidement tout non-respect potentiel des principes dans un délai raisonnable. Si, à l'expiration du délai fixé, les autorités américaines échouent à démontrer de manière satisfaisante que le bouclier de protection des données UE-États-Unis continue de garantir le respect effectif et un niveau de protection adéquat, la Commission lance la procédure conduisant à la suspension partielle ou complète ou à l'abrogation de la présente décision ([207]). La Commission peut également proposer de modifier la présente décision, par exemple en limitant la portée de la constatation concernant le niveau adéquat de la protection aux seuls transferts de données soumis à des conditions supplémentaires.

(151) En particulier, la Commission lancera la procédure de suspension ou d'abrogation lorsque:

a) des éléments indiquent que les autorités américaines ne respectent pas les observations et les engagements contenus dans les documents joints à la présente décision, notamment en ce qui concerne les conditions et les limites relatives à l'accès des autorités publiques américaines, à des fins répressives, de sécurité nationale ou pour un autre intérêt public, aux données à caractère personnel transférées dans le cadre du bouclier de protection des données;

b) les réclamations déposées par les personnes concernées de l'Union européenne ne sont pas traitées comme il convient; à cet égard, la Commission tiendra compte de toutes les circonstances ayant une incidence sur la possibilité pour les personnes concernées de l'Union européenne de faire appliquer leurs droits, notamment, en particulier, l'engagement volontairement souscrit par les entreprises américaines autocertifiées de coopérer avec les APD et de se conformer à leur avis; ou

c) le médiateur du bouclier de protection des données ne réagit pas en temps utile et de manière adéquate aux demandes de personnes concernées de l'Union européenne.

(152) La Commission envisagera également de lancer la procédure conduisant à la modification, à la suspension ou à l'abrogation de la présente décision si, dans le contexte ou non du réexamen annuel conjoint du fonctionnement du bouclier de protection des données UE-États-Unis, le ministère du commerce ou d'autres ministères ou agences concernés par la mise en œuvre de ce bouclier ou, pour des questions liées à la sécurité nationale, des représentants des services de renseignement aux États-Unis ou le médiateur ne fournissent pas les informations ou les clarifications nécessaires pour évaluer le respect des principes, l'efficacité des procédures de traitement des

([207]) À compter de la date d'entrée en application du règlement général sur la protection des données, la Commission fera usage des pouvoirs dont elle dispose pour adopter, en cas d'urgence impérieuse dûment justifiée, un acte d'exécution suspendant la présente décision, qui s'appliquera immédiatement, sans soumission préalable au comité de comitologie concerné, et qui restera en vigueur pour une période qui n'excède pas six mois.

plaintes ou tout abaissement du niveau de protection requis en raison de l'action des services du renseignement national américain, en particulier en raison de la collecte et/ou de l'accès à des données à caractère personnel qui ne sont pas limités à ce qui est strictement nécessaire et proportionné. À cet égard, la Commission prendra en compte la mesure dans laquelle les informations concernées peuvent être obtenues auprès d'autres sources, notamment dans les rapports des entreprises américaines autocertifiées comme le permet l'USA FREEDOM Act.

(153) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué en vertu de l'article 29 de la directive 95/46/CE, a donné son avis sur le niveau de protection assuré par le bouclier de protection des données UE-États-Unis ([208]) et il en a été tenu compte lors de l'élaboration de la présente décision.

(154) Le Parlement européen a adopté une résolution sur les flux de données transatlantiques ([209]).

(155) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué par l'article 31, paragraphe 1, de la directive 95/46/CE,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, 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 dans le cadre du bouclier de protection des données UE-États-Unis.

2. Le bouclier de protection des données UE-États-Unis se compose des principes publiés par le ministère américain du commerce le 7 juillet 2016, qui figurent à l'annexe II, et des observations et engagements officiels contenus dans les documents énumérés à l'annexe I et aux annexes III à VII.

3. Aux fins du paragraphe 1, les données à caractère personnel sont transférées dans le cadre du bouclier de protection des données UE-États-Unis dès lors qu'elles sont transférées depuis l'Union vers des organisations établies aux États-Unis qui figurent sur la liste des organisations adhérant au bouclier de protection des données, tenue à jour et publiée par le ministère américain du commerce, conformément aux sections I et III des principes énoncés à l'annexe II.

Article 2

La présente décision n'a aucune incidence sur l'application de dispositions de la directive 95/46/CE autres que l'article 25, paragraphe 1, qui se rapportent au traitement de données à caractère personnel dans les États membres, et notamment de son article 4.

Article 3

Lorsque les autorités compétentes des États membres exercent leurs pouvoirs conformément à l'article 28, paragraphe 3, de la directive 95/46/CE pour suspendre ou interdire définitivement les flux de données vers une organisation aux États-Unis figurant sur la liste des organisations adhérant au bouclier de protection des données conformément aux sections I et III des principes énoncés à l'annexe II afin de protéger les individus à l'égard du traitement de leurs données à caractère personnel, les États membres concernés en informent la Commission sans délai.

Article 4

1. La Commission procède à un suivi constant du fonctionnement du bouclier de protection des données UE-États-Unis en vue d'évaluer si les États-Unis continuent d'assurer un niveau adéquat de protection des données à caractère personnel transférées dans le cadre de ce bouclier depuis l'Union vers des organisations établies aux États-Unis.

([208]) Avis n° 1/2016 sur le projet de décision d'adéquation du bouclier de protection des données UE-États-Unis, adopté le 13 avril 2016.
([209]) Résolution du Parlement européen du 26 mai 2016 sur les flux de données transatlantiques [2016/2727(RSP)].

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels les organismes gouvernementaux américains dotés du pouvoir réglementaire de faire respecter les principes énoncés à l'annexe II ne prévoient pas de mécanismes de détection et de surveillance permettant d'identifier 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 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 strictement nécessaire 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, puis chaque année par la suite, la Commission évalue la constatation établie à l'article 1er, paragraphe 1, sur la base de toutes les informations disponibles, notamment les informations reçues dans le cadre du réexamen annuel conjoint visé aux annexes I, II et VI.

5. La Commission communique toute constatation pertinente au comité institué par l'article 31 de la directive 95/46/CE.

6. La Commission propose un projet des mesures à prendre, conformément à la procédure visée à l'article 31, paragraphe 2, de la directive 95/46/CE, en vue de suspendre, de modifier ou d'abroger la présente décision ou d'en limiter la portée, entre autres, lorsque des éléments indiquent:

— que les autorités publiques américaines ne respectent pas les observations et engagements contenus dans les documents joints à la présente décision, notamment en ce qui concerne les conditions et les limites relatives à l'accès des autorités publiques américaines, à des fins répressives, de sécurité nationale ou pour un autre intérêt public, aux données à caractère personnel transférées dans le cadre du bouclier de protection des données UE-États-Unis,

— une défaillance systématique dans le traitement effectif des réclamations déposées par les personnes concernées de l'Union européenne, ou

— une défaillance systématique de la part du médiateur du bouclier de protection des données UE-États-Unis, qui ne réagit pas en temps utile et de manière adéquate aux demandes de personnes concernées de l'Union européenne comme l'exige la section 4, point e), de l'annexe III.

La Commission présente également un projet des mesures à prendre si le défaut de coopération des organes chargés de veiller au fonctionnement du bouclier de protection des données UE-États-Unis aux États-Unis l'empêche de déterminer si la constatation établie à l'article 1er, paragraphe 1, est affectée.

Article 5

Les États membres prennent toutes les mesures nécessaires pour se conformer à la présente décision.

Article 6

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 12 juillet 2016.

Par la Commission
Věra JOUROVÁ
Membre de la Commission

ANNEXE I

Lettre de M^me^ Penny Pritzker, secrétaire américaine au commerce

Le 7 juillet 2016

M^me^ Věra JOUROVÁ
Commissaire chargée de la justice, des consommateurs et de l'égalité des genres
Commission européenne
Rue de la Loi 200
1049 Bruxelles
BELGIQUE

Madame la Commissaire,

Au nom des États-Unis, j'ai le plaisir de vous transmettre, par la présente, un ensemble de textes relevant du «bouclier de protection des données UE–États-Unis», qui sont le fruit de deux années de discussions productives entre nos équipes. Cet ensemble de textes, au même titre que d'autres documents auxquels la Commission a accès auprès de sources publiques, constituent une base très solide pour une nouvelle décision de la Commission européenne relative à l'adéquation du niveau de protection ([1]).

Nous pouvons être fiers, de part et d'autre, des améliorations qui ont été apportées au cadre. Le bouclier de protection des données repose sur des principes qui font l'objet d'un fort consensus des deux côtés de l'Atlantique, et nous avons renforcé leur application. Grâce au travail que nous avons accompli ensemble, nous avons réellement l'occasion d'améliorer la protection de la vie privée à travers le monde.

Le paquet «bouclier de protection des données» comprend les principes du bouclier de protection des données, précédés d'une lettre, jointe en annexe 1, de la direction du commerce international du ministère du commerce des États-Unis, qui administre le programme, exposant les engagements pris par notre ministère pour assurer un fonctionnement efficace du bouclier de protection. Le paquet comporte également l'annexe 2, qui renferme d'autres engagements du ministère du commerce des États-Unis concernant le nouveau modèle arbitral prévu par le bouclier de protection des données.

J'ai demandé à mes collaborateurs de consacrer toutes les ressources nécessaires à la mise en œuvre intégrale et rapide du cadre du bouclier de protection des données, et de veiller à ce que les engagements figurant aux annexes 1 et 2 soient mis en pratique sans tarder.

Le paquet «bouclier de protection des données» comporte en outre des documents d'autres agences des États-Unis, à savoir:

— une lettre de la Commission fédérale du commerce (*Federal Trade Commission* — FTC) décrivant son contrôle de l'application du bouclier de protection des données,

— une lettre du ministère des transports des États-Unis décrivant son contrôle de l'application du bouclier de protection des données,

— deux lettres rédigées par le bureau du directeur du renseignement national (*Office of the Director of National Intelligence* — ODNI) concernant les garanties et les restrictions applicables aux autorités de la sécurité nationale des États-Unis,

— une lettre du département d'État accompagnée d'un mémorandum exposant l'engagement pris par le département d'État d'instituer un nouveau médiateur pour les questions ayant trait au bouclier de protection des données, chargé de répondre aux demandes concernant les pratiques de renseignement d'origine électromagnétique (SIGINT) des États-Unis, et

— une lettre du ministère de la justice des États-Unis concernant les garanties et les limites relatives à l'accès du gouvernement américain à des fins répressives ou d'intérêt public.

Soyez assurée que les États-Unis prennent ces engagements au sérieux.

([1]) Pour autant que la décision de la Commission relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis s'applique à l'Islande, au Liechtenstein et à la Norvège, le paquet «bouclier de protection des données» couvrira non seulement l'Union européenne, mais également ces trois pays.

Dans les trente jours suivant l'approbation définitive de la présomption d'adéquation du niveau de protection, l'intégralité du paquet «bouclier de protection des données» sera transmise au Registre fédéral (*Federal Register*) pour publication.

Nous nous réjouissons à la perspective de coopérer avec vous dans la mise en œuvre du bouclier de protection des données et dans la phase suivante de ce processus que nous entamons conjointement.

Veuillez agréer, Madame la Commissaire,
l'expression de ma considération distinguée.

Penny Pritzker

Annexe 1

Lettre de M. Ken Hyatt, sous-secrétaire faisant fonction au commerce international

M^me^ Věra Jourová
Commissaire chargée de la justice, des consommateurs et de l'égalité des genres
Commission européenne
Rue de la Loi 200
1049 Bruxelles
BELGIQUE

Madame la Commissaire,

Au nom de la direction du commerce international, j'ai le plaisir de détailler dans ces pages la protection renforcée des données à caractère personnel qu'assure le cadre du bouclier de protection des données UE–États-Unis (ci-après le «bouclier de protection des données» ou le «cadre») ainsi que les engagements pris par le ministère du commerce des États-Unis (ci-après le «ministère») pour garantir le fonctionnement efficace du bouclier de protection. La conclusion de cet accord historique représente une avancée majeure pour la protection de la vie privée et pour les entreprises des deux côtés de l'Atlantique. Il permet aux citoyens de l'Union européenne d'être confiants dans le fait que leurs données seront protégées et qu'ils disposeront de voies de recours pour remédier à tout problème éventuel. Il offre une sécurité juridique qui contribuera à faire croître l'économie transatlantique en veillant à ce que des milliers d'entreprises européennes et américaines puissent continuer à investir et à exercer des activités par-delà nos frontières. Le bouclier de protection des données est le résultat de plus de deux années de travail acharné et de collaboration intense avec vous, nos collègues de la Commission européenne (ci-après la «Commission»). Nous espérons poursuivre notre travail avec la Commission en vue de garantir que le bouclier de protection des données fonctionne comme prévu.

Nous avons travaillé avec la Commission à l'élaboration du bouclier de protection afin de permettre aux organisations établies aux États-Unis de satisfaire aux exigences du droit de l'Union européenne quant au caractère adéquat du niveau de protection des données. Le nouveau cadre procurera plusieurs avantages majeurs aux particuliers 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 européenne. 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 bouclier de protection des données, de sorte que cet engagement devient contraignant en droit américain, qu'elles recertifient chaque année leur conformité auprès du ministère, qu'elles mettent à disposition des citoyens européens un service de règlement des litiges indépendant et gratuit, et qu'elles soient soumises à l'autorité de la commission fédérale américaine du commerce (*Federal Trade Commission*, ci-après la «FTC»), du ministère américain des transports (*Department of Transportation*, ci-après le «DOT») ou d'un autre organisme de contrôle. En second lieu, le bouclier de protection permettra à des milliers d'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. Avec la moitié de la production économique mondiale, près de mille milliards de dollars d'échanges de biens et services, et des millions d'emplois des deux côtés de l'Atlantique, la relation économique transatlantique est déjà la plus importante au monde. 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 (PME). 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. Reposant sur des principes communs de respect de la vie privée, le bouclier de protection des données jette un pont entre nos approches juridiques tout en servant les objectifs économiques et commerciaux de l'Europe et des États-Unis.

Si la décision d'une entreprise de s'autocertifier par rapport à ce nouveau cadre est volontaire, dès lors qu'elle s'engage publiquement à l'égard du bouclier de protection des données, son engagement est contraignant en droit américain, sous le contrôle soit de la commission fédérale du commerce, soit du ministère des transports, selon l'autorité qui a compétence vis-à-vis de l'organisation adhérant au bouclier de protection des données.

Améliorations apportées dans le cadre des principes du bouclier de protection des données

Le bouclier de protection mis en place renforce la protection de la vie privée par les moyens suivants:

— il exige que des informations supplémentaires soient communiquées aux personnes concernées dans le cadre du principe de notification, notamment une déclaration de participation de l'organisation au bouclier de protection des données, le rappel du droit de toute personne d'accéder à ses données à caractère personnel et l'indication de l'organisme indépendant compétent pour le règlement des litiges,

— il renforce la protection des données à caractère personnel qui sont transférées d'une organisation adhérant au bouclier de protection des données à un tiers responsable du traitement, en exigeant des parties qu'elles concluent un contrat prévoyant que ces données ne peuvent être traitées qu'à des fins limitées et explicites, dans le respect du consentement accordé par la personne concernée, et que le destinataire assure le même niveau de protection que celui consacré par les principes du bouclier,

— il renforce la protection des données à caractère personnel qui sont transférées d'une organisation adhérant au bouclier de protection des données à un tiers mandataire, notamment en exigeant de cette organisation qu'elle prenne les mesures raisonnables et appropriées pour assurer que le mandataire traite effectivement les informations à caractère personnel qui lui sont transférées de manière conforme aux obligations qui incombent à l'organisation en vertu des principes, qu'elle prenne les mesures raisonnables et appropriées pour mettre fin et remédier à un traitement non autorisé dès qu'elle en est avertie et que, sur demande, elle fasse parvenir au ministère un résumé ou une copie représentative des dispositions de protection de la vie privée concernées figurant dans son contrat avec le mandataire,

— il prévoit qu'une organisation adhérant au bouclier de protection des données assume la responsabilité du traitement des informations à caractère personnel qu'elle reçoit dans le cadre du bouclier de protection et transfère ultérieurement à un tiers agissant en qualité de mandataire, et qu'elle demeure responsable au titre des principes si son mandataire traite de telles informations à caractère personnel d'une manière incompatible avec ces principes, à moins qu'elle ne prouve que le fait générateur du dommage ne lui est pas imputable,

— il stipule que les organisations adhérant au bouclier de protection des données doivent limiter les informations à caractère personnel aux seules informations utiles aux fins du traitement,

— il exige d'une organisation qu'elle certifie chaque année auprès du ministère son engagement à appliquer les principes aux informations qu'elle a reçues pendant qu'elle participait au bouclier de protection des données, si elle quitte celui-ci et choisit de conserver les données en question,

— il exige que des mécanismes de recours indépendants soient accessibles sans frais à la personne concernée,

— il exige des organisations et des mécanismes de recours indépendants qu'elles auront retenus qu'ils répondent sans délai aux requêtes et aux demandes d'information du ministère concernant le bouclier de protection des données,

— il exige des organisations qu'elles répondent sans retard aux plaintes pour non-respect des principes que les autorités des États membres de l'Union européenne leur transmettent par l'intermédiaire du ministère, et

— il exige d'une organisation adhérant au bouclier de protection des données qu'elle rende publiques les sections pertinentes, relatives au bouclier de protection des données, des rapports de conformité ou d'évaluation soumis à la FTC, dans l'hypothèse où elle ferait l'objet d'une ordonnance de la FTC ou des tribunaux fondée sur une absence de conformité.

Gestion et supervision du programme du bouclier de protection des données par le ministère du commerce

Le ministère du commerce réitère son engagement de tenir la liste officielle des organisations américaines qui se sont autocertifiées auprès du ministère en déclarant leur engagement à respecter les principes (ci-après la «liste des adhérents au bouclier de protection des données»), et de la mettre à disposition du public. Le ministère tiendra à jour la liste des adhérents au bouclier de protection des données en rayant 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 également le registre officiel des organisations américaines qui s'étaient précédemment autocertifiées auprès du ministère, mais qui ont été radiées de la liste des adhérents au bouclier de protection des données, y compris celles qui l'ont été pour non-respect persistant des principes. Il précisera la raison pour laquelle chaque organisation a été radiée de la liste.

En outre, le ministère s'engage à renforcer la gestion et la supervision du bouclier de protection des données. Concrètement, il prend les engagements suivants.

Étoffer les informations disponibles sur le site internet du bouclier de protection des données, grâce aux actions suivantes:

— tenir la liste des adhérents au bouclier de protection des données ainsi que le registre des organisations qui avaient antérieurement autocertifié leur adhésion aux principes, mais qui ne sont plus en droit de bénéficier des avantages du bouclier de protection des données,

— insérer un texte explicatif, placé bien en évidence, précisant que les organisations radiées de la liste des adhérents au bouclier de protection des données ne bénéficient plus des avantages dudit bouclier de protection des données, mais qu'elles n'en doivent pas moins continuer d'appliquer les principes aux informations à caractère personnel qu'elles ont reçues pendant la période de leur participation au dispositif aussi longtemps qu'elles conserveront ces informations, et

— fournir un lien vers la liste des affaires FTC liées au bouclier de protection des données, figurant sur le site internet de la FTC.

Vérifier le respect des exigences en matière d'autocertification, grâce aux actions suivantes:

— avant de valider l'autocertification d'une organisation (ou le renouvellement annuel de sa certification) et d'inscrire celle-ci sur la liste des adhérents au bouclier de protection des données, vérifier:

  — que l'organisation a fourni les coordonnées qui lui étaient demandées,

  — qu'elle a présenté une description de ses activités relativement aux informations à caractère personnel en provenance de l'Union européenne,

  — qu'elle a indiqué quelles étaient les informations à caractère personnel couvertes par son autocertification,

  — que, si l'organisation possède un site internet public, elle a indiqué l'adresse internet à laquelle les dispositions de protection de la vie privée qu'elle applique sont consultables et que celles-ci sont accessibles à l'adresse internet indiquée ou, si l'organisation ne possède pas de site internet public, qu'elle a indiqué le lieu où le texte de ces dispositions peut être consulté par le public,

  — qu'elle a incorporé dans ses dispositions de protection de la vie privée une déclaration mentionnant qu'elle adhère aux principes et que, si le texte desdites dispositions est consultable en ligne, elle a inséré un hyperlien vers le site internet du bouclier de protection des données géré par le ministère,

  — qu'elle a indiqué le nom de l'instance réglementaire spécifique qui est chargée 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 mentionnée dans les principes ou dans une future annexe aux principes),

  — que, si l'organisation décide de se conformer aux dispositions des points a) i) et a) iii) du principe relatif au droit de recours, au contrôle de la mise en application et à la responsabilité en s'engageant à coopérer avec les autorités de l'Union européenne chargées de la protection des données (ci-après les «APD»), elle a indiqué son intention de coopérer avec les APD dans l'instruction et le règlement des plaintes déposées au titre du bouclier de protection des données, et en particulier de répondre à leurs demandes lorsque des résidents de l'Union européenne concernés ont porté plainte directement auprès de leur APD nationale,

  — qu'elle a indiqué l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation,

  — qu'elle a précisé la méthode de vérification retenue pour assurer le respect des principes (par exemple, en interne ou par des tiers),

  — qu'elle a indiqué, tant dans sa déclaration d'autocertification que dans sa politique de protection de la vie privée, le mécanisme de recours indépendant mis à disposition des personnes concernées pour l'instruction et la résolution de leurs plaintes

  — qu'elle a inséré dans ses dispositions de protection de la vie privée, si celles-ci sont consultables en ligne, un hyperlien vers le site internet ou le formulaire de dépôt de plainte du mécanisme de recours indépendant mis à disposition pour l'instruction des plaintes non résolues, et

  — que, si l'organisation a indiqué avoir l'intention de recevoir des informations relatives aux «ressources humaines» transférées depuis l'Union européenne dans le cadre d'une relation de travail, elle a déclaré son engagement à coopérer avec les APD et à se conformer à leur avis pour résoudre les plaintes portant sur ses activités relatives à ce type de données, qu'elle a communiqué au ministère une copie des dispositions de protection de la vie privée qu'elle applique dans le domaine des ressources humaines et qu'elle a indiqué le lieu où le texte de ces dispositions peut être consulté par les membres du personnel concernés,

— travailler avec les instances de recours indépendantes pour vérifier que les organisations se sont effectivement inscrites auprès de l'instance indiquée dans leur déclaration d'autocertification, lorsque cette inscription est exigée.

Déployer les efforts pour assurer un suivi des organisations qui ont été radiées de la liste des adhérents au bouclier de protection des données, grâce aux actions suivantes:

— aviser les organisations qui sont radiées de la liste des adhérents au bouclier de protection des données pour «non-respect persistant» qu'elles ne sont pas habilitées à conserver les informations qu'elles ont recueillies dans le cadre dudit bouclier de protection, et

— envoyer des questionnaires aux organisations dont les autocertifications ont expiré ou qui se sont volontairement retirées du bouclier de protection des données pour vérifier si l'organisation restituera ou supprimera les informations à caractère personnel qu'elle a reçues pendant la période de sa participation au bouclier de protection des données, ou si elle continuera d'appliquer les principes à ces informations et, dans l'hypothèse où les informations à caractère personnel seraient conservées, vérifier qui, au sein de l'organisation, servira de point de contact permanent pour les questions liées au bouclier de protection des données.

Rechercher et réprimer les fausses déclarations de participation, grâce aux actions suivantes:

— réexaminer les politiques de protection de la vie privée des organisations ayant précédemment participé au bouclier de protection des données, mais qui ont été radiées de la liste des adhérents, afin de détecter toute fausse déclaration de participation au dispositif;

— de manière systématique, lorsqu'une organisation: a) se retire du bouclier de protection des données; b) ne renouvelle pas son adhésion aux principes; ou c) est exclue du bouclier de protection notamment pour «non-respect persistant», procéder d'office à des vérifications tendant à s'assurer que l'organisation a supprimé de ses déclarations publiques relatives à sa politique de protection de la vie privée toute référence au bouclier de protection des données qui laisserait entendre qu'elle continue de participer activement au dispositif et qu'elle est en droit de bénéficier de ses avantages. Si le ministère constate que ces références n'ont pas été supprimées, il avertit l'organisation qu'il saisira, au besoin, l'organisme compétent pour d'éventuelles mesures coercitives si elle continue de prétendre qu'elle est titulaire d'une certification au titre du bouclier de protection des données. Si l'organisation ne supprime pas les références ni n'autocertifie pas sa conformité aux principes du bouclier de protection des données, le ministère saisira d'office la FTC, le ministère des transports ou toute autre autorité répressive compétente ou, le cas échéant, prendra les mesures qui s'imposent pour faire respecter la marque de certification du bouclier de protection des données,

— mobiliser d'autres efforts pour détecter les fausses déclarations de participation au bouclier de protection des données et l'usage abusif de la marque de certification correspondante, notamment en effectuant des recherches sur l'internet pour relever les endroits où la marque de certification du bouclier de protection des données est affichée ainsi que les références faites au bouclier de protection des données dans les politiques de protection de la vie privée adoptées par les organisations,

— réagir promptement à tout problème que nous détectons au cours de notre surveillance d'office des fausses déclarations de participation et des usages abusifs de la marque de certification, notamment en adressant un avertissement aux organisations qui font une présentation mensongère de leur participation au programme du bouclier de protection des données, comme décrit ci-dessus,

— prendre d'autres mesures correctives appropriées, notamment en exerçant toute voie de droit ouverte au ministère et en saisissant la FTC, le ministère des transports ou toute autre autorité répressive compétente, et

— étudier et traiter rapidement les plaintes pour fausse déclaration de participation que nous recevons.

Le ministère procèdera à des réexamens des politiques de protection de la vie privée publiées par les organisations, afin de détecter et de réprimer plus efficacement les fausses déclarations de participation au bouclier de protection des données. Concrètement, il réexaminera les dispositions de protection de la vie privée des organisations dont l'autocertification a expiré parce qu'elles n'ont pas recertifié leur adhésion aux principes. Il effectuera ce type d'examen pour vérifier que ces organisations ont supprimé de leurs déclarations publiques relatives à leur politique de protection de la vie privée toute référence au bouclier de protection des données qui laisserait entendre qu'elles continuent de participer activement au dispositif. À l'issue de ces réexamens, nous recenserons les organisations qui n'ont pas retiré ces références et nous leur adresserons une lettre signée du bureau du contentieux du ministère les avertissant d'éventuelles mesures coercitives si les références ne sont pas supprimées. Le ministère exercera un suivi pour s'assurer que les organisations ont soit supprimé les références inappropriées, soit recertifié leur adhésion aux principes. En outre, il s'emploiera à détecter les fausses déclarations de participation au bouclier de protection des données faites par des organisations qui n'ont jamais participé au dispositif et prendra des mesures correctives analogues à l'égard de ces organisations.

Réaliser d'office périodiquement des contrôles de conformité et des évaluations du programme, grâce aux actions suivantes:

— contrôler, de manière permanente, la conformité effective par rapport aux principes, notamment en adressant des questionnaires détaillés aux organisations participantes, afin de déceler les problèmes qui pourraient nécessiter un suivi complémentaire. Ces contrôles de conformité auront lieu notamment dans les cas suivants: a) le ministère a reçu des plaintes spécifiques et sérieuses liées au non-respect des principes par une organisation; b) une organisation ne répond pas de manière satisfaisante aux demandes d'information du ministère concernant le bouclier de protection des données; ou c) des indices crédibles suggèrent qu'une organisation ne respecte pas ses engagements au titre du bouclier de protection des données. Le ministère consultera, le cas échéant, les autorités compétentes chargées de la protection des données à propos de ces contrôles de conformité, et

— évaluer régulièrement la gestion et la supervision du programme du bouclier de protection des données, afin de s'assurer que les efforts de suivi sont adaptés pour répondre aux nouveaux problèmes qui peuvent se poser.

Le ministère a renforcé les moyens alloués à la gestion et à la supervision du programme du bouclier de protection des données, notamment en doublant le personnel affecté à ces fonctions. Nous continuerons à consacrer les moyens nécessaires aux efforts visant à assurer un contrôle et une gestion efficaces du programme.

Adapter le site internet du bouclier de protection des données à des publics ciblés

Le ministère organisera le site internet du bouclier de protection afin de l'adapter à trois publics cibles: les citoyens européens, les entreprises européennes et les entreprises américaines. L'inclusion de matériel d'information ciblant directement les citoyens et les entreprises de l'Union européenne favorisera la transparence de plusieurs manières. À l'intention des citoyens européens, cette documentation expliquera clairement: 1) les droits que le bouclier de protection des données confère aux citoyens de l'Union européenne; 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 bouclier de protection des données. À l'intention des entreprises européennes, elle facilitera les vérifications suivantes: 1) la confirmation que telle organisation est en droit de bénéficier des avantages du bouclier de protection des données; 2) le type d'informations couvertes par l'autocertification d'une organisation au titre du bouclier de protection des données; 3) la politique 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.

Renforcer la coopération avec les APD

Pour accroître les possibilités de coopération avec les APD, le ministère désignera en son sein une personne de contact chargée de la liaison avec les APD. Dans les cas où une APD estime qu'une organisation ne se conforme pas aux principes, notamment à la suite d'une plainte déposée par un citoyen européen, elle peut s'adresser à la personne de contact au ministère pour que l'organisation soit soumise à un examen plus approfondi. La personne de contact recevra également les réclamations qui lui seront déférées concernant des organisations qui prétendent faussement participer au bouclier de protection des données, alors qu'elles n'ont jamais autocertifié leur adhésion aux principes. Elle aidera les APD qui cherchent à obtenir des renseignements sur l'autocertification ou la participation antérieure d'une organisation donnée et répondra aux demandes d'information des APD concernant la mise en œuvre d'exigences spécifiques du bouclier de protection des données. En outre, le ministère fournira aux APD des informations sur le bouclier de protection pour qu'elles l'intègrent à leur propre site, aux fins de renforcer la transparence pour les citoyens et les entreprises de l'Union européenne. Une sensibilisation accrue au bouclier de protection 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.

Faciliter le règlement des plaintes pour non-respect des principes

Le ministère, par l'intermédiaire de sa personne de contact, recevra les plaintes qui lui sont déférées par une APD au sujet du non-respect des principes par une organisation adhérant au bouclier de protection des données. Il mettra tout en œuvre pour faciliter le règlement de la plainte avec l'organisation adhérant au bouclier de protection des données. Dans les 90 jours suivant la réception de la plainte, il communiquera l'état d'avancement du dossier à l'APD. Pour faciliter l'introduction de ces plaintes, il établira un formulaire type que les APD transmettront à sa personne de contact. Celui-ci assurera le suivi de toutes les plaintes déférées par les APD au ministère, lequel établira, dans le cadre du réexamen annuel décrit ci-après, un rapport analysant sous forme agrégée les plaintes reçues chaque année.

Adopter des procédures d'arbitrage et désigner des arbitres en concertation avec la Commission

Le ministère remplira ses engagements au titre de l'annexe I et publiera les procédures après conclusion d'un accord.

Mécanisme de réexamen conjoint du fonctionnement du bouclier de protection

Le ministère du commerce, la FTC et, au besoin, d'autres organismes tiendront des réunions annuelles avec la Commission, les APD concernées et les représentants compétents du groupe de travail «article 29» au cours desquelles le ministère fera le point sur le programme du bouclier de protection des données. Ces réunions annuelles 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 bouclier de protection des données, y compris les plaintes déférées au ministère par les APD et les résultats des contrôles de conformité exercés d'office, et pourront également porter sur les modifications législatives en la matière. Le premier réexamen annuel ainsi que les réexamens ultérieurs, le cas échéant, comprendront un dialogue sur d'autres sujets, par exemple dans le domaine de la prise de décision automatisée, y compris les aspects relatifs aux similarités et aux différences dans les approches suivies par l'Union européenne et par les États-Unis.

Mise à jour de concerne 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 bouclier de protection des données 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.

Dérogation pour raison de sécurité nationale

En ce qui les limitations à l'adhésion aux principes du bouclier de protection pour des motifs de sécurité nationale, le conseiller juridique principal du bureau du directeur du renseignement national, M. Robert Litt, a également envoyé deux lettres adressées à MM. Justin Antonipillai et Ted Dean du ministère du commerce, qui vous ont été transmises. Ces lettres examinent de manière approfondie, entre autres, les politiques, les garanties et les limites applicables aux activités de renseignement d'origine électromagnétique adoptées par les États-Unis. Elles expliquent également la transparence assurée par les services de renseignement sur ces questions. Aux fins de l'analyse, par la Commission, du cadre du bouclier de protection des données, les informations contenues dans ces lettres offrent des assurances permettant de conclure que ledit bouclier de protection fonctionnera correctement, en accord avec les principes qui le constituent. Nous croyons savoir qu'il vous sera possible de soulever des questions à propos d'informations rendues publiques par les services de renseignement, au même titre que pour toute autre information, afin d'alimenter le réexamen annuel du cadre du bouclier de protection des données.

Sur la base des principes du bouclier de protection des données 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 déterminera que le cadre du bouclier de protection des données UE–États-Unis assure un niveau de protection adéquat aux fins du droit de l'Union européenne et que les transferts de données depuis l'Union européenne se poursuivront vers les organisations adhérant au bouclier de protection.

Veuillez agréer, Madame la Commissaire,
l'expression de ma considération distinguée.

Ken Hyatt

Annexe 2

Modèle d'arbitrage

ANNEXE I

La présente annexe I définit les conditions selon lesquelles les organisations adhérant au bouclier de protection des données 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 bouclier de protection des données UE–États-Unis. Cette option vise à proposer un mécanisme rapide, indépendant et équitable, selon le choix des personnes concernées, permettant de résoudre les violations alléguées des principes, qui n'ont pas été résolues par les autres mécanismes mis en place au titre du bouclier de protection des données, le cas échéant.

A. **Portée**

Un particulier peut opter pour l'arbitrage en vue de déterminer, pour les plaintes résiduelles, si une organisation adhérant au bouclier de protection des données n'a pas satisfait à ses obligations au titre des principes envers ce particulier et si cette infraction reste entièrement ou partiellement sans réparation. Cette possibilité est offerte uniquement à ces fins. Cette option 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 bouclier de protection des données.

B. **Recours possibles**

Dans le cadre de cette option d'arbitrage, le panel du bouclier de protection des données (composé d'un ou de trois arbitres, comme convenu par les parties) est habilité à imposer une mesure de réparation équitable non pécuniaire propre à chaque personne (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 d'arbitrage en matière de recours. Dans son examen des recours, le panel d'arbitrage est tenu de prendre en considération les recours déjà imposés par d'autres instances dans le cadre du bouclier de protection des données. Les recours en dommages-intérêts, portant sur des honoraires, frais ou dépens, et les autres recours 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 III.11(d)(i) des principes; 2) faire appel à l'instance de recours indépendante prévue par les principes, gratuite pour les particuliers; et 3) faire part du problème au ministère du commerce par l'intermédiaire de son autorité chargée de la protection des données et laisser au ministère du commerce 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* (administration du commerce international) du ministère du commerce, sans aucun 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 judiciaire 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 autorité chargée de la protection des données (APD) de l'Union européenne: 1) est compétente au titre des sections III.5 ou III.9 des principes; 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 européenne n'empêche pas à elle seule d'invoquer 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 se prévaloir de cette option d'arbitrage contraignant est entièrement volontaire. Les décisions d'arbitrage 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]) Section I.5 des principes.

E. **Contrôle et application**

Les personnes concernées et les organisations adhérant au bouclier de protection des données pourront demander le contrôle juridictionnel et la mise en application des décisions d'arbitrage conformément à la législation américaine au titre de la *Federal Arbitration Act* ([1]). Tout dossier de ce type doit être porté devant le tribunal fédéral de première instance compétent pour le lieu principal d'activité de l'organisation adhérant au bouclier de protection des données.

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 les procédures d'arbitrage futures devant les tribunaux de l'Union européenne ou des États-Unis ou dans le cadre de procédures lancées par la Commission fédérale du commerce (*Federal Trade Commission* — FTC).

F. **Le panel d'arbitrage**

Les parties sélectionneront les arbitres parmi la liste d'arbitres examinée ci-dessous.

Conformément au droit applicable, le ministère du commerce américain et la Commission européenne dresseront une liste de 20 arbitres, sélectionnés sur la base de leur indépendance, de leur intégrité et de leur expertise. Ce processus sera soumis aux principes suivants:

Les arbitres:

1) resteront sur la liste pendant une période de 3 ans, sauf circonstances exceptionnelles ou motif valable, cette période étant renouvelable une fois;

2) ne recevront aucune consigne ni des parties, ni d'une organisation adhérant au bouclier de protection des données, ni des États-Unis, de l'Union européenne ou d'un État membre de l'Union européenne, 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 européen en matière de protection des données.

G. **Procédures d'arbitrage**

Conformément au droit en vigueur, dans un délai de 6 mois à compter de la décision constatant le niveau de protection adéquat, le ministère du commerce et la Commission européenne conviendront d'adopter un ensemble existant et bien établi de procédures arbitrales américaines (comme les procédures AAA ou JAMS) pour régir les procédures devant le panel du bouclier de protection des données, sous réserve des considérations suivantes:

1) Un particulier 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.

([1]) Le chapitre 2 de la Federal Arbitration Act («FAA») dispose qu'«un 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, 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.

2) Des procédures seront mises en place afin que la 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 européenne ou d'un État membre de l'Union européenne ou de tout autre organe étatique, autorité publique ou autorité répressive ne peut participer à ces arbitrages, étant entendu qu'à la demande d'un particulier de l'Union européenne, les APD de l'Union européenne peuvent apporter une assistance dans la préparation de la notification uniquement. Les APD de l'Union européenne ne peuvent par contre 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 du fait que le particulier est représenté ou non 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 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.

H. **Coûts**

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

Sous réserve de la législation en vigueur, et en concertation avec la Commission européenne, le ministère du commerce facilitera la création d'un fonds auquel les organisations adhérant au bouclier de protection des données seront tenues d'apporter une contribution annuelle basée en partie sur leur taille et qui couvrira les coûts d'arbitrage, y compris les honoraires des arbitres, jusqu'à des montants plafonnés. Le fonds sera géré par une partie tierce qui rendra compte régulièrement de son fonctionnement. Lors du réexamen annuel, le ministère du commerce et la Commission européenne examineront le fonctionnement du fonds, notamment la nécessité éventuelle d'ajuster le montant des contributions ou des plafonds, et prendront 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 adhérant au bouclier de protection des données. Les honoraires d'avocats ne sont pas couverts par la présente disposition ni par aucun fonds relevant de la présente disposition.

ANNEXE II

PRINCIPES DU CADRE «BOUCLIER 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 ont comme objectif commun de protéger davantage la vie privée, les États-Unis préconisent dans ce domaine une approche différente de celle de l'Union européenne. 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. Au vu de ces différences, et afin d'offrir aux organisations établies aux États-Unis un mécanisme fiable pour les transferts de données à caractère personnel vers les États-Unis depuis l'Union européenne tout en permettant aux personnes concernées de l'Union européenne de continuer de bénéficier de garanties et de protections efficaces comme l'exige la législation européenne au regard du traitement de leurs données à caractère personnel transférées dans des pays non membres de l'Union européenne, le ministère du commerce (*Department of Commerce*) publie les présents principes du bouclier de protection des données, y compris les principes complémentaires (collectivement «les principes») 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, le secteur d'activité concerné et d'autres parties prenantes dans le but de faciliter le commerce et les relations d'affaires entre les États-Unis et l'Union européenne. Ils sont exclusivement destinés aux organisations établies aux États-Unis recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives au bouclier de protection des données et de bénéficier ainsi de la décision de la Commission constatant l'adéquation du niveau de protection ([1]). Les principes n'ont aucune incidence sur l'application de dispositions nationales mettant en œuvre la directive 95/46/CE (ci-après la «directive») qui se rapportent au traitement de données à caractère personnel dans les États membres. Ils ne limitent pas non plus les obligations en matière de vie privée applicables par ailleurs en vertu de la législation des États-Unis.

2. Pour pouvoir se prévaloir du bouclier de protection des données afin de transférer des données à caractère personnel depuis l'Union européenne, une organisation doit autocertifier son respect des principes auprès du ministère du commerce (ou auprès de la personne désignée par celui-ci) (ci-après le «ministère»). Si la décision prise par les organisations d'adhérer au cadre du bouclier de protection des données est entièrement volontaire, le respect de ses règles est obligatoire: les organisations qui autocertifient leur engagement auprès du ministère et qui annoncent publiquement leur engagement à respecter les principes sont tenues de s'y conformer entièrement. Pour adhérer au cadre du bouclier de protection des données, une organisation doit: a) être soumise aux pouvoirs d'enquête et aux pouvoirs répressifs de la Commission fédérale du commerce (*Federal Trade Commission* — FTC), du ministère des transports ou d'un autre organe réglementaire qui assurera concrètement le respect des principes (d'autres organes réglementaires 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 ses politiques de respect de la vie privée, qui doivent être conformes aux principes; et d) appliquer les principes dans leur intégralité. Toute non-conformité d'une organisation peut faire l'objet de mesures d'exécution conformément à la section 5 de la loi sur la Commission fédérale du commerce (*Federal Trade Commission Act*), qui interdit les pratiques déloyales ou frauduleuses dans le domaine du commerce [15 U.S.C. § 45(a)], ou à toute autre loi du même type.

3. Le ministère du commerce tiendra et mettra à la disposition du public une liste officielle des organisations des États-Unis qui se sont autocertifiées auprès du ministère et qui ont déclaré leur engagement à respecter les principes (la «liste du bouclier de protection des données»). Une organisation peut prétendre aux avantages du cadre du bouclier de protection des données dès le moment où le ministère l'inscrit sur la liste du bouclier de protection des données. Le ministère supprimera une organisation de la liste du bouclier de protection des données si cette organisation se retire volontairement du bouclier de protection des données ou si elle manque à son obligation de recertification annuelle envers le ministère. La suppression d'une organisation de la liste du bouclier de protection des données a pour conséquence que cette organisation ne bénéficie plus de la décision de la Commission européenne constatant un niveau de protection adéquat en vue de recevoir des informations à caractère personnel depuis l'Union européenne. L'organisation reste tenue d'appliquer les principes aux informations à caractère personnel qu'elle a reçues alors qu'elle participait au bouclier de protection des données et de déclarer annuellement au ministère son engagement à le faire, aussi longtemps qu'elle conserve ces informations; dans le cas contraire, l'organisation doit restituer ou supprimer les informations concernées ou assurer une protection «adéquate» de ces informations par d'autres moyens. Le ministère supprimera également de la liste du bouclier de protection des données les organisations qui, de manière récurrente, ne respectent pas les principes; ces organisations ne répondent pas aux conditions requises pour accéder aux avantages du bouclier de protection des données et doivent restituer ou supprimer les informations à caractère personnel reçues dans le cadre du bouclier de protection des données.

4. Le ministère tiendra et mettra également à la disposition du public une liste officielle des organisations des États-Unis qui s'étaient précédemment autocertifiées auprès du ministère mais qui ont été supprimées de la liste du

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

bouclier de protection des données. Le ministère publiera une mise en garde claire indiquant que ces organisations ne participent pas au bouclier de protection des données, que leur suppression de la liste du bouclier de protection des données signifie qu'elles ne peuvent pas prétendre se conformer au cadre du bouclier de protection des données et qu'elles doivent éviter toute déclaration ou toute pratique trompeuse qui laissent entendre qu'elles participent au bouclier de protection des données, et qu'elles ne peuvent plus prétendre au bénéfice de la décision de la Commission européenne constatant un niveau de protection adéquat leur permettant de recevoir des informations à caractère personnel en provenance de l'Union européenne. Toute organisation qui prétend participer au bouclier de protection des données ou qui fait des déclarations trompeuses relatives au bouclier de protection des données après avoir été supprimée de la liste du bouclier de protection des données est susceptible de faire l'objet de mesures répressives de la part de la FTC, du ministère des transports et d'autres autorités répressives.

5. L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect de la législation; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation puisse démontrer que le non-respect des principes est limité dans la mesure nécessaire pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; ou c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent s'efforcer d'appliquer ces principes de manière complète et transparente, y compris en indiquant — dans leurs codes de protection de la vie privée — dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront de façon régulière. 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 base du bouclier de protection des données après leur adhésion à celui-ci. Les organisations qui décident d'étendre les avantages du bouclier de protection des données à des informations à caractère personnel tirées de fichiers qui concernent les ressources humaines en provenance de l'Union européenne afin de les utiliser dans le cadre d'une relation de travail doivent mentionner cette intention lorsqu'elles autocertifient leur engagement auprès du ministère et doivent se conformer aux exigences exposées dans le principe complémentaire relatif à l'autocertification.

7. Le droit des États-Unis est applicable en ce qui concerne l'interprétation et le respect des principes du bouclier de protection des données et des mesures de protection de la vie privée mises en œuvre par les organisations adhérant au bouclier de protection des données, à l'exception des cas dans lesquels des organisations se sont engagées à coopérer avec les autorités européennes chargées de la protection des données (APD). Sauf indication contraire, toutes les dispositions des principes sont applicables lorsqu'elles sont pertinentes.

8. Définitions:

   a) Par «donnée ou information à caractère personnel», il faut entendre toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application de la directive, qui est transférée de l'Union européenne vers une organisation américaine 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 les moyens du traitement de données à caractère personnel.

9. La date d'entrée en vigueur des principes est la date d'approbation définitive de la décision de la Commission européenne constatant le niveau de protection adéquat.

II. PRINCIPES

1. **Notification**

   a) Toute organisation doit informer les personnes concernées:

      i) de sa participation au bouclier de protection des données, en fournissant l'adresse internet de la liste du bouclier de protection des données ou un lien menant à cette liste;

      ii) des types de données à caractère personnel collectées et, le cas échéant, des entités ou filiales 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 bouclier de protection des données;

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 en vue de restreindre l'utilisation et la divulgation de leurs données à caractère personnel;

ix) de l'organe indépendant de règlement des litiges désignés pour traiter les plaintes et assurer gratuitement un recours adéquat aux personnes, 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 européenne; 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 d'exécution de la FTC, du ministère des transports ou de tout autre organe réglementaire agréé aux États-Unis;

xi) de la possibilité pour la personne concernée, sous certaines conditions, de faire appel à un arbitrage contraignant;

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.

b) Cette notification doit être communiquée de manière claire et visible aux personnes concernées 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 concernées la possibilité de décider (opposition) si leurs informations à caractère personnel: i) peuvent être divulguées à une tierce personne; ou ii) peuvent être utilisées dans un but matériellement différent du ou des objectifs pour lesquels les données ont été initialement collectées ou du ou des objectifs approuvés ultérieurement par la personne concernée. 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 (consentement) des personnes concernés 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 si le tiers indique que cette information est sensible et la traite en conséquence.

3. **Responsabilité en cas de tranfert 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 s'assurer que le mandataire traite effectivement les informations à caractère personnel transférées d'une façon conforme aux obligations de l'organisation au titre 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 ([1]). 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 ([2]) uniquement tant que cette conservation sert à atteindre l'objectif de traitement au sens du point 5a. 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 bouclier de protection des données. 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.

([1]) 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.

([2]) 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».

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 systèmes de recours indépendants et aisément accessibles, permettant d'étudier et de résoudre rapidement et sans aucun frais toute plainte et tout litige 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 renseignements et les indications fournies par les organisations sur 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 instances de recours indépendantes qu'elles ont sélectionnées doivent réagir rapidement aux questions et aux demandes d'informations émanant du ministère concernant le bouclier de protection des données. Toutes les organisations doivent répondre sans retard aux plaintes relatives au respect des principes formulées par les autorités des États membres de l'Union européenne par l'intermédiaire du ministère. Les organisations qui ont choisi de coopérer avec des autorités chargées de la protection des données, notamment les organisations qui traitent des données concernant les ressources humaines, doivent répondre directement à ces autorités concernant l'examen et la résolution des plaintes.

c) Les organisations sont tenues d'assurer l'arbitrage des plaintes et de respecter les conditions exposées à l'annexe I, pour autant qu'une personne ait demandé le recours à un arbitrage contraignant en en notifiant 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 adhérant au bouclier de protection des données assume la responsabilité du traitement des informations à caractère personnel qu'elle reçoit au titre du bouclier de protection des données et qu'elle transfère ultérieurement à un tiers agissant pour son compte en qualité de mandataire. L'organisation adhérant au bouclier de protection des données reste responsable au titre des principes si son mandataire traite ces informations à caractère personnel d'une manière non conforme aux principes, sauf si l'organisation apporte la preuve qu'elle n'est pas responsable des événements donnant lieu au préjudice.

e) Toute organisation qui fait l'objet d'une ordonnance de la FTC ou d'une ordonnance judiciaire pour cause de non-conformité est tenue de rendre publique les parties liées au bouclier de protection des données de tout rapport de conformité ou d'évaluation soumis à la FTC dans les limites des exigences de confidentialité. Le ministère a mis en place un point de contact spécifique que les autorités chargées de la protection des données peuvent contacter pour tout problème de non-conformité par des organisations. La FTC examinera en priorité les dossiers de non-conformité avec les principes déférés par le ministère et par les autorités des États membres de l'Union européenne et échangera sans retard des informations relatives à chaque dossier aux 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 l'individu.

2. **Exceptions journalistiques**

a) Compte tenu des garanties qu'offre la Constitution américaine en ce qui concerne la liberté de la presse et de l'exemption prévue dans la directive pour les informations utilisées par les journalistes, 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 recueillies 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 du bouclier de protection des données.

3. **Responsabilité secondaire**

a) Les fournisseurs d'accès Internet (FAI), les sociétés de télécommunications et d'autres organismes ne sont pas soumis aux principes du bouclier de protection des données lorsqu'ils se limitent à transmettre, acheminer, remplacer ou masquer des informations pour le compte d'un autre organisme. Pas plus que la directive elle-même, le bouclier de protection des données ne fait 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 l'assentiment 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 adhérant au bouclier de protection des données, 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 adhérant au bouclier de protection des données 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 autorités chargées de la protection des données (APD) de l'Union européenne selon les modalités décrites ci-dessous. Dans le cadre du bouclier de protection des données, les organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne doivent s'engager à utiliser des mécanismes efficaces assurant le respect des principes du bouclier de protection des données. 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 contrôler la véracité des affirmations et des déclarations faites par les organisations en ce qui concerne le respect de la vie privée; et a) iii) des dispositions aux termes desquelles les organisations sont tenues de résoudre les problèmes qui découlent du non-respect des principes et d'assumer les conséquences qui en résultent. 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 déclarant, dans son autocertification d'adhésion au bouclier de protection des données adressée au ministère du commerce (voir le 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» du bouclier de protection des données en s'engageant à coopérer avec les APD;

ii) coopérera avec les APD au niveau de l'instruction et du règlement des plaintes déposées au titre du bouclier de protection des données; et

iii) suivra tout avis donné par les APD selon lequel l'organisation doit prendre des mesures spécifiques pour respecter les principes du bouclier de protection des données, y compris toute mesure de réparation ou d'indemnisation au bénéfice des particuliers qui ont subi un préjudice en raison du non-respect desdits principes, et informera par écrit les APD des mesures prises à cet effet.

c) Fonctionnement des panels d'APD

i) La coopération des APD se traduira par des informations et des avis donnés selon les modalités suivantes:

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

2) Le panel conseillera les organisations américaines concernées au sujet de plaintes non résolues de particuliers portant sur le traitement des informations à caractère personnel qui ont été transférées au départ de l'Union européenne au titre du bouclier de protection des données. Les conseils donnés viseront à assurer une application correcte des principes du bouclier de protection des données et porteront également sur les mécanismes de règlement des litiges que les APD jugeront appropriés pour le ou les particuliers concernés.

3) Le panel donnera son avis en réponse aux recours formés par les organisations concernées et/ou aux plaintes introduites directement par des particuliers contre des organisations qui se sont engagées à coopérer avec les APD aux fins du respect des principes du bouclier de protection des données, tout en encourageant et, le cas échéant, en aidant ces particuliers à faire d'abord usage des mécanismes internes d'instruction des plaintes 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 plainte ou du recours.

5) S'il le juge approprié, le panel rendra publics les résultats de l'examen des plaintes 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 devront s'engager à se conformer aux avis émis par les APD. Si une organisation ne s'exécute par 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 déférer l'affaire à la Federal Trade Commission, au ministère des transports ou à une autre instance réglementaire américaine visée à l'annexe des principes du bouclier de protection des données 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 du commerce afin que celui-ci corrige la liste du bouclier de protection des données. Tout manquement à l'engagement de coopérer avec le panel ainsi que tout non-respect des principes du bouclier de protection des données seront considérés comme constitutifs d'un acte frauduleux au titre de la section 5 de la loi instituant la Federal Trade Commission ou de lois équivalentes.

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

e) Les organisations optant pour cette formule devront verser une cotisation annuelle couvrant les frais de gestion du panel et seront, le cas échéant, invitées à participer aux frais de traduction résultant de l'examen, par le panel, des recours formés et des plaintes déposées contre elles. La cotisation annuelle n'excédera pas 500 dollars des États-Unis et sera réduite pour les petites entreprises.

6. **Autocertification**

a) Une organisation peut prétendre aux avantages offerts par le bouclier de protection des données dès le moment où le ministère l'inscrit sur la liste du bouclier de protection des données, après avoir déterminé que son dossier d'autocertification était complet.

b) Pour autocertifier son adhésion au bouclier de protection des données, une organisation doit remettre au ministère américain un dossier d'autocertification signé par un dirigeant de l'organisation adhérant au bouclier de protection des données, contenant au moins les informations suivantes:

i) le nom de l'organisation, son adresse postale, son adresse électronique, ses numéros de téléphone et de télécopieur;

ii) une description des activités de l'organisation relativement aux informations à caractère personnel en provenance de l'Union européenne;

iii) une description des dispositions de protection de la vie privée appliquées par l'organisation auxdites informations, précisant:

1) si l'organisation possède un site internet public, l'adresse internet à laquelle ces dispositions sont accessibles ou, si l'organisation ne possède pas de site internet public, le lieu où le texte de ces dispositions peut être consulté par le public;

2) la date de mise en œuvre de ces dispositions;

3) le service à contacter en cas de plainte, pour des demandes d'accès et pour toute autre question relevant du bouclier de protection des données;

4) le nom de l'instance réglementaire spécifique qui est chargée 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 mentionnée dans les principes ou une future annexe aux principes);

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

6) la méthode de vérification (par exemple, en interne ou par des tiers) (voir le principe complémentaire «Vérification»); et

7) l'instance de recours indépendante qui pourra instruire les plaintes non résolues.

c) Une organisation peut étendre les avantages du bouclier de protection des données à des informations relatives aux ressources humaines qui sont transférées depuis l'Union européenne afin d'être utilisées dans le cadre de relations de travail, lorsque l'une des instances réglementaires mentionnées dans les principes ou une future annexe aux principes est compétente pour statuer sur les plaintes déposées contre l'organisation en raison du traitement des informations relatives aux ressources humaines. En outre, l'organisation doit indiquer dans son dossier d'autocertification 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 de respect de la vie privée concernant les ressources humaines et indiquer le lieu où la politique de respect de la vie privée peut être consultée par les salariés concernés.

d) Le ministère tiendra la liste du bouclier de protection des données énumérant toutes les organisations qui ont déposé des dossiers d'autocertification complets, assurant ainsi à ces organisations le bénéfice du bouclier de protection des données. Il mettra cette liste à jour sur la base des dossiers annuels de renouvellement de l'autocertification et des notifications reçues conformément au principe complémentaire «Résolution des litiges et application des décisions». Ces dossiers d'autocertification doivent être déposés au moins une fois par an. Dans le cas contraire, l'organisation sera supprimée de la liste du bouclier de protection des données et ne bénéficiera plus des avantages découlant du bouclier de protection des données. La liste du bouclier de protection des données et les dossiers d'autocertification déposés par les organisations seront rendus publics. Toute organisation inscrite sur la liste du bouclier de protection des données par le ministère doit également mentionner, dans ses déclarations publiques relatives à sa politique en matière de protection de la vie privée,

qu'elle adhère aux principes du bouclier de protection des données. Si elle est disponible en ligne, la politique de protection de la vie privée d'une organisation doit inclure un hyperlien vers le site internet du bouclier de protection des données du ministère et un hyperlien vers le site ou le formulaire de dépôt de plainte de l'instance de recours indépendante qui pourra instruire les plaintes non résolues.

e) Les principes du bouclier de protection des données s'appliquent dès la certification. Conscientes du fait que les principes auront une incidence sur leurs relations commerciales avec des tiers, les organisations qui certifient leur engagement à adhérer au cadre du bouclier de protection des données dans les deux mois suivant la date de prise d'effet du cadre mettront leurs relations commerciales existantes avec des tiers en conformité avec le principe «Responsabilité en cas de transfert ultérieur» le plus rapidement possible et, en tout état de cause, dans un délai de neuf mois au maximum à compter de la date de leur certification au titre du bouclier de protection des données. Au cours de cette période intermédiaire, les organisations qui transfèrent des données à un tiers doivent: i) appliquer les principes «Notification» et «Choix»; et ii), en cas de transfert de données à caractère personnel à un tiers agissant en qualité de mandataire, s'assurer que le mandataire est tenu d'offrir un niveau de protection au moins égal à celui requis par les principes.

f) Une organisation doit appliquer les principes du bouclier de protection des données à toutes les données à caractère personnel reçues depuis l'Union européenne au titre du bouclier de protection des données. L'engagement d'adhérer aux principes du bouclier de protection des données 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 bouclier de protection des données. 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 bouclier de protection des données pour quelque raison que ce soit. Une organisation qui se retire du bouclier de protection des données 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 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); dans le cas contraire, l'organisation doit restituer ou supprimer les informations concernées. Une organisation qui se retire du bouclier de protection des données doit supprimer de toute politique de protection de la vie privée concernée toute référence au bouclier de protection des données donnant à penser que l'organisation continue de participer activement au bouclier de protection des données et peut prétendre à ses avantages.

g) Lorsqu'une organisation cesse d'exister en tant qu'entité juridique distincte en raison d'une opération de fusion ou d'absorption, elle doit le notifier à l'avance au ministère. La notification doit également indiquer si l'entité qui l'absorbe ou l'entité qui naît de la fusion: i) reste soumise aux principes du bouclier de protection des données en vertu des dispositions juridiques régissant la fusion ou l'absorption; ou ii) si elle choisit d'autocertifier son adhésion aux principes du bouclier de protection des données ou de mettre en place d'autres garanties telles qu'un accord écrit certifiant l'adhésion à ces principes. Si aucune des solutions visées aux points i) et ii) n'est mise en œuvre, toute donnée à caractère personnel acquise dans le cadre du bouclier de protection des données doit être effacée sans tarder.

h) Une organisation qui se retire du bouclier de protection des données pour quelque raison que ce soit doit supprimer toute déclaration donnant à penser qu'elle continue de participer au bouclier de protection des données ou qu'elle peut prétendre aux avantages conférés par le bouclier de protection des données. La marque de certification du bouclier de protection des données 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 du bouclier de protection des données peut donner lieu à des poursuites devant la FTC ou devant 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 dans le cadre du bouclier de protection des données sont sincères et que ces pratiques ont été mises en œuvre conformément à leurs déclarations et aux principes du bouclier de protection des données.

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) Dans le cadre de l'autoévaluation, la vérification doit établir que la politique en matière de protection de la vie privée, en ce qui concerne les informations à caractère personnel reçues de l'Union européenne, qui est rendue publique par l'organisation, est appropriée, complète, affichée de façon bien visible, totalement mise en œuvre et accessible. Elle doit aussi montrer que cette politique est conforme aux principes du bouclier de protection des données, que les personnes sont informées de l'existence de mécanismes internes de traitement des réclamations et des mécanismes indépendants par le truchement desquels ils peuvent diligenter leurs plaintes, 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 vérifiant l'autoévaluation 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, ce dernier devra démontrer que la politique de l'organisation en matière de protection de la vie privée, en ce qui concerne les informations reçues de l'Union européenne, respecte les principes du bouclier de protection des données, que cette politique est respectée et que les particuliers sont informés 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 dans le cadre du bouclier de protection des données et remettre celles-ci sur demande, dans le cadre d'une enquête ou d'une réclamation pour non-conformité, à l'organisme indépendant 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 d'accès dans la pratique

i) Conformément aux principes du bouclier de protection des données, 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 d'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 ([1]);

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.

([1]) 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) 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 à toute personne qui en fait la demande d'accéder 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.

ii) Si les informations commerciales confidentielles peuvent être aisément séparées d'autres 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.

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 de la directive, 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;

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

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

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

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 bouclier de protection des données

i) Si une organisation située dans l'Union européenne transfère des informations à caractère personnel relatives à ses salariés (actuels ou anciens) et rassemblées 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 adhère aux principes du bouclier de protection des données, ce transfert bénéficie du bouclier de protection des données. Dans ce cas, la collecte d'informations ainsi que son traitement avant le transfert sont soumis aux lois nationales du pays de l'Union européenne 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 du bouclier de protection des données 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 européenne sur les salariés dans le cadre du bouclier de protection des données peut les communiquer à des tiers et/ou les utiliser à d'autres fins uniquement si les principes qui régissent la notification et le choix sont respectés. Ainsi, si une organisation américaine veut utiliser les informations à caractère personnel rassemblées 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 recueillies 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 européenne peuvent exclure d'autres utilisations de ces informations, même après leur transfert en dehors du territoire de l'Union européenne, et que ces conditions doivent être respectées.

iii) Par ailleurs, les employeurs doivent s'efforcer 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 d'accès

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 européenne, les employeurs doivent naturellement respecter les réglementations locales et veiller à ce que les salariés de l'Union européenne 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 bouclier de protection des données, une organisation traitant de telles données aux États-Unis doit coopérer en fournissant cet accès, soit directement, soit par le biais de l'employeur de l'Union européenne.

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 du bouclier de protection des données. 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 adhérant aux principes du bouclier de protection des données qui utilise des données de l'Union européenne relatives aux ressources humaines transférées à partir de l'Union européenne dans le cadre d'une relation de travail et qui souhaite que ces transferts soient couverts par le bouclier de protection des données doit s'engager à cet effet à coopérer aux enquêtes des autorités compétentes de l'Union européenne et à respecter l'avis de celles-ci.

e) Application du principe de responsabilité en cas de transfert ultérieur

Pour les besoins opérationnels occasionnels liés à l'emploi d'une organisation adhérant au bouclier de protection des données et concernant des données à caractère personnel transférées au titre du bouclier de protection des données, 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 de la partie tierce (comme l'exige normalement le principe «Responsabilité en cas de transfert ultérieur»), pour autant que l'organisation adhérant au bouclier de protection des données 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 européenne 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 bouclier de protection des données.

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 européenne, et que le sous-traitant participe ou non au bouclier de protection des données. 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 participants au bouclier de protection des données assurent une protection adéquate, les contrats de simple traitement conclus avec ces derniers ne nécessitent pas d'autorisation préalable (ou alors cette autorisation est octroyée automatiquement par les États membres), contrairement aux contrats dont les bénéficiaires ne participent pas au bouclier de protection des données ou qui n'assurent pas de protection adéquate.

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

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 d'un 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 européenne 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 adhérant au bouclier de protection des données reste responsable du respect des principes.

c) Transferts entre responsables du traitement

Pour les transferts entre responsables du traitement, le responsable du traitement qui reçoit les données ne doit pas nécessairement être une organisation adhérant au bouclier de protection des données ni posséder d'instance de recours indépendante. L'organisation adhérant au bouclier de protection des données doit conclure, avec le responsable du traitement tiers qui reçoit les données, un contrat prévoyant un niveau de protection égal à celui requis dans le cadre du bouclier de protection des données, à ceci près que le responsable du traitement tiers ne doit pas être une organisation adhérant au bouclier de protection des données ni posséder d'instance de recours indépendante 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 bouclier de protection des données. 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 du bouclier de protection des données 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 plaintes de particuliers et la résolution des litiges; iii) en s'engageant à coopérer avec les autorités chargées de la protection des données au sein de l'Union européenne 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 la section 5 de la *Federal Trade Commission Act*, qui interdit les pratiques déloyales ou frauduleuses, ou à toute autre loi du même type.

c) Afin de garantir le respect de leurs engagements au titre du bouclier de protection des données et de faciliter l'administration du programme, les organisations ainsi que leurs instances de recours indépendantes doivent fournir des informations relatives au bouclier de protection des données à la demande du ministère. En outre, les organisations doivent répondre sans retard aux plaintes relatives au respect des principes formulées par les APD par l'intermédiaire du ministère. La réponse doit déterminer si la plainte est fondée et, le cas échéant, comment l'organisation compte corriger le problème. Le ministère protègera la confidentialité des informations qu'elle reçoit conformément à la législation américaine.

d) Instances de recours

i) Les consommateurs devraient être encouragés à soumettre toute plainte éventuelle à l'organisation concernée avant de faire appel à des instances de recours indépendantes. Les organisations doivent répondre aux consommateurs dans les 45 jours suivant réception d'une plainte. L'indépendance d'une instance 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», le recours dont disposent les particuliers doit être facilement accessible et gratuit. Les organismes d'instruction des litiges devraient étudier toutes les plaintes déposées par des particuliers, à moins qu'elles ne soient manifestement non fondées ou abusives. Cette condition n'empêche pas l'établissement, par l'instance de recours, de critères d'éligibilité, mais ceux-ci devraient être transparents et justifiés (ils pourraient viser, par exemple, à exclure les plaintes 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 plaintes légitimes. Les instances de recours devraient, en outre, fournir aux particuliers des informations complètes et facilement accessibles sur le fonctionnement de la procédure lors du dépôt de la plainte. Ces informations devraient inclure une description des pratiques suivies en matière de protection de la vie privée, conformément aux principes du bouclier de protection des données. Les instances devraient, en outre, coopérer en vue de mettre au point des outils, tels que des formulaires standards de plainte, destinés à faciliter le fonctionnement de la procédure de résolution des litiges.

ii) Les instances de recours indépendantes doivent inclure sur leurs sites internet publics des informations relatives aux principes du bouclier de protection des données et aux services qu'elles fournissent dans le cadre de ce bouclier de protection. Ces informations doivent comprendre: 1) des informations relatives aux exigences en matière d'instances de recours indépendantes au titre des principes du bouclier de protection des données, ou un lien vers ces exigences; 2) un lien vers le site internet «bouclier de protection des données» du ministère; 3) l'indication que les services de règlement des litiges qu'elles proposent sont gratuits pour les particuliers; 4) une description des modalités de dépôt d'une plainte relative au bouclier de protection des données; 5) le délai de traitement des plaintes relatives au bouclier de protection des données; et 6) une description des possibilités de recours.

iii) Les instances de recours indépendantes doivent publier un rapport annuel présentant des statistiques agrégées relatives à leurs services de résolution des litiges. Ce rapport annuel doit indiquer: 1) le nombre total de plaintes relatives au bouclier de protection des données reçues au cours de l'année faisant l'objet du rapport; 2) les types de plaintes reçues; 3) des indicateurs de qualité de la résolution des litiges, par exemple le délai de traitement des plaintes; et 4) les résultats du traitement des plaintes reçues, notamment le nombre et les types de recours et les sanctions infligées.

iv) Comme indiqué à l'annexe I, un particulier peut opter pour l'arbitrage en vue de déterminer, pour les plaintes résiduelles, si une organisation adhérant au bouclier de protection des données n'a pas satisfait à ses obligations au titre des principes envers ce particulier 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 bouclier de protection des données. Dans le cadre de cette option d'arbitrage, le panel du bouclier de protection des données (composé d'un ou de trois arbitres, comme convenu par les 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 adhérant au bouclier de protection des données pourront demander le contrôle juridictionnel et l'application des décisions d'arbitrage conformément à la législation américaine au titre de la loi fédérale sur l'arbitrage (*Federal Arbitration Act ou FAA*).

([1]) Section I.5 des principes.

e) Recours et sanctions

Tout recours auprès de l'organisme d'instruction 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, le cas échéant, à l'arrêt du traitement des données personnelles de la personne qui a déposé la plainte. Les sanctions doivent être suffisamment sévères pour garantir le respect des principes de la part de l'organisation. Une série de sanctions ayant des degrés de sévérité différents permettra aux instances de résolution des litiges de répondre de manière adéquate à des niveaux différents de non-respect. Les sanctions doivent inclure à la fois la publication des violations et l'obligation d'effacer les données dans certaines circonstances ([1]). 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 organismes de résolution des litiges et d'autoréglementation du secteur privé doivent signaler aux tribunaux ou aux pouvoirs publics compétents, selon le cas, les organisations adhérant aux principes du bouclier de protection des données qui ne respectent pas leurs décisions et en informer le ministère.

f) Action de la FTC

La FTC s'est engagée à examiner en priorité les cas de non-conformité alléguée par rapport aux principes, soumis par: i) les organisations d'autoréglementation en matière de protection de la vie privée et les autres organismes indépendants d'instruction des litiges; ii) les États membres de l'Union européenne; et iii) le ministère, afin de déterminer s'il y a eu une violation de la section 5 de la Federal Trade Commission 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 obtenant 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. Ces infractions incluent les déclarations mensongères d'adhésion aux principes du bouclier de protection des données ou de participation au bouclier de protection des données par des organisations qui ont été supprimées de la liste du bouclier de protection des données ou qui ne se sont jamais autocertifiées 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 criminelle 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 déterminant l'adhésion aux principes du bouclier de protection des données.

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 bouclier de protection des données. Les organisations qui ne respectent pas les principes de manière persistante seront supprimées de la liste du bouclier de protection des données par le ministère, et elles devront restituer ou supprimer les informations à caractère personnel reçues dans le cadre du bouclier de protection des données.

ii) Il y a non-respect persistant lorsqu'une organisation qui a déclaré son adhésion aux principes au ministère 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 un organisme public, ou lorsqu'un tel organisme constate qu'elle viole fréquemment les principes, au point que sa déclaration d'adhésion n'est plus crédible. L'organisation doit alors en informer sans retard le ministère du commerce. 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 bouclier de protection des données en réaction à toute notification de non-respect persistant qu'il recevrait, qu'elle provienne de l'organisation elle-même, d'un organisme d'autoréglementation du respect de la vie privée, d'un autre organisme indépendant d'instruction 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. La liste publique du bouclier de protection des données

([1]) Les circonstances dans lesquelles ces sanctions doivent être appliquées sont laissées à l'appréciation des organismes d'instruction 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 divulguées en violation manifeste des principes du bouclier de protection des données.

tenue par le ministère précisera donc quelles organisations bénéficient des avantages du bouclier de protection des données 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 bouclier de protection des données devra fournir à cet organisme des informations exhaustives sur sa participation antérieure au bouclier de protection des données.

12. **Choix — Moment de l'exercice du droit de refus (ou de choix)**

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 de choix) 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 par le biais d'un programme central de refus, tel que le «mail preference service» de la Direct Marketing Association. Les organisations participant au «mail preference service» de la Direct Marketing Association devraient promouvoir la disponibilité de celui-ci auprès des consommateurs ne souhaitant pas recevoir d'informations commerciales. 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 aucun 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 aux organisations situées en dehors de l'Union européenne 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. Conformément à l'article 26 de la directive, les données à caractère personnel peuvent être transférées vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25, paragraphe 2, à condition: i) que le transfert soit nécessaire à la prestation des services demandés par le client ou à l'exécution d'un contrat, tel qu'un contrat «de fidélité»; ou ii) que le passager ait indubitablement donné son consentement. Les organisations américaines adhérant aux principes du bouclier de protection des données assurent une protection adéquate des données à caractère personnel et peuvent donc recevoir ces données de l'Union européenne sans satisfaire à ces conditions ni aux autres conditions spécifiées par l'article 26 de la directive. Étant donné que les principes du bouclier de protection des données comportent 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 adhérant aux principes du bouclier de protection des données. L'organisation transférant l'information doit cependant appliquer dans chaque cas la législation nationale de l'État membre de l'Union européenne 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 européenne ou des principes du bouclier de protection des données

La législation des États membres de l'Union européenne s'applique à la collecte des données personnelles et à tout traitement intervenant avant le transfert aux États-Unis. Les principes du bouclier de protection des données 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 personnelles élaborées dans le cadre d'études médicales ou pharmaceutiques jouent souvent un rôle précieux dans la recherche scientifique. Lorsque les données personnelles recueillies pour une étude sont transférées à une organisation des États-Unis dans le cadre du bouclier de protection des données, 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 recueillies ou auxquels la personne concernée a consenti par la suite, il convient d'obtenir un nouveau consentement.

c) Retrait d'un essai clinique

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 recueillies avant le retrait peuvent encore être traitées avec les autres données recueillies 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

Les sociétés d'appareils pharmaceutiques et médicaux ont le droit de fournir des données personnelles 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 mettrait en question 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

Les sociétés d'appareils pharmaceutiques ou médicaux ne doivent pas appliquer les principes du bouclier de protection des données «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

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 intéressés. 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 personnelles ainsi codées ne représente pas un transfert de données à caractère personnel soumis aux principes du bouclier de protection des données.

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» relevant du bouclier de protection des données 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 bouclier de protection des données.

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 adhérant au bouclier de protection des données 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 adhérant au bouclier de protection des données, associées aux informations publiées par le secteur du renseignement et d'autres informations, peuvent être utilisées pour éclairer l'examen annuel conjoint du fonctionnement du bouclier de protection des données 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 d'arbitrage

La présente annexe I définit les conditions selon lesquelles les organisations adhérant au bouclier de protection des données 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 bouclier de protection des données UE–États-Unis. Cette option vise à proposer un mécanisme rapide, indépendant et équitable, selon le choix des personnes concernées, permettant de résoudre les violations alléguées des principes, qui n'ont pas été résolues par les autres mécanismes mis en place au titre du bouclier de protection des données, le cas échéant.

A. **Portée**

Un particulier peut opter pour l'arbitrage en vue de déterminer, pour les plaintes résiduelles, si une organisation adhérant au bouclier de protection des données n'a pas satisfait à ses obligations au titre des principes envers ce particulier et si cette infraction reste entièrement ou partiellement sans réparation. Cette possibilité est offerte uniquement à ces fins. Cette option 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 bouclier de protection des données.

B. **Recours possibles**

Dans le cadre de cette option d'arbitrage, le panel du bouclier de protection des données (composé d'un ou de trois arbitres, comme convenu par les 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. Il s'agit des seuls pouvoirs du panel d'arbitrage en matière de recours. Dans son examen des recours, le panel d'arbitrage est tenu de prendre en considération les recours déjà imposés par d'autres instances dans le cadre du bouclier de protection des données. Les recours en dommages-intérêts, portant sur des honoraires, frais ou dépens, et les autres recours 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 III.11(d)(i) des principes; 2) faire appel à l'instance de recours indépendante prévue par les principes, gratuite pour les particuliers; et 3) faire part du problème au ministère du commerce par l'intermédiaire de son autorité chargée de la protection des données et laisser au ministère du commerce 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* (administration du commerce international) du ministère du commerce, sans aucun 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 judiciaire 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 autorité chargée de la protection des données (APD) de l'Union européenne: 1) est compétente au titre des sections III.5 ou III.9 des principes; 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 européenne n'empêche pas à elle seule d'invoquer 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 se prévaloir de cette option d'arbitrage contraignant est entièrement volontaire. Les décisions d'arbitrage 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]) Section I.5 des principes.

E. **Contrôle et application**

Les personnes concernées et les organisations adhérant au bouclier de protection des données pourront demander le contrôle juridictionnel et la mise en application des décisions d'arbitrage conformément à la législation américaine au titre de la *Federal Arbitration Act* ([1]). Tout dossier de ce type doit être porté devant le tribunal fédéral de première instance compétent pour le lieu principal d'activité de l'organisation adhérant au bouclier de protection des données.

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 les procédures d'arbitrage futures devant les tribunaux de l'Union européenne ou des États-Unis ou dans le cadre de procédures lancées par la Commission fédérale du commerce (*Federal Trade Commission* — FTC).

F. **Le panel d'arbitrage**

Les parties sélectionneront les arbitres parmi la liste d'arbitres examinée ci-dessous.

Conformément au droit applicable, le ministère du commerce américain et la Commission européenne dresseront une liste de 20 arbitres, sélectionnés sur la base de leur indépendance, de leur intégrité et de leur expertise. Ce processus sera soumis aux principes suivants:

Les arbitres:

1) resteront sur la liste pendant une période de 3 ans, sauf circonstances exceptionnelles ou motif valable, cette période étant renouvelable une fois;

2) ne recevront aucune consigne ni des parties, ni d'une organisation adhérant au bouclier de protection des données, ni des États-Unis, de l'Union européenne ou d'un État membre de l'Union européenne, 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 européen en matière de protection des données.

G. **Procédures d'arbitrage**

Conformément au droit en vigueur, dans un délai de 6 mois à compter de la décision constatant le niveau de protection adéquat, le ministère du commerce et la Commission européenne conviendront d'adopter un ensemble existant et bien établi de procédures arbitrales américaines (comme les procédures AAA ou JAMS) pour régir les procédures devant le panel du bouclier de protection des données, sous réserve des considérations suivantes:

1) Un particulier 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.

([1]) Le chapitre 2 de la *Federal Arbitration Act* («FAA») dispose qu'«un 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.

2) Des procédures seront mises en place afin que la 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 européenne ou d'un État membre de l'Union européenne ou de tout autre organe étatique, autorité publique ou autorité répressive ne peut participer à ces arbitrages, étant entendu qu'à la demande d'un particulier de l'Union européenne, les APD de l'Union européenne peuvent apporter une assistance dans la préparation de la notification uniquement. Les APD de l'Union européenne ne peuvent par contre 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 du fait que le particulier est représenté ou non 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 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.

H. **Coûts**

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

Sous réserve de la législation en vigueur, et en concertation avec la Commission européenne, le ministère du commerce facilitera la création d'un fonds auquel les organisations adhérant au bouclier de protection des données seront tenues d'apporter une contribution annuelle basée en partie sur leur taille et qui couvrira les coûts d'arbitrage, y compris les honoraires des arbitres, jusqu'à des montants plafonnés. Le fonds sera géré par une partie tierce qui rendra compte régulièrement de son fonctionnement. Lors du réexamen annuel, le ministère du commerce et la Commission européenne examineront le fonctionnement du fonds, notamment la nécessité éventuelle d'ajuster le montant des contributions ou des plafonds, et prendront 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 adhérant au bouclier de protection des données. Les honoraires d'avocats ne sont pas couverts par la présente disposition ni par aucun fonds relevant de la présente disposition.

ANNEXE III

Lettre de M. John Kerry, secrétaire d'État américain

Le 7 juillet 2016

Madame la Commissaire,

Je suis heureux que nous soyons parvenus à un accord sur le bouclier de protection des données UE–États-Unis qui inclura un mécanisme de médiation par lequel les autorités de l'Union européenne pourront soumettre des demandes au nom de citoyens de l'Union concernant les pratiques de renseignement d'origine électromagnétique des États-Unis.

Le 17 janvier 2014, le président Barack Obama a annoncé d'importantes réformes concernant le renseignement décrites dans la directive présidentielle n° 28 (PPD-28). En vertu de la PPD-28, j'ai désigné la sous-secrétaire d'État Catherine A. Novelli, qui est également coordinatrice principale de la diplomatie internationale en matière de technologie de l'information, comme point de contact des États-Unis vis-à-vis des gouvernements étrangers qui souhaitent exprimer leurs préoccupations concernant les activités de renseignement d'origine électromagnétique des États-Unis. Sur cette base, j'ai mis en place un mécanisme de médiation dans le cadre du bouclier de protection des données conformément aux conditions indiquées à l'annexe A, ayant fait l'objet d'une mise à jour depuis ma lettre du 22 février 2016. J'ai chargé la sous-secrétaire Catherine A. Novelli d'assurer la fonction de médiateur. La sous-secrétaire Catherine A. Novelli est indépendante des services de renseignement américains et me rend compte directement.

J'ai donné consigne à mon équipe de consacrer les ressources nécessaires à la mise en œuvre de ce nouveau mécanisme de médiation, et je suis convaincu qu'il constituera un moyen efficace de répondre aux préoccupations des citoyens de l'Union européenne.

Veuillez agréer, Madame la Commissaire,
l'expression de ma considération distinguée.

John F. Kerry

Annexe A

Mécanisme de médiation du bouclier de protection des données UE–États-Unis concernant le renseignement d'origine électromagnétique

Eu égard à l'importance que revêt le cadre que constitue le bouclier de protection des données UE–États-Unis, le présent mémorandum décrit la procédure de mise en œuvre d'un nouveau mécanisme, en conformité avec la directive présidentielle n° 28 (PPD-28), concernant le renseignement d'origine électromagnétique ([1]).

Le 17 janvier 2014, le président Obama a prononcé un discours annonçant d'importantes réformes en matière de renseignement. Dans ce discours, il a souligné que «[n]os efforts contribuent à protéger non seulement notre nation, mais aussi nos amis et alliés. Nos efforts ne porteront leurs fruits que si les citoyens d'autres pays sont convaincus que les États-Unis respectent aussi leur vie privée». Le président Obama a annoncé l'adoption d'une nouvelle directive présidentielle, la PPD-28, en vue de «fixer clairement ce que nous faisons, et ce que nous ne faisons pas, en matière de surveillance à l'étranger».

La section 4(d) de la PPD-28 charge le secrétaire d'État de désigner un «coordinateur principal de la diplomatie internationale en matière de technologie de l'information» (le coordinateur principal) pour «servir de point de contact en ce qui concerne les activités de renseignement d'origine électromagnétique menées par les États-Unis». La sous-secrétaire Catherine A. Novelli assume la fonction de coordinatrice principale depuis janvier 2015.

Le présent mémorandum décrit un nouveau mécanisme que la coordinatrice principale appliquera afin de faciliter le traitement des demandes et la formulation des réponses aux demandes concernant l'accès pour raison de sécurité nationale aux données transmises depuis l'Union européenne vers les États-Unis au titre du bouclier de protection des données, de clauses contractuelles types, de règles d'entreprise contraignantes, de «dérogations» ([2]) ou d'«éventuelles futures dérogations» ([3]) par les voies établies conformément à la législation et à la politique américaines en vigueur.

1) **Le médiateur du bouclier de protection des données.** La coordinatrice principale assumera les fonctions de médiateur du bouclier de protection des données et désignera, selon les besoins, d'autres fonctionnaires du département d'État chargés de l'aider à s'acquitter de ses responsabilités décrites dans le présent mémorandum. (La coordinatrice et tous les fonctionnaires chargés de ces tâches sont désignés ci-après par les termes «médiateur du bouclier de protection des données» ou «médiateur».) Le médiateur du bouclier de protection des données travaillera en étroite collaboration avec les fonctionnaires d'autres ministères et agences chargés de traiter les demandes dans le respect de la législation et de la politique américaines en vigueur. Le médiateur est indépendant des services de renseignement. Il rend compte directement au secrétaire d'État, qui veillera à ce que le médiateur remplisse sa mission en toute objectivité et à l'abri de toute influence inappropriée susceptible d'affecter la réponse qu'il devra donner.

2) **Coordination efficace.** Le médiateur du bouclier de protection des données sera en mesure de faire appel aux organes de surveillance décrits ci-dessous et de les coordonner de manière efficace, afin de garantir que sa réponse aux demandes émanant de l'organe européen de traitement des plaintes individuelles s'appuie sur les informations

([1]) Pour autant que la décision de la Commission constatant le caractère adéquat du niveau de protection assurée par le bouclier de protection des données UE–États-Unis s'applique à l'Islande, au Liechtenstein et à la Norvège, le paquet «bouclier de protection des données» couvrira non seulement l'Union européenne, mais également ces trois pays. Dès lors, les références à l'Union européenne et à ses États membres doivent s'entendre comme incluant également l'Islande, le Liechtenstein et la Norvège.

([2]) Dans ce contexte, on entend par «dérogations» un ou plusieurs transferts commerciaux effectués à la condition: a) que la personne concernée ait indubitablement donné son consentement au transfert envisagé; ou b) que le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée; ou c) que le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers; ou d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice; ou e) que le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée; ou f) que le transfert intervienne au départ d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

([3]) Dans ce contexte, on entend par «éventuelles futures dérogations» un ou plusieurs transferts commerciaux effectués sur la base de l'une des conditions suivantes, dans la mesure où la condition constitue un motif licite de transfert de données à caractère personnel depuis l'Union européenne vers les États-Unis: a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées; ou b) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; ou c) dans le cas d'un transfert vers un pays tiers ou une organisation internationale et lorsque aucune des autres dérogations ou aucune éventuelle future dérogation n'est applicable, uniquement s'il n'est pas répétitif, s'il concerne uniquement un nombre limité de personnes concernées, s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits et libertés de la personne concernée, et à condition que le responsable du traitement ait évalué toutes les circonstances relatives au transfert de données et offert, sur la base de cette évaluation, des garanties appropriées au regard de la protection des données à caractère personnel.

pertinentes. Lorsque les demandes portent sur la compatibilité de la surveillance avec le droit américain, le médiateur pourra coopérer avec l'un des organes de surveillance indépendants dotés de pouvoirs d'enquête.

a) Le médiateur du bouclier de protection des données travaillera en étroite collaboration avec d'autres représentants du gouvernement américain, et notamment les organes de surveillance indépendants appropriés, afin que les demandes complétées soient traitées et résolues conformément aux lois et politiques en vigueur. Le médiateur du bouclier de protection des données sera notamment en mesure d'assurer une coordination étroite avec le bureau du directeur du renseignement national (*Office of the Director of National Intelligence*), le ministère de la justice et d'autres départements et agences impliqués dans la sécurité nationale des États-Unis selon les besoins, ainsi qu'avec les inspecteurs généraux, les responsables de l'application de la loi sur la liberté de l'information et les responsables des libertés civiles et du respect de la vie privée.

b) Le gouvernement des États-Unis contribuera, en s'appuyant sur des mécanismes de coordination et de surveillance des questions de sécurité nationale entre les départements et agences, à ce que le médiateur du bouclier de protection des données soit en mesure de répondre, au sens de la section 4(e), aux demandes complétées au titre de la section 3(b).

c) Le médiateur du bouclier de protection des données peut soumettre au conseil de surveillance de la vie privée et des libertés civiles (*Privacy and Civil Liberties Oversight Board*) des questions liées aux demandes.

3) **Soumission des demandes**

a) Toute demande sera soumise initialement à l'autorité de contrôle de l'État membre chargée de la surveillance des services de sécurité nationale et/ou du traitement des données personnelles par les autorités publiques. La demande sera soumise au médiateur par l'intermédiaire d'un organisme centralisé de l'Union européenne (ci-après, conjointement, l'«organe européen de traitement des plaintes individuelles»).

b) L'organe européen de traitement des plaintes individuelles s'assurera que la demande est complète en accomplissant les actions suivantes:

i) vérifier l'identité de la personne et vérifier que la personne agit pour son propre compte, et non en qualité de représentant d'une organisation gouvernementale ou intergouvernementale;

ii) s'assurer que la demande est faite par écrit et qu'elle contient les informations de base suivantes:

— toute information constituant le fondement de la demande,

— la nature des informations ou de la réparation demandées,

— les entités du gouvernement américain dont la personne pense qu'elles sont impliquées, le cas échéant, et

— les autres mesures prises pour obtenir les informations ou la réparation demandées et les réponses obtenues à la suite de ces autres mesures;

iii) vérifier que la demande porte sur des données dont on peut raisonnablement penser qu'elles ont été transférées depuis l'Union européenne vers les États-Unis au titre du bouclier de protection des données, de clauses contractuelles types, de règles d'entreprise contraignantes, de dérogations ou d'éventuelles futures dérogations;

iv) constater qu'a priori la demande n'est pas dénuée de fondement, vexatoire ou faite de mauvaise foi.

c) Pour être complète aux fins de la poursuite du traitement par le médiateur du bouclier de protection des données au titre du présent mémorandum, la demande ne doit pas démontrer que les données du demandeur ont effectivement été consultées par le gouvernement des États-Unis dans le cadre d'activités de renseignement d'origine électromagnétique.

4) **Engagements concernant la communication avec l'organe européen de traitement des plaintes individuelles soumettant la demande**

a) Le médiateur du bouclier de protection des données accusera réception de la demande auprès de l'organe européen des plaintes individuelles qui soumet cette demande.

b) Le médiateur du bouclier de protection des données procédera à un premier examen pour s'assurer que la demande a été complétée conformément à la section 3 b). Si le médiateur du bouclier de protection des données relève des lacunes ou s'il a des questions concernant le caractère complet de la demande, il s'efforcera de résoudre ces problèmes en collaboration avec l'organe européen de traitement des plaintes individuelles qui soumet la demande.

c) Si, afin de faciliter un traitement approprié de la demande, le médiateur du bouclier de protection des données a besoin de plus d'informations concernant la demande, ou si la personne qui a soumis la demande à l'origine doit entreprendre des démarches supplémentaires, le médiateur du bouclier de protection des données en informera l'organe européen de traitement des plaintes individuelles qui a soumis la demande.

d) Le médiateur du bouclier de protection des données assurera le suivi des demandes et informera l'organe européen de traitement des plaintes individuelles qui a soumis la demande des progrès réalisés, le cas échéant.

e) Une fois une demande complétée au sens de la section 3 du présent mémorandum, le médiateur du bouclier de protection des données apportera sans retard une réponse appropriée à l'organe européen de traitement des plaintes individuelles qui a soumis la demande, dans le respect de l'obligation de protection des informations en vertu des lois et politiques en vigueur. Le médiateur du bouclier de protection des données fournira à l'organe européen de traitement des plaintes individuelles qui a soumis la demande une réponse confirmant: i) que la plainte a été correctement instruite; et ii) que les lois et autres actes législatifs, ordonnances exécutives, directives présidentielles et politiques des agences des États-Unis, compte tenu des limites et garanties décrites dans la lettre du bureau du directeur du renseignement nationaux, ont été respectées ou, dans l'hypothèse inverse, que ces cas de non-respect ont été corrigés. Le médiateur du bouclier de protection des données ne confirmera ni ne démentira que la personne a fait l'objet d'une surveillance, pas plus qu'il ne confirmera la mesure de réparation spécifique appliquée. Ainsi qu'il est expliqué plus en détail à la section 5, les demandes au titre de la loi sur la liberté de l'information (*Freedom of Information Act*, FOIA) seront traitées conformément à cet acte législatif et à la réglementation en vigueur.

f) Le médiateur du bouclier de protection des données communiquera directement avec l'organe européen de traitement des plaintes individuelles, qui sera chargé à son tour de communiquer avec la personne qui a soumis la demande. Dans le cas où l'un des processus sous-jacents décrits ci-dessous inclut des communications directes, ces communications seront assurées dans le respect des procédures existantes.

g) Les engagements pris dans le présent mémorandum ne s'appliqueront pas aux allégations d'ordre général concernant la non-conformité du bouclier de protection des données UE–États-Unis aux exigences de l'Union européenne en matière de protection des données. Les engagements pris dans le présent mémorandum tiennent compte du fait, admis tant par la Commission européenne que par le gouvernement américain, qu'étant donné la portée des engagements pris au titre de ce mécanisme, des limites en termes de ressources sont à prévoir, notamment en ce qui concerne les demandes relatives à la FOIA. Si la réalisation des tâches dévolues au médiateur du bouclier de protection des données excédait des limites raisonnables en termes de ressources raisonnables et rendait impossible le respect de ces engagements, le gouvernement des États-Unis discuterait avec la Commission européenne des ajustements à envisager pour corriger la situation.

5) **Demandes de renseignements.** Des demandes d'accès aux archives du gouvernement américain peuvent être introduites et traitées en vertu de la loi sur la liberté de l'information (FOIA).

a) La FOIA permet à toute personne, quelle que soit sa nationalité, de demander l'accès aux archives existantes des agences fédérales. Cet acte législatif est inscrit au Code des États-Unis (*United States Code*, U.S.C.) au chapitre 5 U.S. C. § 552. Le texte de cet acte législatif ainsi que des informations supplémentaires concernant la FOIA sont disponibles à l'adresse www.FOIA.gov et http://www.justice.gov/oip/foia-resources. Toutes les agences disposent d'un responsable pour la FOIA et fournissent des informations sur leur site internet public concernant la façon de leur soumettre une demande au titre de cette loi. Les agences ont mis en place des procédures de consultation réciproque concernant les demandes présentées au titre de la FOIA et visant les archives d'une autre agence.

b) Par exemple:

i) Le bureau du directeur du renseignement national (*Office of the Director of National Intelligence*, ODNI) a mis en place le portail FOIA pour l'ODNI: http://www.dni.gov/index.php/about-this-site/foia. Ce portail fournit des informations sur la façon de soumettre une demande, de vérifier l'état d'avancement d'une demande en cours et d'accéder aux informations communiquées et publiées par l'ODNI au titre de la FOIA. Le portail FOIA de l'ODNI inclut des liens vers d'autres sites FOIA pour les différentes composantes des services de renseignement: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Le bureau de la politique de l'information (*Office of Information Policy*) du ministère de la justice fournit des informations complètes concernant la FOIA: http://www.justice.gov/oip. Ce site présente non seulement des informations concernant la façon de soumettre une demande au titre de la FOIA au ministère de la justice, mais aussi des orientations destinées aux pouvoirs publics américains quant à la façon d'interpréter et d'appliquer les exigences de la FOIA.

c) En vertu de la FOIA, l'accès aux archives des pouvoirs publics est soumis à un certain nombre d'exceptions reprises dans une liste. Il s'agit notamment des limites imposées à l'accès aux informations classifiées de sécurité nationale, aux informations à caractère personnel de tiers, et aux informations relatives aux enquêtes des services répressifs. Ces restrictions sont comparables aux limites imposées par les États membres de l'Union européenne matière d'accès à l'information. Ces restrictions s'appliquent tout autant aux citoyens américains qu'aux ressortissants d'autres pays.

d) Les litiges relatifs à la communication d'archives demandées au titre de la FOIA peuvent être portés devant une juridiction administrative, puis devant un tribunal fédéral. Le tribunal est alors amené à déterminer de novo si l'accès aux archives en question a été refusé à juste titre [5 U.S.C. § 552(a)(4)(B)]. Il peut obliger le gouvernement à accorder l'accès aux archives en question. Il est arrivé que les tribunaux infirment les allégations des pouvoirs publics selon lesquelles l'accès aux informations devait être refusé car elles étaient classifiées. Si aucune réparation financière ne peut être obtenue, les tribunaux peuvent accorder le remboursement des frais d'avocat.

6) **Demandes d'actions supplémentaires.** Toute demande affirmant qu'il y a eu violation de la loi ou autre action fautive sera transmise à l'organisme gouvernemental américain approprié, y compris à un organe de surveillance indépendant, compétent pour instruire la demande concernée et pour remédier aux manquements, comme décrit ci-dessous.

a) Les inspecteurs généraux bénéficient d'une indépendance statutaire. Ils disposent d'un large pouvoir d'appréciation pour réaliser des enquêtes, des audits et des examens des programmes, y compris en ce qui concerne les fraudes, abus ou violations de la loi. Ils peuvent également recommander des mesures correctives.

i) La loi sur les inspecteurs généraux (*Inspector General Act*) de 1978, telle que modifiée, a instauré des inspecteurs généraux (IG) fédéraux en tant qu'unités indépendantes et impartiales au sein de la plupart des agences chargées de lutter contre le gaspillage, la fraude et les abus dans les programmes et les activités de leurs agences respectives. À cette fin, chaque IG est chargé de mener des audits et des enquêtes sur les programmes et activités de son agence. En outre, les IG donnent une impulsion, assurent une coordination et recommandent des politiques en vue d'actions visant à promouvoir l'économie, l'efficience et l'efficacité, et à prévenir et déceler les fraudes et les abus dans les programmes et activités des agences.

ii) Chaque composante des services de renseignement (*Intelligence Community*) possède son propre bureau de l'inspecteur général chargé, entre autres, de surveiller les activités de renseignement à l'étranger. Différents rapports des inspecteurs généraux concernant les programmes de renseignement ont été publiés.

iii) Par exemple:

— Le bureau de l'inspecteur général des services de renseignement (IC IG) a été créé conformément à la section 405 de la loi d'habilitation des services de renseignement pour l'exercice 2010 (Intelligence Authorization Act of Fiscal Year 2010). L'IC IG est chargé de réaliser des audits, des enquêtes, des inspections et des examens sur l'ensemble des services de renseignement en vue de recenser et de combattre les risques, points faibles et lacunes systémiques touchant toutes les missions des agences de renseignement, afin d'avoir une incidence positive sur l'économie et l'efficience du secteur dans l'ensemble. L'IC IG est autorisé à enquêter sur la base de plaintes ou d'informations concernant des allégations de violation de la loi, des règles et des réglementations, ainsi que des allégations de gaspillage, de fraude, d'abus de pouvoir ou de danger grave et précis pour la santé et la sécurité publiques en lien avec l'ODNI et/ou les programmes et activités des services de renseignement. L'IC IG fournit des informations sur la façon de le contacter directement afin de soumettre un rapport: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— Le bureau de l'inspecteur général (*Office of the Inspector General*, OIG) du ministère américain de la justice (*Department of Justice*, DOJ) est une entité indépendante instituée par la loi et qui a pour mission de détecter et de décourager le gaspillage, la fraude, les abus et les actions fautives dans les programmes et au sein du personnel du DOJ, et de promouvoir l'économie et l'efficience dans ces programmes. L'OIG enquête sur les violations alléguées du droit pénal et civil par des employés du DOJ et effectue également des audits et des inspections de ses programmes. L'OIG est compétent pour statuer sur toutes les plaintes pour action fautive déposées à l'encontre des employés du ministère de la justice, y compris les agences et services suivants: *Federal Bureau of Investigation*; *Drug Enforcement Administration*; *Federal Bureau of Prisons*; *U. S. Marshals Service*; *Bureau of Alcohol, Tobacco, Firearms, and Explosives*; *United States Attorneys Offices*, ainsi que sur les plaintes à l'encontre des employés travaillant dans d'autres divisions ou bureaux du ministère de la justice (La seule exception est que les allégations d'action fautive de la part d'un avocat employé par le ministère ou des membres du personnel répressif en lien avec le mandat donné à l'avocat du ministère

d'instruire, de plaider ou de fournir des conseils juridiques relèvent de la compétence du bureau de la responsabilité professionnelle du ministère.) Par ailleurs, la section 1001 de la loi USA PATRIOT, promulguée le 26 octobre 2001, charge l'inspecteur général d'examiner les informations et de recevoir les plaintes faisant état d'atteintes aux droits civils et aux libertés civiles par des employés du ministère de la justice. L'OIG possède un site internet public — https://www.oig.justice.gov — intégrant un «service d'appel d'urgence» pour la soumission de plaintes — https://www.oig.justice.gov/hotline/index.htm.

b) Les bureaux et entités chargés de la protection de la vie privée et des libertés civiles au sein des pouvoirs publics américains sont également dotés de responsabilités en la matière. Par exemple:

i) La section 803 de la loi de 2007 mettant en œuvre les recommandations de la commission du 11 septembre (*9/11 Commission Act*), inscrit au Code des États-Unis au chapitre 42 U.S.C. § 2000-ee1, instaure des responsables de la vie privée et des libertés civiles au sein de certains ministères et agences (notamment le département d'État, le ministère de la justice et l'ODNI). La section 803 prévoit que ces responsables de la vie privée et des libertés civiles joueront le rôle de conseillers principaux en vue, notamment, de veiller à ce que ces ministères, agences ou composantes disposent de procédures adéquates pour traiter les plaintes émanant de particuliers affirmant que ces services ont violé leur vie privée ou leurs libertés civiles.

ii) Le bureau des libertés civiles et de la vie privée de l'ODNI (ODNI CLPO) est dirigé par le responsable de la protection des libertés civiles de l'ODNI, un poste institué par la loi sur la sécurité nationale (*National Security Act*) de 1948 telle que modifiée. L'ODNI CLPO a notamment pour mission de s'assurer que les politiques et procédures des différentes composantes des services de renseignement prévoient des mesures de protection adéquates de la vie privée et des libertés civiles, et d'examiner et d'instruire les plaintes faisant état d'abus ou d'atteintes aux libertés civiles et à la vie privée dans les programmes et activités de l'ODNI. L'ODNI CLPO fournit des informations au public sur son site internet, notamment des instructions sur la façon de soumettre une plainte: www.dni.gov/clpo. Si l'ODNI CLPO reçoit une plainte relative à la vie privée et aux libertés civiles impliquant les programmes et activités des services de renseignement, il consulte les autres composantes des services de renseignement pour déterminer comment traiter cette plainte au sein du secteur. On notera que l'Agence nationale de sécurité (National Security Agency, NSA) possède son propre bureau des libertés civiles et de la vie privée, qui fournit des informations relatives à ses responsabilités sur son site internet https://www.nsa.gov/civil_liberties/. Si des informations indiquent qu'une agence ne respecte pas ses obligations en matière de protection de la vie privée (par ex. une exigence aux termes de la section 4 de la PPD-28), les agences disposent de mécanismes de mise en conformité permettant d'analyser l'incident et d'y remédier. En vertu de la PPD-28, les agences sont tenues de signaler les incidents de conformité à l'ODNI.

iii) Le bureau la vie privée et des libertés civiles (OPCL) du ministère de la justice assiste le responsable en chef de la vie privée et des libertés civiles (CPCLO) du ministère dans ses missions et responsabilités. L'OPCL a pour mission principale de protéger la vie privée et les libertés civiles des citoyens américains par l'examen, la surveillance et la coordination des activités du ministère concernant la protection de la vie privée. L'OPCL fournit des conseils juridiques et des orientations aux différentes composantes du ministère et garantit le respect par le ministère de la réglementation en la matière, et notamment le respect de la loi sur la protection de la vie privée (*Privacy Act*) de 1974, des dispositions relatives à la vie privée de la loi sur l'administration en ligne (*E-Government Act*) de 2002 et de la loi fédérale sur la gestion de la sécurité de l'information (*Federal Information Security Management Act*), ainsi que des directives administratives adoptées sur la base de ces lois. Il élabore et organise les formations au respect de la vie privée au sein du ministère, il aide le CPCLO à élaborer une politique ministérielle de respect de la vie privée, il prépare les rapports au président et au Congrès concernant la protection de la vie privée et il examine les pratiques de traitement des informations du ministère pour s'assurer qu'elles sont conformes à la protection de la vie privée et des libertés civiles. L'OPCL fournit au public des informations relatives à ses responsabilités à l'adresse suivante: http://www.justice.gov/opcl.

iv) En vertu du chapitre 42 U.S.C. § 2000ee *et seq*, le conseil de surveillance de la vie privée et des libertés civiles (*Privacy and Civil Liberties Oversight Board*, PCLOB) réexamine en permanence: i) les politiques et procédures adoptées et mises en œuvre par les ministères, agences et autres composantes du pouvoir exécutif dans le cadre des efforts déployés pour protéger la nation du terrorisme afin de s'assurer que la vie privée et les libertés civiles sont protégées; et ii) les autres actions du pouvoir exécutif liées à ces efforts afin de déterminer si ces actions protègent correctement la vie privée et les libertés civiles et sont conformes aux lois, réglementations et politiques en vigueur en matière de vie privée et de libertés civiles. Ce conseil reçoit et examine les rapports et autres informations des responsables de la vie privée et des responsables des libertés civiles et, si nécessaire, leur adresse des recommandations concernant leurs activités. La section 803 de la *9/11 Commission Act* de 2007, inscrite au Code des États-Unis au chapitre 42 U.S.C. § 2000-ee1, charge les responsables de la vie privée et des libertés civiles de huit agences fédérales (notamment le secrétaire de la défense, le secrétaire à

la sécurité intérieure, le directeur du renseignement national et le directeur de la CIA) et de toute autre agence désignée par le conseil de soumettre des rapports périodiques au PCLOB indiquant le nombre, la nature et la teneur des plaintes reçues par chacune de ces agences pour des violations alléguées. La législation d'habilitation du PCLOB charge le conseil de recevoir ces rapports et, si nécessaire, d'adresser des recommandations aux responsables de la vie privée et des libertés civiles concernant leurs activités.

ANNEXE IV

Lettre de M^me^ Edith Ramirez, présidente de la commission fédérale du commerce

Le 7 juillet 2016

PAR COURRIER ÉLECTRONIQUE

Věra Jourová
Commissaire pour la justice, les consommateurs et l'égalité des genres
Commission européenne
Rue de la Loi, 200
1049 Bruxelles
BELGIQUE

Madame la Commissaire,

La commission fédérale du commerce des États-Unis (*Federal Trade Commission*, FTC) apprécie l'occasion qui lui est donnée de décrire la manière dont elle applique le nouveau cadre du bouclier de protection des données UE–États-Unis (ci-après le «cadre du bouclier de protection des données» ou le «cadre»). Nous pensons que ce cadre jouera un rôle de premier plan pour faciliter des transactions commerciales respectueuses de la vie privée 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 européenne des mesures de protection considérables de leur vie privée. La FTC s'est engagée depuis longtemps à protéger la vie privée partout dans le monde et fera de l'application du nouveau cadre l'une de ses principales priorités. Nous expliquerons ci-dessous comment, de manière générale, la FTC a fait par le passé une application stricte des règles de respect de la vie privée, et notamment du programme initial de la sphère de sécurité (*SAFE Harbour*); nous décrirons ensuite l'approche adoptée par la FTC pour la mise en application du nouveau cadre.

La FTC a manifesté publiquement son engagement à appliquer le programme de la sphère de sécurité pour la première fois en 2000. Le président de la FTC de l'époque, Robert Pitofsky, avait alors envoyé à la Commission européenne une lettre décrivant l'engagement de la FTC à faire respecter de manière stricte les principes de la sphère de sécurité relatifs à la protection de la vie privée. La FTC a continué de respecter cet engagement moyennant près de 40 actions de mise en application, de nombreuses enquêtes complémentaires et une coopération avec différentes autorités chargées de la protection des données (ADP) de l'Union européenne sur des questions d'intérêt mutuel.

Après que la Commission européenne, en novembre 2013, a exprimé des inquiétudes concernant l'administration et la mise en application du programme de la sphère de sécurité, la FTC et le ministère américain du commerce ont entamé des consultations avec des représentants de la Commission européenne afin d'étudier les moyens de renforcer ce programme. Le 6 octobre 2015, tandis que ces consultations se poursuivaient, la Cour de justice européenne a rendu un arrêt dans l'affaire Schrems invalidant, entre autres, la décision de la Commission européenne constatant le niveau de protection adéquat du programme de la sphère de sécurité. À la suite de cette décision, nous avons continué de collaborer étroitement avec le ministère du commerce et avec la Commission européenne en vue de renforcer les mesures de protection de la vie privée des particuliers de l'Union européenne. Le cadre du bouclier de protection des données est le résultat de ces consultations. Comme pour le programme de la sphère de sécurité, la FTC s'engage aujourd'hui à faire respecter le nouveau cadre de manière stricte. La présente lettre consacre cet engagement.

Nous affirmons notamment notre engagement dans quatre domaines-clés: 1) la hiérarchisation et l'instruction des dossiers soumis; 2) la lutte contre les déclarations mensongères ou frauduleuses d'adhésion au bouclier de protection des données; 3) la poursuite du contrôle des ordonnances; et 4) le renforcement de l'engagement et de la coopération en matière de mise en application avec les ADP de l'Union européenne. Nous fournirons ci-dessous des informations détaillées concernant chacun de ces engagements et replacerons dans son contexte le rôle de la FTC en matière de protection de la vie privée des consommateurs et d'application de la sphère de sécurité; nous décrirons également le paysage général de la protection de la vie privée aux États-Unis ([1]).

I. CONTEXTE

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

([1]) Nous fournissons des informations supplémentaires concernant les lois américaines relatives à la protection de la vie privée au niveau fédéral comme au niveau des États à l'annexe A. En outre, une synthèse de nos activités récentes en matière de protection de la vie privée et de sécurité est disponible sur le site internet de la FTC à l'adresse: https://www.ftc.gov/reports/privacy-data-security-update-2015.

veille à l'application d'un large éventail de lois afin de protéger la confidentialité et la sécurité des données des consommateurs. La législation primaire mise en application par la FTC, la loi portant établissement de la commission fédérale du commerce (*FTC Act*), interdit les actes ou pratiques «déloyaux» et «frauduleux» dans le domaine du commerce ([1]).Une déclaration, omission ou pratique est frauduleuse si elle est concrète et susceptible d'induire en erreur des consommateurs agissant de manière raisonnable compte tenu des circonstances ([2]).Un acte ou une pratique sont déloyaux s'ils entraînent ou sont susceptibles 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 ([3]).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.

Au titre de la loi qui l'établit, le mandat de la FTC concerne le domaine du commerce. 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 ([4]). 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 déférer des dossiers, le cas échéant.

L'application de la législation est la pierre angulaire de l'approche de protection de la vie privée adoptée par la FTC. À ce jour, la FTC a intenté plus de 500 actions visant à protéger la confidentialité et la sécurité des informations des consommateurs. Ces dossiers couvrent aussi bien des informations en ligne que hors ligne et incluent des mesures de mise en application visant des petites comme des grandes entreprises qui, selon la FTC, n'ont pas mis correctement à l'écart certaines données sensibles à propos de consommateurs, n'ont pas sécurisé les informations à caractère personnel des consommateurs, ont suivi des consommateurs en ligne de manière frauduleuse, envoyé des courriers électroniques non désirés (spam) aux consommateurs, installé des logiciels espions ou malveillants sur les ordinateurs de consommateurs, enfreint les consignes «Do Not Call» (ne pas appeler) ou d'autres règles en matière de télémarketing et collecté et partagé de manière inappropriée des informations relatives aux consommateurs sur des appareils mobiles. Les activités de mise en application de la FTC, dans le monde physique comme dans le monde numérique, envoient un message important aux entreprises à propos de la nécessité de protéger la vie privée des consommateurs.

La FTC a également mené de nombreuses initiatives stratégiques qui visaient à renforcer la protection de la vie privée des consommateurs et qui guident son action de mise en application des lois. La FTC a organisé des ateliers et publié des rapports recommandant de bonnes pratiques en vue d'améliorer le respect de la vie privée dans l'écosystème mobile, de renforcer la transparence du secteur des sociétés de courtage de données, d'exploiter au maximum les avantages des mégadonnées tout en en atténuant les risques, en particulier pour les consommateurs à faibles revenus et négligés par les entreprises, et de mettre en exergue les implications pour la vie privée et la sécurité de la reconnaissance faciale et de l'internet des objets, entre autres.

La FTC mène également des initiatives de sensibilisation des consommateurs et des entreprises afin de renforcer l'impact de ces initiatives d'application des lois et d'élaboration de politiques. La FTC a utilisé différents outils (publications, ressources en ligne, ateliers et médias sociaux) afin de fournir des documents de sensibilisation sur un large éventail de sujets, notamment les applications mobiles, la vie privée des enfants et la sécurité des données. Plus récemment, la FTC a lancé son initiative «*Start With Security*» («Commençons par la sécurité»), qui présente aux entreprises de nouvelles lignes directrices fondées sur les enseignements tirés des dossiers de l'agence en matière de sécurité des données, ainsi qu'une série d'ateliers à travers le pays. Par ailleurs, la FTC est depuis longtemps à la pointe des initiatives visant à sensibiliser les consommateurs aux principes de base de la sécurité informatique. L'année dernière, notre site «OnGuard Online» et son pendant en espagnol «Alerta en Linea» ont été consultés plus de cinq millions de fois.

B. **Mesures de protection juridiques aux États-Unis bénéficiant aux consommateurs de l'Union européenne**

Le bouclier de protection des données s'inscrira dans le contexte plus large des mesures adoptées aux États-Unis qui protègent aussi les consommateurs de l'Union européenne de différentes façons.

([1]) 15 U.S.C. § 45(a).

([2]) Voir la déclaration de politique de la FTC en matière de fraude, jointe au dossier Cliffdale Assocs., Inc., 103 FTC 110, 174 (1984), disponible à l'adresse: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

([3]) Voir 15 U.S.C § 45(n); Déclaration de politique de la FTC concernant le caractère déloyal, jointe au dossier Int'l Harvester Co, 104 FTC 949, 1070 (1984), disponible à l'adresse https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

([4]) *Voir California Dental Ass'n v. FTC*, 526 U.S. 756 (1999).

L'interdiction des actes et pratiques déloyaux ou frauduleux instaurée par la *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, y compris la restitution, auxquelles il est possible de recourir pour protéger les consommateurs américains.

Il est clair que les activités de mise en application des lois de la FTC profitent aux consommateurs étrangers comme aux consommateurs américains. Ainsi, nos actions visant à faire respecter la section 5 de la FTC Act ont protégé la vie privée tant des consommateurs américains que des consommateurs étrangers. Dans une action intentée contre un courtier en informations, Accusearch, la FTC a avancé l'argument selon lequel la vente par cette société de registres téléphoniques confidentiels à des tiers sans en informer les consommateurs ni obtenir leur consentement constituait une pratique déloyale contraire à la section 5 de la *FTC Act*. Accusearch vendait des informations relatives à des consommateurs américains et étrangers ([1]). Le tribunal a prononcé une injonction interdisant à Accusearch, entre autres, de commercialiser ou de vendre les informations à caractère personnel des consommateurs sans leur consentement écrit, sauf dans les cas où il s'agissait d'informations publiques obtenues de façon licite, et a ordonné le versement d'indemnités à hauteur de près de 200 000 USD ([2]).

La transaction conclue par la FTC avec TRUSTe en est un autre exemple. Cet accord garantit que les consommateurs, y compris les consommateurs de l'Union européenne, peuvent se fier aux déclarations d'une organisation mondiale autoréglementée concernant son examen et sa certification de services en ligne nationaux et étrangers ([3]). Il importe de noter que notre action contre TRUSTe renforce aussi de façon plus générale le système d'autoréglementation de la protection de la vie privée en garantissant la responsabilité des entités qui jouent un rôle important dans les mécanismes d'autoréglementation, y compris les cadres transfrontaliers de lutte contre le piratage.

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 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. Outre les lois fédérales américaines dont la FTC assure l'application, certaines autres lois de protection des consommateurs et de la vie privée au niveau fédéral et au niveau des États sont susceptibles d'apporter des avantages aux consommateurs de l'Union européenne.

C. **Mise en application de la sphère de sécurité**

Dans le cadre de son programme de mise en application des règles en matière de vie privée et de sécurité, la FTC s'est également efforcée de protéger les consommateurs de l'Union européenne en menant des actions destinées à prévenir ou réparer toute violation des principes de la sphère de sécurité. La FTC a lancé 39 actions de mise en application liées à la sphère de sécurité: 36 actions faisaient état de fausses déclarations de certification et trois actions (contre Google, Facebook et Myspace) concernaient une violation alléguée des principes de la sphère de sécurité relatifs à la protection de la vie privée ([4]). Ces affaires démontrent la possibilité de faire respecter les principes de certification et les conséquences en cas de non-conformité. Des ordonnances par consentement sur vingt ans imposent à Google, Facebook et Myspace de mettre en œuvre des programmes complets de protection de la vie privée qui doivent être raisonnablement conçus pour lutter contre les risques pour la vie privée liés au développement et à la gestion de produits et services nouveaux et existants et pour protéger la vie privée et la confidentialité des informations à caractère personnel. Les programmes complets de protection de la vie privée imposés par ces ordonnances doivent identifier les risques substantiels prévisibles et mettre en place des mesures de contrôle pour lutter contre ces risques. Les entreprises doivent également se soumettre à des évaluations permanentes et indépendantes de leurs programmes de protection de la vie privée, qui doivent être communiquées à la FTC. Les ordonnances interdisent également à ces entreprises de faire de fausses déclarations quant à leurs pratiques en matière de protection de la vie privée et à leur participation à tout programme de protection de la vie privée ou de la sécurité. Cette interdiction s'applique aussi aux actes et pratiques des

([1]) Voir Commissariat à la protection de la vie privée du Canada, plainte au titre de la LPRPDE contre Accusearch, Inc., agissant sous l'appellation Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Le Commissariat à la protection de la vie privée du Canada a déposé un mémoire d'amicus curiae dans la procédure d'appel de l'action lancée par la FTC et mené sa propre enquête, qui a conclu que les pratiques d'Accusearch enfreignaient aussi la législation canadienne.

([2]) Voir *FTC v. Accusearch, Inc.*, No. 06CV015D (D. Wyo. Dec. 20, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Voir *In the Matter of True Ultimate Standards Everywhere, Inc.*, N° C-4512 (FTC 12 mars 2015) (décision et ordonnance), disponible à l'adresse https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Voir *In the Matter of Google, Inc.*, N° C-4336 (FTC 13 octobre 2011) (décision et ordonnance), disponible à l'adresse https://www ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Facebook, Inc.*, N° C-4365 (F.T.C. 27 juillet 2012) (décision et ordonnance), disponible à l'adresse https://www ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, N° C-4369 (F.T.C. 30 août 2012) (décision et ordonnance), disponible à l'adresse https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

entreprises dans le nouveau cadre du bouclier de protection des données. La FTC peut assurer l'exécution de ces ordonnances en réclamant des sanctions civiles. De fait, Google a payé une pénalité civile d'un montant record de 22,5 millions d'USD en 2012 à la suite d'allégations selon lesquelles elle avait violé l'ordonnance la concernant. Ces ordonnances de la FTC contribuent donc à protéger plus d'un milliard de consommateurs dans le monde, dont plusieurs centaines de millions en Europe.

Les actions intentées par la FTC se sont aussi centrées sur les déclarations mensongères, frauduleuses ou trompeuses de participation à la sphère de sécurité. La FTC prend ces déclarations au sérieux. Dans l'affaire FTC v. Karnani par exemple, la FTC a intenté en 2011 une action contre un site commercial basé aux États-Unis au motif que cette entreprise faisait croire aux consommateurs britanniques qu'elle était basée au Royaume-Uni, notamment en utilisant des noms de domaine en «.uk», en affichant ses prix en devise britannique et en se référant au système postal britannique ([1]). Cependant, au moment de recevoir les produits commandés, les consommateurs découvraient qu'ils devaient payer des droits à l'importation imprévus, que les garanties n'étaient pas valables au Royaume-Uni et que des frais étaient demandés pour obtenir un remboursement. La FTC a également conclu que les défendeurs avaient trompé les consommateurs concernant leur participation au programme de la sphère de sécurité. On notera que tous les consommateurs victimes se trouvaient au Royaume-Uni.

Bon nombre de nos autres dossiers de mise en application de la sphère de sécurité portaient sur des organisations qui avaient adhéré à ce programme mais qui n'avaient pas renouvelé leur certification annuelle tout en continuant à se présenter comme participants actuels. Comme indiqué ci-après, la FTC s'engage également à lutter contre les déclarations mensongères de participation au cadre du bouclier de protection des données. Ces activités stratégiques de mise en application des lois viendront s'ajouter aux démarches renforcées du ministère du commerce visant à vérifier le respect des exigences de certification et de recertification du programme, son contrôle de la conformité effective, notamment par l'utilisation de questionnaires adressés aux participants au cadre et ses efforts accrus visant à détecter toute affirmation mensongère d'adhésion au cadre et toute utilisation abusive du label de certification du cadre ([2]).

II. HIÉRARCHISATION ET INSTRUCTION DES DOSSIERS SOUMIS

Tout comme nous l'avons fait pour le programme de la sphère de sécurité, la FTC s'engage à donner la priorité aux dossiers soumis par des États membres de l'Union européenne dans le cadre du bouclier de protection des données. Nous donnerons également la priorité aux dossiers concernant la non-conformité aux lignes directrices d'autoréglementation liées au cadre du bouclier de protection des données par les organisations d'autoréglementation en matière de protection de la vie privée et d'autres organes indépendants de résolution des litiges.

Afin de faciliter la saisine par les États membres de l'Union européenne dans le cadre du bouclier de protection des données, la FTC met actuellement en place un processus normalisé de soumission et fournit des indications aux États membres de l'Union européenne quant aux informations les mieux à même d'aider la FTC dans l'instruction des dossiers. Dans le cadre de cette démarche, la FTC va désigner un point de contact en son sein pour les dossiers soumis par des États membres de l'Union européenne. 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 réception d'un dossier soumis par un État membre de l'Union européenne ou par une organisation d'autoréglementation, la FTC peut prendre différentes mesures pour corriger les problèmes soulevés. Nous pouvons, par exemple, examiner les politiques de protection de la vie privée de l'entreprise concernée, obtenir des informations complémentaires directement auprès de l'entreprise 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 de mesures de sensibilisation des entreprises et des consommateurs et, le cas échéant, lancer une procédure d'exécution.

La FTC s'engage également à échanger des informations avec les autorités de mise en application qui les 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

([1]) Voir *FTC v. Karnani*, N° 2:09-cv-05276 (C.D. Cal. 20 mai 2011) (ordonnance définitive stipulée), disponible à l'adresse https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; voir aussi Lesley FAIR, FTC Business Center Blog, *Around the World in Shady Ways*, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 juin 2011).

([2]) Lettre de M. Ken Hyatt, sous-secrétaire faisant fonction au commerce chargé du commerce international, administration du commerce international, à M^me^ Věra Jourová, commissaire pour la justice, les consommateurs et l'égalité des genres.

d'accroître l'efficacité des démarches visant à lutter contre les comportements répréhensibles. Si une autorité de mise en application soumettant un dossier souhaite obtenir des informations sur l'état d'avancement des dossiers soumis afin de mener sa propre procédure d'exécution, 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 ADP de l'Union européenne 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 agences étrangères de mise en application des lois lorsque l'agence étrangère concernée s'efforce de faire respecter des lois interdisant des pratiques essentiellement similaires aux pratiques interdites par les lois dont la FTC assure le respect ([1]). 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'ADP de l'Union européenne 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'ADP, 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 ([2]).

Outre la hiérarchisation des dossiers relatifs au bouclier de protection des données soumis par des États membres de l'Union européenne et par des organisations d'autoréglementation ([3]), la FTC s'engage à enquêter sur les éventuelles violations du cadre de sa propre initiative le cas échéant en utilisant un éventail d'outils.

Depuis plus d'une décennie, la FTC mène un solide programme d'enquêtes sur les aspects de la protection de la vie privée et de la sécurité impliquant des organisations commerciales. Dans le cadre de ces enquêtes, la FTC vérifie d'office si l'entité concernée a fait des déclarations relatives à la sphère de sécurité. Dans les cas où l'entité a fait des déclarations de ce type et où l'enquête révèle des violations manifestes des principes de la sphère de sécurité relatifs à la protection de la vie privée, la FTC inclut des allégations de violation des principes de la sphère de sécurité dans ses actions de mise en application. Nous poursuivrons notre stratégie proactive au titre du nouveau cadre. À noter que la FTC mène de nombreuses autres enquêtes aboutissant, en définitive, à des actions publiques d'application des lois. De nombreuses enquêtes de la FTC sont closes sans suite parce que ses agents ne décèlent aucune violation manifeste de la loi. Étant donné que les enquêtes de la FTC sont confidentielles (et non accessibles au public), la clôture d'une enquête n'est généralement pas rendue publique.

La FTC a lancé près de 40 actions de mise en application dans le cadre du programme de la sphère de sécurité, ce qui témoigne de l'engagement de l'agence à faire appliquer, de façon proactive, les programmes transfrontaliers de protection de la vie privée. La FTC inscrira les violations potentielles du cadre du bouclier de protection des données au programme des enquêtes qu'elle mène régulièrement en matière de protection de la vie privée et de sécurité.

III. LUTTE CONTRE LES DÉCLARATIONS MENSONGÈRES OU FRAUDULEUSES D'ADHÉSION AU BOUCLIER DE PROTECTION DES DONNÉES

Comme indiqué ci-dessus, la FTC prendra des mesures contre les entités qui font des déclarations mensongères concernant leur participation au cadre. La FTC examinera en priorité les dossiers soumis par le ministère du commerce concernant les organisations identifiées comme se présentant indûment comme adhérant actuellement au cadre, ou qui utilisent un label de certification du cadre sans autorisation.

Par ailleurs, nous faisons observer que, si une organisation promet, dans sa politique de protection de la vie privée, de respecter les principes du bouclier de protection des données, le fait qu'elle ne soit pas ou plus inscrite auprès du ministère du commerce ne la dispensera pas en principe de l'obligation, contrôlée par la FTC, de respecter ces engagements au titre du cadre.

([1]) 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.

([2]) Au cours des exercices fiscaux 2012 à 2015, par exemple, la FTC a fait usage de ses compétences au titre de la loi US SAFE WEB pour échanger des informations en réponse à près de 60 demandes émanant d'agences étrangères, et elle a émis près de 60 demandes d'enquêtes civiles (équivalentes à des citations à comparaître administratives) en vue de contribuer à 25 enquêtes étrangères.

([3]) 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 au bouclier de protection des données soumis par les ADP de l'Union européenne. Par ailleurs, la FTC utilise les plaintes enregistrées dans sa base de données «Consumer Sentinel», accessible à de nombreuses autres agences répressives, pour repérer les tendances, déterminer les priorités de mise en application et recenser les cibles d'enquêtes potentielles. Les citoyens de l'Union européenne 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 au bouclier de protection des données, cependant, il peut être préférable pour les citoyens de l'Union européenne de soumettre les plaintes à l'ADP de leur État membre ou à une instance de règlement extrajudiciaire des litiges.

IV. SUIVI DES ORDONNANCES

La FTC s'engage également à assurer le suivi des ordonnances d'exécution afin de garantir le respect du cadre du bouclier de protection des données.

Nous exigerons le respect du cadre par différentes injonctions appropriées dans les futures ordonnances relatives au cadre du bouclier de protection des données. Nous interdirons notamment les déclarations trompeuses relatives au cadre et à d'autres programmes de protection de la vie privée lorsque ces déclarations sont à l'origine de l'action sous-jacente de la FTC.

Les actions menées par la FTC pour faire appliquer le programme initial de la sphère de sécurité sont instructives. Dans les 36 dossiers portant sur des déclarations mensongères ou frauduleuses de certification du titre de la sphère de sécurité, chaque ordonnance interdit au défendeur de donner une image fausse de sa participation à la sphère de sécurité ou à tout autre programme de protection de la vie privée ou de sécurité et impose à l'entreprise de mettre des rapports de conformité à la disposition de la FTC. Dans certains dossiers portant sur des violations des principes de la sphère de sécurité relatifs à la protection de la vie privée, les entreprises concernées ont été tenues de mettre en œuvre des programmes complets de protection de la vie privée et de faire évaluer ces programmes par des tiers indépendants tous les deux ans pendant vingt ans. Elles doivent fournir les résultats de ces évaluations à la FTC.

Le non-respect d'ordonnances administratives de la FTC peut entraîner des sanctions civiles allant jusqu'à 16 000 USD par infraction ou 16 000 USD par jour en cas d'infraction persistante ([1]). 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 des documents attestant de leur conformité pendant un nombre d'années déterminé. Les ordonnances doivent également être communiquées aux employés chargés d'en assurer le respect.

La FTC contrôle systématiquement le respect des ordonnances relatives à la sphère de sécurité, comme elle le fait pour toutes ses autres ordonnances. La FTC prend au sérieux le respect de ses ordonnances en matière de protection de la vie privée et de sécurité des données, et lance des actions en vue de les faire respecter si nécessaire. Par exemple, comme indiqué ci-dessus, Google a payé une amende civile de 22,5 millions d'USD à la suite d'allégations selon lesquelles elle n'avait pas respecté l'ordonnance de la FTC la concernant. 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 continuera de tenir une liste en ligne d'entreprises faisant l'objet d'ordonnances liées à l'application du programme de la sphère de sécurité et du nouveau cadre du bouclier de protection des données ([2]). Par ailleurs, les principes du bouclier de protection des données imposent désormais aux entreprises faisant l'objet d'une ordonnance de la FTC, ou d'une ordonnance judiciaire pour non-conformité aux principes, de rendre publiques toutes les parties des rapports de conformité ou d'évaluation soumis à la FTC qui sont liées au bouclier de protection des données, dans la mesure autorisée par les lois et règles en matière de confidentialité.

V. ENGAGEMENT AUPRÈS DES ADP DE L'UNION EUROPÉENNE ET COOPÉRATION EN MATIÈRE D'APPLICATION

La FTC a conscience du rôle important joué par les ADP de l'Union européenne dans le respect des principes du cadre et encourage un renforcement des initiatives de consultation et une coopération accrue en matière d'application de la réglementation. Outre les consultations avec les ADP sur des questions propres à chaque dossier qu'elles soumettent, la FTC s'engage à participer à des réunions périodiques avec les représentants désignés du groupe de travail «article 29» afin de discuter de manière générale de la façon d'améliorer la coopération en matière d'application du cadre. La FTC participera également, aux côtés du ministère du commerce, de la Commission européenne et du groupe de travail «article 29», à l'examen annuel du cadre 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 ADP de l'Union européenne et avec les autres autorités d'application des règles de protection de la vie privée du monde entier. La FTC, avec ses partenaires en matière répressive dans l'Union européenne et dans le monde entier, a notamment lancé l'année dernière un système d'alerte au sein du réseau mondial d'application des lois pour la protection de la vie privée (*Global Privacy Enforcement Network*, GPEN) afin de partager des informations relatives aux enquêtes et de promouvoir la coordination en matière d'application des lois. L'outil d'alerte du GPEN pourrait s'avérer particulièrement utile dans le cadre du bouclier de protection des données. La FTC et les ADP de l'Union européenne pourraient l'utiliser afin de coordonner leurs actions concernant le cadre et les autres enquêtes en matière de protection de la vie privée, y compris comme point de départ pour le partage d'informations afin d'assurer une

([1]) 15 U.S.C. § 45(m); 16 CFR § 1.98.

([2]) Voir FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

protection coordonnée et plus efficace de la vie privée des consommateurs. Nous nous réjouissons de pouvoir poursuivre notre collaboration avec les autorités participantes de l'Union européenne en vue d'un déploiement plus large du système d'alerte du GPEN et de l'élaboration d'autres outils permettant d'améliorer la coopération dans l'application des lois dans les dossiers de protection de la vie privée, notamment ceux impliquant le cadre.

La FTC est heureuse de réaffirmer son engagement à faire appliquer le nouveau cadre du bouclier de protection des données. Nous nous réjouissons également de poursuivre notre engagement auprès de nos collègues de l'Union européenne dans notre travail commun visant à protéger la vie privée des consommateurs.

Veuillez agréer, Madame la Commissaire,
l'expression de ma considération distinguée.

Edith Ramirez

Présidente

Appendice A

Le cadre du bouclier de protection des données UE-États-Unis dans son contexte: panorama du système juridique américain en matière de protection de la vie privée et de sécurité

On retrouve les mesures de protection prévues par le cadre du bouclier de protection des données UE-États-Unis (ci-après, le «cadre») parmi les mesures plus générales de protection de la vie privée mises en place par le système juridique américain dans son ensemble. D'une part, la commission fédérale du commerce (*Federal Trade Commission*, FTC) s'est dotée d'un solide programme de protection de la vie privée et de sécurité des données couvrant les pratiques commerciales des États-Unis et protégeant les consommateurs dans le monde entier. D'autre part, le paysage américain de la protection de la vie privée et de la sécurité des consommateurs a considérablement évolué depuis 2000, date à laquelle le programme initial de la sphère de sécurité UE-États-Unis a été adopté. Depuis lors, de nombreuses lois sur la protection de la vie privée et la sécurité ont été promulguées tant au niveau fédéral que des États, et le nombre de procédures judiciaires, impliquant les pouvoirs publics comme des particuliers, visant l'application des droits en matière de vie privée a sensiblement augmenté. Les mesures de protection prévues par le système juridique américain en matière de protection de la vie privée et de la sécurité des consommateurs couvrant les pratiques commerciales des États-Unis complètent, par leur vaste champ d'application, les mesures de protection offertes aux particuliers de l'Union européenne par le nouveau cadre.

I. LE PROGRAMME GÉNÉRAL DE CONTRÔLE DU RESPECT DE LA VIE PRIVÉE ET DE LA SÉCURITÉ DE LA FTC

La FTC est la principale agence américaine de protection des consommateurs spécialisée dans le respect de la vie privée dans le secteur du commerce. La FTC a compétence pour poursuivre en justice les auteurs d'actes ou de pratiques déloyaux ou frauduleux portant atteinte à la vie privée des consommateurs; elle assure également l'application de législations plus ciblées qui protègent certaines informations en matière de finances et de santé, ainsi que des informations concernant les enfants et des informations utilisées pour prendre certaines décisions d'éligibilité concernant les consommateurs.

La FTC possède une expérience inégalée dans le contrôle du respect de la vie privée des consommateurs. Ses interventions ont permis de contrer des pratiques déloyales dans divers environnements tant en ligne que hors ligne. Ainsi, la FTC a adopté des mesures de coercition à l'encontre de sociétés ayant pignon sur rue — telles que Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC et Snapchat — mais également de sociétés moins connues. Elle a poursuivi en justice des entreprises qui sont réputées avoir envoyé des courriers électroniques non désirés (spam) aux consommateurs, installé des logiciels espions ou malveillants sur des ordinateurs, omis de sécuriser des informations à caractère personnel de consommateurs, suivi des consommateurs en ligne de manière frauduleuse, enfreint la vie privée d'enfants, collecté de manière illicite des informations relatives aux consommateurs sur des appareils mobiles et omis de sécuriser des appareils connectés à l'internet et utilisés pour stocker des informations à caractère personnel. Les ordonnances rendues à l'encontre de ces entreprises instauraient généralement un contrôle continu par la FTC sur une durée de 20 ans, interdisaient toute autre infraction et soumettaient les entreprises à de lourdes sanctions financières en cas de manquement à l'ordonnance ([1]). Il est important de noter que les ordonnances rendues par la FTC ne visent pas uniquement à protéger les personnes qui ont porté plainte; elles protègent également l'ensemble des consommateurs qui, par la suite, ont affaire avec les entreprises concernées. Dans le contexte international, la FTC a compétence pour protéger les consommateurs, où qu'ils se trouvent dans le monde, de pratiques à l'œuvre aux États-Unis ([2]).

À ce jour, la FTC a soumis à la justice plus de 130 cas d'envoi de courriers électroniques non désirés et d'installation de logiciels espions, plus de 120 cas d'infraction à des consignes «Do Not Call» (ne pas appeler) en matière de télémarketing, plus de 100 cas au titre de la loi sur l'impartialité des rapports de solvabilité (*FAIR Credit Reporting Act*), près de 60 cas concernant la sécurité des données, plus de 50 cas d'atteintes générales au respect de la vie privée, près de 30 cas de manquement à la loi Gramm-Leach-Bliley et plus de 20 cas de mise en application de la loi sur le respect de la vie privée des enfants en ligne (*Children's Online Privacy Protection Act*, COPPA) ([3]). En outre, la FTC a également rédigé et publié des lettres d'avertissement ([4]).

([1]) Le manquement aux ordonnances de la FTC peut entraîner des sanctions civiles allant jusqu'à 16 000 USD par infraction ou 16 000 USD par jour en cas d'infraction persistante. Voir 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) Le Congrès a expressément confirmé la compétence de la FTC pour présenter des recours en justice, y compris des demandes de restitution, contre les actes et pratiques déloyaux ou frauduleux concernant le commerce extérieur qui: 1) entraînent ou sont susceptibles d'entraîner des préjudices raisonnablement prévisibles aux États-Unis; ou 2) impliquent un comportement concret aux États-Unis. Voir 15 U.S.C. § 45(a)(4).

([3]) Dans certaines affaires concernant le respect de la vie privée et la sécurité des données, la FTC a allégué que l'entreprise en cause avait des pratiques aussi bien frauduleuses que déloyales; elle a également parfois invoqué des manquements à plusieurs actes législatifs tels que la loi sur l'impartialité des rapports de solvabilité, la loi Gramm-Leach-Bliley et la COPPA.

([4]) Voir, par exemple, le communiqué de presse publié par la FTC: «FTC Warns Children's App Maker BabyBus About Potential COPPA Violations» (22 décembre 2014), https://www.ftc.gov/news-events/press- releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; le communiqué de presse publié par la FTC: «FTC Warns Data Broker Operations of Possible Privacy Violations» (7 mai 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; le communiqué de presse publié par la FTC: «FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to FAIR Credit Reporting Act» (3 avril 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Dans le cadre de son expérience passée d'une application stricte des règles en matière de vie privée, la FTC a également recherché de façon régulière les infractions potentielles au programme de la sphère de sécurité. Depuis l'adoption dudit programme, la FTC a mené, de sa propre initiative, de nombreuses enquêtes de conformité aux règles de la sphère de sécurité et à soumis à la justice 39 cas de manquement imputables à des sociétés américaines. La FTC poursuivra sa stratégie proactive en faisant du contrôle de l'application du nouveau cadre une priorité.

II. MESURES DE PROTECTION DE LA VIE PRIVÉE DES CONSOMMATEURS AU NIVEAU FÉDÉRAL ET AU NIVEAU DES ÉTATS

L'étude relative à la mise en œuvre des principes de la «sphère de sécurité», qui figure en annexe de la décision de la Commission européenne relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité», offre une synthèse de l'essentiel des lois de protection de la vie privée en vigueur au niveau fédéral et au niveau des États au moment où le programme de la sphère de sécurité a été adopté en 2000 ([1]). À cette époque, de nombreux actes législatifs fédéraux régissaient la collecte et l'utilisation à des fins commerciales d'informations à caractère personnel, outre la section 5 de la loi portant établissement de la commission fédérale du commerce (*FTC Act*), et notamment les lois suivantes: *Cable Communications Policy Act*, *Driver's Privacy Protection Act*, *Electronic Communications Privacy Act*, *Electronic Funds Transfer Act*, *FAIR Credit Reporting Act*, *Gramm-Leach-Bliley Act*, *Right to Financial Privacy Act*, *Telephone Consumer Protection Act* et *Video Privacy Protection Act*. De nombreux États fédérés avaient des lois analogues dans ces domaines.

Depuis 2000, de nombreuses initiatives tant au niveau fédéral qu'au niveau des États ont donné lieu à l'adoption de mesures de protection supplémentaires concernant le respect de la vie privé des consommateurs ([2]). Au niveau fédéral, par exemple, la FTC a modifié le règlement COPPA en 2013 pour introduire des mesures supplémentaires de protection des données personnelles concernant les enfants. La FTC a également adopté deux règlements d'exécution de la loi Gramm-Leach-Bliley (le règlement sur le respect de la vie privée — *Privacy Rule* — et le règlement en matière de garanties — *Safeguards Rule*) qui imposent aux institutions financières ([3]) de divulguer leurs pratiques de partage de l'information et de mettre en œuvre un programme global de sécurité de l'information pour protéger les données des consommateurs ([4]). De la même manière, la loi relative à l'impartialité et à la fiabilité des opérations de crédit (*FAIR and Accurate Credit Transactions Act*, FACTA), promulguée en 2003, vient compléter des lois anciennes en matière de crédit en introduisant des exigences pour le masquage, le partage et la mise à l'écart de certaines données financières sensibles. La FTC a adopté un certain nombre de règlements au titre de la FACTA, notamment sur les questions suivantes: droit des consommateurs de disposer gratuitement d'un rapport annuel de solvabilité; exigences pour la mise à l'écart en toute sécurité des données contenues dans les rapports des consommateurs; droit des consommateurs de renoncer à recevoir certaines offres de crédit et d'assurance; droit des consommateurs de refuser l'utilisation de données fournies par une filiale pour commercialiser ses produits et ses services; et exigences imposées aux institutions financières et aux créanciers afin qu'ils mettent en œuvre des programmes de détection et de prévention de l'usurpation d'identité ([5]). En outre, les règlements adoptés au titre de la loi relative à la portabilité et à la responsabilisation en matière d'assurance-maladie (*Health Insurance Portability and Accountability Act*, HIPAA) ont été révisés en 2013, et des mesures de protection supplémentaires y ont été introduites pour assurer le respect de la vie privée et la sécurité des données médicales à caractère personnel ([6]). Des règlements protégeant les consommateurs d'appels de télémarketing intempestifs, d'appels par des automates et de courriers électroniques non désirés ont également pris effet. Par ailleurs, le Congrès a adopté des lois exigeant de certaines entreprises collectant des données médicales de signaler toute infraction aux consommateurs ([7]).

Les États ont également beaucoup légiféré dans le domaine du respect de la vie privée et de la sécurité. Depuis 2000, 47 États, ainsi que le District of Columbia, Guam, Porto Rico et les îles Vierges ont adopté des lois exigeant des

([1]) Voir le document du ministère américain du commerce: SAFE Harbor Enforcement Overview (Étude relative à la mise en œuvre des principes de la «sphère de sécurité»), https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Pour une synthèse plus complète des mesures de protection juridiques aux États-Unis, voir Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5e édition 2015).

([3]) Les institutions financières sont définies de manière très large dans la loi Gramm-Leach-Bliley comme étant toutes les entreprises qui «se consacrent dans une large mesure» à la fourniture de produits ou de services financiers. Cette définition inclut, par exemple, les entreprises d'encaissement de chèques, les sociétés de prêt sur salaire, les courtiers en hypothèques, les établissements de prêt non bancaires, les évaluateurs de biens personnels ou immobiliers et les préparateurs de déclarations de taxe professionnelle.

([4]) En vertu de la loi sur la protection des consommateurs dans le secteur financier (*Consumer Financial Protection Act*, CFPA) de 2010, Titre X de Pub. L. 111-203, 124 Stat. 1955 (21 juillet 2010) (également connue sous le nom de *Dodd-Frank Wall Street Reform and Consumer Protection Act*), la plupart des compétences décisionnelles de la FTC au titre de la loi Gramm-Leach-Bliley ont été transférées au bureau de protection des consommateurs dans le secteur financier (*Consumer Financial Protection Bureau*, CFPB). La FTC demeure l'autorité coercitive au titre de la loi Gramm-Leach- Bliley et l'autorité décisionnelle concernant le Safeguards Rule, et conserve un pouvoir décisionnel limité au titre du *Privacy Rule* en ce qui concerne les concessionnaires automobiles.

([5]) En vertu de la CFPA, la commission partage avec le CFPB sa mission de contrôle de l'application de la FCRA, mais l'essentiel de ses compétences décisionnelles sont transférées à ce dernier (à l'exception des règlements en matière d'usurpation d'identité — *Red Flags Rule* — et de mise à l'écart des informations — *Disposal Rule*).

([6]) *Voir* 45 C.F.R. pts. 160, 162, 164.

([7]) Voir, par exemple, American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) et les actes réglementaires pertinents, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R. pt. 318.

entreprises qu'elles signalent aux particuliers toute infraction concernant la sécurité des données à caractère personnel ([1]). Au moins 32 États et Porto Rico disposent de lois sur l'effacement des données, instaurant des exigences concernant la destruction ou la mise à l'écart des données à caractère personnel ([2]). Un certain nombre d'États ont adopté des législations générales sur la sécurité des données. En outre, la Californie a adopté diverses lois relatives au respect de la vie privée, et notamment une loi imposant aux entreprises de se doter de politiques en la matière et de divulguer leurs pratiques en matière de protection contre le pistage («Do Not Track») ([3]); une loi «Shine the Light» exigeant une plus grande transparence de la part des courtiers de données ([4]); et une loi imposant une fonction «effacer» permettant aux mineurs de demander la suppression de certaines informations sur les médias sociaux ([5]). Sur la base de ces lois et autres décisions administratives, le gouvernement fédéral et les gouvernements des États ont infligé de lourdes amendes à des entreprises qui avaient omis de protéger la vie privée et d'assurer la sécurité des données à caractère personnel des consommateurs ([6]).

Des poursuites engagées par des particuliers ont également abouti à des jugements et des transactions favorables prévoyant des mesures de protection supplémentaires en la matière pour les consommateurs. Par exemple, en 2015, la société Target a accepté de payer 10 millions d'USD dans le cadre de transactions avec des clients qui invoquaient une atteinte à leurs informations financières à caractère personnel en raison d'une violation à grande échelle concernant des données. En 2013, AOL a accepté de payer, dans le cadre d'une transaction, 5 millions d'USD pour mettre fin à une action collective («class action») dont les auteurs alléguaient une anonymisation insuffisante en lien avec la divulgation de requêtes de recherche de centaines de milliers de membres d'AOL. En outre, une cour fédérale a entériné un règlement de 9 millions d'USD imposé à Netflix pour avoir conservé des historiques de location en violation de la loi sur le respect de la vie privée dans le cadre de la fourniture de matériel vidéo (*Video Privacy Protection Act*) de 1988. En Californie, les cours fédérales ont entériné deux transactions distinctes avec Facebook — l'une d'un montant de 20 millions d'USD et l'autre de 9,5 millions d'USD — en lien avec la collecte, l'utilisation et le partage par cette entreprise des données à caractère personnel de ses utilisateurs. Enfin, en 2008, une juridiction de l'État de Californie a approuvé une transaction imposant à LensCrafters le versement de 20 millions d'USD pour divulgation illicite d'informations médicales concernant des consommateurs.

En fin de compte, comme le montre le présent résumé, les États-Unis assurent aux consommateurs une protection juridique non négligeable dans le domaine du respect de la vie privée et de la sécurité. Le nouveau cadre du bouclier de protection des données, qui offre aux particuliers de l'Union européenne des garanties significatives s'inscrira dans ce contexte plus large, où la protection de la vie privée et de la sécurité des consommateurs restera une priorité importante.

([1]) Voir, par exemple, le document de la conférence nationale des législatures d'État (*National Conference of State Legislatures*, NCSL): *State Security Breach Notification Laws* (4 janvier 2016), disponible à l'adresse http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 janvier 2016), disponible à l'adresse http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) Cal. Bus. & Professional Code §§ 22575-22579.

([4]) Cal. Civ. Code §§ 1798.80-1798.84.

([5]) Cal. Bus. & Professional Code § 22580-22582.

([6]) Voir Jay Cline, U.S. Takes the Gold in Doling Out Privacy Fines, Computerworld (17 février 2014), disponible à l'adresse http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privac-y-fines?taxonomyId=17&pageNumber=1.

ANNEXE V

Lettre de M. Anthony Foxx, secrétaire américain aux transports

19 février 2016

M[me] la Commissaire Věra Jourová
Commission européenne
Rue de la Loi, 200
1049 Bruxelles
BELGIQUE

Objet: Cadre du bouclier de protection des données UE–États-Unis

Madame la 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 du bouclier de protection des données UE–États-Unis. Ce cadre joue 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 européenne 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 dans une lettre transmise à la Commission européenne il y a plus de 15 ans. 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. Il continue à respecter cet engagement tel que consacré par cette lettre.

Le DOT réaffirme notamment son engagement dans les domaines clés suivants: 1) hiérarchisation des enquêtes sur les allégations de violations du bouclier de protection des données; 2) répression adéquate contre les entités effectuant des déclarations de certification fausses ou frauduleuses au titre du bouclier de protection des données; et 3) surveillance des violations du bouclier de protection des données et 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 du cadre du bouclier de protection des données.

I. 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. L'autorité du DOT est habilitée à prendre des mesures dans ce domaine 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» pour la vente de prestations de transport aérien qui porte ou risque de porter préjudice au consommateur. 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). Selon notre interprétation, la législation sur les pratiques déloyales ou frauduleuses interdit aux compagnies aériennes et aux agents de billetterie: 1) d'enfreindre les dispositions de leur politique sur le respect de la vie privée; ou 2) de collecter ou divulguer des informations privées d'une manière contraire à l'ordre public, immorale ou entraînant pour les consommateurs un préjudice important non compensé par des avantages. Nous interprétons également la section 41712 comme interdisant aux transporteurs aériens et aux agents de billetterie: 1) d'enfreindre les règles établies par le ministère déterminant les pratiques déloyales ou frauduleuses; ou 2) d'enfreindre la loi sur la protection de la vie privée des enfants en ligne (*Children's Online Privacy Protection Act*, COPPA) ou les règles de la FTC portant exécution de la COPPA. 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 de respect de la vie privée établis par le cadre du bouclier de protection des données, 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 cadre du bouclier de protection des données relatifs au respect de la vie privée, 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 l'application de la législation et les procédures en matière d'aéronautique (*Aviation Enforcement Office*) 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, des 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'Aviation Enforcement Office prend essentiellement connaissance des violations potentielles au travers des plaintes qu'il reçoit de particuliers, d'agents de voyage, de compagnies aériennes et d'agences gouvernementales américaines et étrangères. Les consommateurs peuvent utiliser le site web du DOT pour déposer des plaintes en matière de respect de la vie privée contre les compagnies aériennes et les agents de billetterie ([1]).

Lorsqu'une transaction raisonnable et appropriée ne peut être conclue, l'*Aviation Enforcement Office* 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 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 27 500 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'*Aviation Enforcement Office*, 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 par le passé et pourrait également arriver dans le contexte de l'application des principes du bouclier de protection des données lorsque les circonstances le permettent. 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 plaintes faisant état de violations de la vie privée par des agents de billetterie ou des compagnies aériennes. Lorsqu'il y a plainte, celle-ci est instruite conformément aux principes susmentionnés.

C. **Mesures de protection juridiques adoptées par le DOT bénéficiant aux consommateurs de l'Union européenne**

Au titre de la section 41712, l'interdiction des pratiques déloyales ou frauduleuses relatives au transport aérien ou à 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 à la fois les consommateurs étrangers et américains dans la mesure où ces pratiques sont intervenues dans le cadre de la fourniture de services de transport de 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.

Le DOT met également en œuvre, en ce qui concerne les compagnies aériennes, d'autres lois ciblées dont la protection s'étend aux consommateurs non américains, comme la 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 DU BOUCLIER DE PROTECTION DES DONNÉES

Lorsqu'une compagnie aérienne ou un agent de billetterie décide de participer au cadre du bouclier de protection des données et que le ministère reçoit une plainte alléguant une violation du cadre par cette compagnie ou cet agent, le ministère prend les mesures suivantes afin d'appliquer fermement le cadre.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Hiérarchisation des enquêtes sur allégation de violations**

L'*Aviation Enforcement Office* du ministère des transports enquête sur chaque allégation de violation du bouclier de protection des données (y compris les plaintes émanant des autorités européennes de protection des données). Il prend des mesures répressives lorsqu'une violation est avérée. L'Aviation Enforcement Office coopère en outre avec la FTC et le ministère du commerce et donne la priorité aux allégations de manquement, par les entités réglementées, des engagements pris en matière de respect de la vie privée dans le cadre du bouclier de protection des données.

Lorsqu'une allégation de violation du cadre du bouclier de protection des données lui parvient, l'Aviation Enforcement Office peut prendre une série de mesures dans le cadre de son enquête. Il peut, par exemple, examiner les politiques 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 tierces parties, 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, le cas échéant, entame une procédure d'exécution.

Si des violations potentielles du bouclier de protection des données 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 d'application du bouclier de protection des données.

B. **Traitement des déclarations d'adhésion fausses ou frauduleuses**

Le ministère maintient son engagement à enquêter sur les violations du bouclier de protection des données, y compris les déclarations fausses ou frauduleuses d'adhésion au programme du bouclier de protection des données. Nous examinerons en priorité les dossiers soumis par le ministère du commerce concernant les organisations qui, selon lui, affirment indûment adhérer au bouclier de protection des données ou utilisent sans autorisation le label de certification du cadre du bouclier de protection des données.

Signalons également que, lorsqu'une organisation affirme, dans sa politique sur le respect de la vie privée, être en conformité avec les principes matériels du bouclier de protection des données, le fait qu'elle ne soit pas ou plus enregistrée 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 d'exécution publiques relatives des violations du bouclier de protection des données**

L'*Aviation Enforcement Office* du ministère des transports maintient également son engagement à contrôler les ordonnances d'exécution selon les besoins, afin d'assurer le respect du programme du bouclier de protection des données. Plus précisément, lorsqu'il délivre une ordonnance exigeant qu'une compagnie aérienne ou un agent de billetterie mette fin ou renonce à des violations du bouclier de protection des données et de la section 41712, elle contrôle le respect, par l'entité, de la clause de cessation et d'abstention incluse dans l'ordonnance. L'Office veille en outre à ce que les ordonnances découlant d'affaires relatives au bouclier de protection des données soient publiées sur son site web.

Nous nous nous réjouissons à l'idée de poursuivre notre collaboration avec nos partenaires fédéraux et les acteurs de l'Union européenne sur les questions ayant trait au bouclier de protection des données.

J'espère que ces informations vous seront utiles et me tiens à votre disposition pour tout renseignement complémentaire.

Veuillez agréer, Madame la Commissaire,
l'expression de ma considération distinguée.

Anthony R. Foxx

Secrétaire aux transports

ANNEXE VI

Lettre de M. Robert Litt, conseiller général
Bureau du directeur du renseignement national

Le 22 février 2016

M. Justin S. Antonipillai
Conseiller
Ministère américain du commerce
1401 Constitution Ave., NW
Washington, DC 20230

M. Ted Dean
Sous-secrétaire adjoint
Administration du commerce international
1401 Constitution Ave., NW
Washington, DC 20230

Monsieur Antonipillai, Monsieur Dean,

Au cours des deux ans et demi écoulés, dans le cadre des négociations pour le bouclier de protection des données UE–États-Unis, les États-Unis ont fourni une quantité importante d'informations sur la collecte de renseignements d'origine électromagnétique par les services de renseignement américains Il s'agit notamment d'informations sur le cadre juridique en vigueur, la supervision à plusieurs niveaux de ces activités, la grande transparence qui entoure ces activités et les mesures de protection générales offertes en matière de respect de la vie privée et de respect des libertés civiles, afin d'aider la Commission européenne à se faire une idée de l'adéquation de ces protections dans le cadre de l'exception aux principes du bouclier de protection des données relative à la sécurité nationale. Le présent document résume les informations qui ont été fournies.

I. LA PPD-28 ET LES ACTIVITÉS AMÉRICAINES DE RENSEIGNEMENT D'ORIGINE ÉLECTROMAGNÉTIQUE

Les services de renseignement des États-Unis collectent des renseignements étrangers d'une manière minutieusement contrôlée, dans le strict respect de la législation américaine et sur la base de plusieurs niveaux de supervision, en se centrant sur certaines priorités importantes en matière de renseignement étranger et de sécurité nationale. Une mosaïque de lois et de politiques régissent la collecte de renseignements d'origine électromagnétique par les États-Unis, et notamment la constitution américaine, la loi sur la surveillance du renseignement étranger (50 U.S.C. § 1801 et suivants) (*Foreign Intelligence Surveillance Act*, FISA), le décret exécutif 12333 et ses procédures d'exécution, l'orientation présidentielle et de nombreuses procédures et lignes directrices, approuvées par la Cour FISA et le procureur général, qui établissent des règles supplémentaires limitant la collecte, la conservation, l'utilisation et la diffusion de renseignements étrangers ([1]).

a) **Aperçu de la PPD 28**

En janvier 2014, le président Obama a prononcé un discours décrivant plusieurs réformes concernant les activités de renseignement d'origine électromagnétique, qu'il a ensuite inscrites dans la directive présidentielle n° 28 (PPD-28) ([2]). Le président a insisté sur le fait que les activités de renseignement d'origine électromagnétique contribuent à protéger non seulement notre pays et nos libertés, mais aussi la sécurité et les libertés des autres pays, dont les États membres de l'Union européenne, qui se basent sur les informations obtenues par les agences de renseignement américaines pour protéger leurs propres citoyens.

La PPD-28 définit une série de principes et d'exigences applicables à l'ensemble des activités de renseignement d'origine électromagnétique américaines et à tous les individus, quelle que soit leur nationalité ou leur localisation. Elle établit notamment des exigences relatives aux procédures de traitement, de conservation et de diffusion d'informations à caractère personnel sur des ressortissants non américains suivies dans le cadre du renseignement d'origine électromagnétique américain. Ces exigences sont décrites ci-après, de façon résumée.

— La PPD rappelle que les États-Unis ne collectent des renseignements d'origine électromagnétique que dans la mesure autorisée par la législation, les décrets exécutifs et d'autres directives présidentielles.

([1]) D'autres informations sur les activités de renseignement étranger américaines sont publiées en ligne et accessibles au public par le site IC on the Record (www.icontherecord.tumblr.com), site web public de l'ODNI destiné à accroître la visibilité des activités de renseignement du gouvernement pour le grand public.

([2]) Disponible à l'adresse https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— La PPD définit des procédures visant à garantir que les activités de collecte de renseignements d'origine électromagnétique ne sont réalisées qu'à des fins de sécurité nationale légitimes et autorisées.

— La PPD dispose également que le respect de la vie privée et les libertés civiles doivent être pleinement pris en considération dans la planification des activités de collecte de renseignements d'origine électromagnétique. En particulier, les États-Unis ne collectent pas de renseignements dans le but d'éliminer ou d'entraver les critiques ou désaccords, de défavoriser des personnes au motif de leur appartenance ethnique, de leur race, de leur genre, de leur orientation sexuelle ou de leur religion, ou de conférer un avantage concurrentiel commercial aux entreprises et secteurs commerciaux américains.

— Selon la PPD, la collecte de renseignements d'origine électromagnétique doit être aussi spécifique que possible et les renseignements d'origine électromagnétiques collectés en vrac ne peuvent être utilisés qu'aux fins spécifiques énoncées.

— La PPD dispose que les services de renseignement doivent adopter des procédures «raisonnablement conçues afin de limiter la diffusion et la conservation d'informations à caractère personnel provenant d'activités de renseignement d'origine électromagnétique», en étendant notamment certaines protections accordées aux informations à caractère personnel des ressortissants américains aux informations concernant des ressortissants non américains.

— Des procédures pour la mise en œuvre de la PPD-28 par les agences ont été adoptées et rendues publiques.

L'applicabilité des procédures et des mesures de protection ici mentionnées au bouclier de protection des données est claire. Lorsque des données sont transférées à des sociétés américaines dans le cadre du bouclier de protection des données, ou par tout autre moyen, les agences de renseignement américaines peuvent demander des données à ces sociétés uniquement si leur demande est conforme à la FISA ou si elle est introduite en vertu de l'une des dispositions statutaires de la lettre de sécurité nationale, abordées ci-dessous ([1]). En outre, sans confirmer ni infirmer les dires des médias selon lesquels les services de renseignement américains collecteraient des données originaires de câbles transatlantiques pendant leur transmission vers les États-Unis, précisons que, si les services de renseignement américains collectaient des données provenant de câbles transatlantiques, ils le feraient dans le respect des limitations et garanties ici mentionnées, y compris des exigences de la PPD-28.

b) **Limitations en matière de collecte**

La PPD-28 énonce une série de principes généraux importants qui régissent la collecte de renseignements d'origine électromagnétique:

— la collecte de renseignements d'origine électromagnétique doit être autorisée par la législation ou par le président des États-Unis et doit être réalisée dans le respect de la constitution et de la loi,

— le respect de la vie privée et des libertés civiles doit être pleinement pris en considération au moment de la planification des activités de renseignement d'origine électromagnétique,

— des renseignements d'origine électromagnétique ne sont collectés qu'à des fins valables de renseignement étranger ou de contre-espionnage,

— les États-Unis ne collectent pas de renseignements d'origine électromagnétique dans le but d'éliminer ou d'entraver les critiques ou désaccords,

— les États-Unis ne collectent pas de renseignements d'origine électromagnétique dans le but de défavoriser des individus sur la base de leur appartenance ethnique, de leur race, de leur genre, de leur orientation sexuelle ou de leur religion,

— les États-Unis ne collectent pas de renseignements d'origine électromagnétique dans le but de conférer un avantage concurrentiel commercial aux entreprises et secteurs commerciaux américains,

— les activités de renseignement d'origine électromagnétique des États-Unis doivent toujours être aussi spécifiques que possible, en tenant compte de la disponibilité d'autres sources d'information, ce qui signifie notamment que les activités de collecte de renseignements d'origine électromagnétique doivent être effectuées dans la mesure du possible de manière ciblée et non en vrac.

L'exigence selon laquelle les activités de renseignement d'origine électromagnétique soient «aussi spécifiques que possible» s'applique à la manière dont les renseignements d'origine électromagnétique sont collectés ainsi qu'à la nature des renseignements collectés. Par exemple, pour déterminer s'il y a lieu de collecter des renseignements d'origine électromagnétique, les services de renseignement doivent tenir compte de la disponibilité d'autres informations, y compris

([1]) Les agences répressives ou réglementaires peuvent demander des informations auprès des sociétés à des fins d'enquête aux États-Unis en vertu d'autres pouvoirs en matière pénale, civile et réglementaire non abordés dans le présent document, qui se limite aux pouvoirs en rapport avec la sécurité nationale.

provenant de sources diplomatiques ou publiques, et privilégier la collecte par ces moyens, dans la mesure de ce qui est approprié et faisable. Par ailleurs, les politiques applicables aux composantes des services de renseignement doivent exiger que la collecte soit orientée, dans la mesure du possible, sur des cibles ou des sujets spécifiques du renseignement étranger moyennant l'utilisation de discriminants (p.exemple des canaux, critères de sélection et identifiants spécifiques).

Il est important d'envisager les informations fournies à la Commission dans leur globalité. Les décisions relatives à ce qui est «faisable» ou «possible» ne sont pas laissées à la discrétion des individus, mais sont régies par les politiques convenues par les agences au titre de la PPD-28 — publiquement disponibles — et aux autres processus qui y sont décrits ([1]). Selon la PPD-28, on entend par collecte en vrac de renseignements d'origine électromagnétique une collecte qui «pour des raisons techniques ou opérationnelles, est effectuée sans utiliser de discriminants (par exemple des identifiants ou des critères de sélection spécifiques)». La PPD-28 reconnaît à cet égard que les composantes des services de renseignement doivent, dans certaines circonstances, collecter en vrac des renseignements d'origine électromagnétique afin de détecter les menaces nouvelles ou émergentes ainsi que d'autres informations cruciales de sécurité nationale souvent dissimulées dans le vaste et complexe système des communications mondiales modernes. Elle reconnaît également que la collecte en vrac de renseignements d'origine électromagnétique puisse susciter des préoccupations relatives au respect de la vie privée et des libertés publiques. La PPD-28 exige par conséquent des services de renseignement qu'ils privilégient les solutions permettant l'obtention de renseignements d'origine électromagnétique ciblés plutôt que la collecte en vrac de tels renseignements. Les composantes des services de renseignement doivent dès lors préférer autant que possible les activités de collecte ciblée aux activités de collecte en vrac, en ce qui concerne les renseignements d'origine électromagnétique ([2]). Grâce à ces principes, l'exception relative à la collecte en vrac ne prendra pas le pas sur la règle générale.

En ce qui concerne la notion de «caractère raisonnable», il s'agit de l'un des principes fondamentaux du droit américain. Cela signifie que les composantes des services de renseignement ne sont pas tenues d'adopter toutes les mesures théoriquement envisageables, mais doivent trouver un équilibre entre leurs efforts visant à protéger les intérêts légitimes relatifs au respect de la vie privée et des libertés civiles et les nécessités pratiques des activités de renseignement d'origine électromagnétique. Ici encore, les politiques des agences ont été rendues publiques et peuvent garantir que le terme «raisonnablement conçues afin de limiter la diffusion et la conservation d'informations à caractère personnel» ne nuit pas à la règle générale.

La PPD-28 dispose également que les renseignements d'origine électromagnétique collectés en vrac ne peuvent être utilisés qu'à six fins spécifiques: la détection et la neutralisation de certaines activités de puissances étrangères; le contre-terrorisme; la contre-prolifération; la cybersécurité; la détection et la neutralisation des menaces vis-à-vis des forces armées américaines ou alliées; et la lutte contre les menaces criminelles transnationales, y compris contre le non-respect des sanctions. Le conseiller du président des États-Unis pour la sécurité nationale (*National Security Advisor*) procède chaque année, en consultation avec le directeur du renseignement national (*Director for National Intelligence*, DNI), à un réexamen des utilisations autorisées des renseignements d'origine électromagnétique collectés en vrac afin de déterminer s'il convient de les modifier. Le DNI rend publique cette liste, dans toute la mesure du possible, compte tenu des impératifs de la sécurité nationale. Cela constitue une limitation importante et transparente de l'utilisation de la collecte en vrac de renseignements d'origine électromagnétique.

En outre, les composantes des services de renseignement chargées de la mise en œuvre de la PPD-28 ont renforcé les pratiques et normes d'analyse existantes pour les requêtes portant sur des renseignements d'origine électromagnétique non évalués ([3]). Les analystes doivent structurer leurs demandes ou autres critères et techniques de recherche afin de s'assurer qu'ils conviennent à l'identification de renseignements pertinents pour une mission valide de renseignement étranger ou d'application de la loi. À cette fin, les composantes des services de renseignement doivent axer leurs requêtes relatives à des personnes sur les catégories de renseignements d'origine électromagnétique qui relèvent d'un impératif de renseignement étranger ou d'application de la loi, de manière à éviter l'utilisation d'informations à caractère personnel sans pertinence pour le renseignement étranger ou l'application de la loi.

Il importe de souligner que les activités de collecte en vrac de communications internet menées par les services de renseignement américains au travers du renseignement d'origine électromagnétique ne portent que sur une partie réduite de l'internet. Par ailleurs, l'utilisation de requêtes ciblées, comme décrit ci-dessus, garantit que seuls les éléments considérés comme présentant un intérêt potentiel pour le renseignement sont soumis aux analystes. Ces limitations ont pour but de protéger la vie privée et les libertés civiles de tous les citoyens, quelle que soit leur nationalité et quel que soit l'endroit où ils résident.

([1]) Disponible à l'adresse www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Ces procédures portent application des concepts de ciblage et de spécificité dont il est question dans cette lettre d'une manière qui est propre à chaque composante des services de renseignement.

([2]) Pour ne citer qu'un exemple, les procédures de la NSA mettant en œuvre la PPD-28 disposent que «[a]utant que possible, la collecte est effectuée à l'aide d'un ou plusieurs critères de sélection afin de l'orienter vers des cibles spécifiques de renseignement étranger (par exemple un terroriste ou groupe terroriste international connu spécifique) ou des sujets spécifiques de renseignement étranger (par exemple la prolifération d'armes de destruction massive par une puissance étrangère ou ses agents)».

([3]) Disponible à l'adresse http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Les États-Unis disposent de procédures élaborées garantissant que les activités de renseignement d'origine électromagnétique sont uniquement réalisées à des fins adéquates de sécurité nationale. Chaque année, le président des États-Unis définit les grandes priorités de la nation en matière de collecte de renseignements étrangers à l'issue d'un vaste processus formel interagences. Le DNI est chargé de traduire ces priorités en un «cadre des priorités du renseignement national» (*National Intelligence Priorities Framework*, NIPF). La PPD-28 a renforcé et amélioré ce processus interagences afin que toutes les priorités des services de renseignement soient examinées et approuvées par les hauts responsables. La directive relative aux services de renseignement (*Intelligence Community directive*, ou ICD) n° 204 contient d'autres orientations sur le NIPF. Elle a été mise à jour en janvier 2015 afin de tenir compte des exigences de la PPD-28 ([1]). Bien que les données du NIPF soient classifiées, les informations relatives aux priorités spécifiques de renseignement étranger sont reprises chaque année dans le document déclassifié du DNI sur l'évaluation mondiale des menaces (*Wordwide Threat Assessment*), également disponible sur le site web de l'ODNI.

Les priorités du NIPF sont formulées à un niveau de généralité relativement élevé. Elles abordent notamment des thèmes tels que la constitution de capacités nucléaires et de capacités en matière de missiles balistiques par certains adversaires étrangers, les conséquences de la corruption pratiquée par les cartels de la drogue et les violations des droits de l'homme dans certains pays. En outre, elles ne s'appliquent pas uniquement au renseignement d'origine électromagnétique, mais à toutes les activités de renseignement. L'organisation responsable de la concrétisation des priorités du NIPF sous la forme d'activités réelles de collecte de renseignements d'origine électromagnétique s'appelle le comité national du renseignement d'origine électromagnétique (*National Signals Intelligence Committee*, SIGCOM). Ce comité est placé sous l'égide du directeur de l'Agence de sécurité nationale (*National Security Agency*, NSA), désigné par le décret exécutif n° 12333 comme étant le «directeur fonctionnel du renseignement d'origine électromagnétique», responsable de la supervision et de la coordination du renseignement d'origine électromagnétique dans l'ensemble des services de renseignement sous la surveillance du ministre de la défense et du DNI. Le SIGCOM est constitué de représentants de toutes les composantes des services de renseignement et, dès que les États-Unis auront pleinement mis en œuvre la PPD-28, inclura également une représentation à part entière des autres ministères et agences ayant un intérêt stratégique dans le renseignement d'origine électromagnétique.

Tous les ministères et agences des États-Unis consommateurs de renseignements étrangers soumettent leurs demandes de collecte au SIGCOM. Le SIGCOM examine ces demandes, veille à ce qu'elles soient conformes au NIPF et leur assigne une priorité selon des critères tels que:

— Le renseignement d'origine électromagnétique peut-il fournir des informations utiles dans le cas envisagé, ou existe-t-il des sources d'information plus efficaces ou plus rentables pour satisfaire la demande de renseignements concernée, comme l'imagerie ou les informations provenant de sources ouvertes?

— Quel est le degré de nécessité de ces informations? Si elles constituent une priorité élevée dans le NIPF, il s'agira généralement d'une haute priorité de renseignement d'origine électromagnétique.

— Quel type de renseignement d'origine électromagnétique pourrait être utilisé?

— La collecte est-elle aussi spécifique que possible? Des limitations temporelles, géographiques ou autres sont-elles nécessaires?

Le processus d'évaluation des besoins de renseignements d'origine électromagnétique mis en œuvre par les États-Unis implique également de tenir explicitement compte d'autres facteurs tels que:

— La cible ou la méthode de la collecte sont-elles particulièrement sensibles? Si oui, la collecte devra faire l'objet d'un examen supplémentaire par des hauts responsables.

— La collecte présente-t-elle un risque injustifié pour la vie privée et les libertés civiles, quelle que soit la nationalité des personnes concernées?

— D'autres garanties en matière de diffusion et de conservation sont-elles nécessaires pour protéger la vie privée ou les intérêts de sécurité nationale?

Enfin, à la fin du processus, des membres dûment formés du personnel de la NSA reprennent les priorités validées par le SIGCOM et isolent et étudient certains critères de sélection, tels que des numéros de téléphone ou des adresses de courrier électronique, qui doivent permettre de collecter des renseignements étrangers correspondant à ces priorités. Tous les sélecteurs doivent être examinés et approuvés avant d'être inclus dans les systèmes de collecte de la NSA.

([1]) Disponible à l'adresse http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

Toutefois, même lorsque ces conditions sont remplies, l'autorisation et le moment de la collecte à proprement parler dépendront en partie d'autres aspects tels que la disponibilité de ressources de collecte appropriées. Ce processus permet de garantir que les activités américaines de collecte de renseignements d'origine électromagnétique répondent à des besoins de renseignement étrangers valables et importants. En outre, lorsqu'une collecte est effectuée conformément à la FISA, la NSA et les autres agences doivent naturellement respecter les restrictions supplémentaires approuvées par la Cour FISA. En résumé, ni la NSA ni les autres agences de renseignement américaines ne décident seules de ce qu'elles collectent.

De manière générale, ce processus permet de garantir que toutes les priorités de renseignement américain sont établies par les hauts responsables les mieux placés pour déterminer quels sont les besoins des États-Unis en matière de renseignement étranger et que tous ces responsables tiennent compte non seulement de la valeur potentielle de la collecte de renseignements, mais aussi des risques associés à cette collecte, y compris sur le plan du respect de la vie privée, des intérêts économiques nationaux et des relations étrangères.

En ce qui concerne les données transmises aux États-Unis conformément au bouclier de protection des données, bien que les États-Unis ne puissent confirmer ou infirmer certaines méthodes ou activités de renseignement, les exigences établies par la PPD-28 s'appliquent à toutes les activités de collecte de renseignements d'origine électromagnétique effectuées par les États-Unis, quel que soit le type ou la source des données collectées. En outre, les limitations et garanties applicables à la collecte de renseignements d'origine électromagnétique s'appliquent à toutes les finalités autorisées, y compris celles ayant trait aux relations étrangères et à la sécurité nationale.

Les procédures dont il est question ci-dessus illustrent l'engagement clairement pris par les États-Unis d'éviter la collecte arbitraire et indifférenciée de renseignements d'origine électromagnétique et d'appliquer — jusqu'aux plus hauts niveaux de notre gouvernement — le principe du caractère raisonnable. La PPD-28 et ses procédures d'exécution établies par les agences précisent les limitations, nouvelles ou non, et décrivent plus en détail les finalités pour lesquelles les États-Unis collectent et utilisent des renseignements d'origine électromagnétique. Elles garantiront que les activités de renseignement d'origine électromagnétique sont et continueront d'être effectuées dans l'unique but d'atteindre des objectifs de renseignement étranger légitimes.

c) **Limitations en matière de conservation et de diffusion**

La section 4 de la PPD-28 dispose que chaque composante des services de renseignement doit respecter des limites explicites en matière de conservation et de diffusion des informations à caractère personnel relatives à des ressortissants non américains collectées par le renseignement d'origine électromagnétique, lesquelles limites doivent être comparables aux limites applicables aux ressortissants américains. Ces règles sont intégrées dans des procédures destinées à chaque composante des services de renseignement; publiées en février 2015, ces procédures sont à la disposition du public. Pour pouvoir être conservées ou diffusées en tant que renseignements étrangers, les informations à caractère personnel doivent être en rapport avec un besoin de renseignement autorisé, conformément au processus NIPF décrit ci-dessus; il doit exister des raisons valables de penser que ces informations apportent la preuve d'une infraction; ou elles doivent répondre à l'un des autres critères de conservation d'informations sur des ressortissants américains énoncés dans le décret exécutif 12333, section 2.3.

Les informations pour lesquelles aucun de ces critères n'est rempli ne peuvent être conservées plus de cinq ans, à moins que le DNI ne décide expressément que leur conservation prolongée répond aux intérêts de sécurité nationale des États-Unis. Les composantes des services de renseignement sont donc tenues de supprimer les informations relatives à des ressortissants non américains qu'elles ont collectées par le renseignement d'origine électromagnétique dans les cinq ans suivant leur collecte, à moins qu'il ne soit établi qu'elles répondent à un besoin de renseignement étranger autorisé ou que le DNI ne considère, après prise en compte du point de vue de l'agent de l'ODNI pour la protection des libertés civiles et des responsables de la protection de la vie privée et des libertés civiles des agences, qu'une conservation prolongée répond aux intérêts de la sécurité nationale.

Par ailleurs, toutes les politiques de mise en œuvre de la PPD-28 adoptées par les agences disposent désormais explicitement que les informations relatives à une personne ne peuvent être diffusées au seul motif qu'il s'agit d'un ressortissant non américain et l'ODNI a adressé une directive à toutes les composantes des services de renseignement ([1]) afin qu'elles tiennent compte de cette exigence. Le personnel des services de renseignement a l'obligation expresse de tenir compte du respect de la vie privée des ressortissants non américains lorsqu'il élabore et diffuse des rapports de renseignement. En particulier, le renseignement d'origine électromagnétique sur les activités habituelles d'un étranger ne peut être considéré comme du renseignement étranger pouvant être diffusés ou conservés indéfiniment sur la base de ce seul fait, à moins qu'ils ne répondent à une nécessité de renseignement étranger autorisée. Cette disposition constitue une limitation importante qui fait suite aux préoccupations de la Commission européenne relatives à la portée de la définition de «renseignement étranger» incluse dans le décret exécutif 12333.

([1]) Directive relative aux services de renseignement (ICD) 203, disponible à l'adresse http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d) **Respect des exigences et surveillance**

Le système américain de surveillance du renseignement étranger assure un contrôle rigoureux et à plusieurs niveaux, afin de garantir le respect des lois et procédures applicables, y compris celles relatives à la collecte, à la conservation et à la diffusion des informations sur les ressortissants non américains obtenues par le renseignement d'origine électromagnétique conformément à la PPD-28. Ce système de surveillance se présente comme suit:

— Les services de renseignement emploient des centaines d'agents de surveillance. La NSA compte à elle seule 300 personnes exclusivement chargées du contrôle du respect des lois et procédures et d'autres composantes possèdent également des bureaux de surveillance. En outre, le ministère de la justice assure une surveillance approfondie des activités de renseignement. Le ministère de la défense effectue lui aussi des activités de surveillance.

— Chaque composante des services de renseignement possède son propre bureau de l'inspecteur général chargé, entre autres, de surveiller les activités de renseignement à l'étranger. Les inspecteurs généraux bénéficient d'une indépendance statutaire. Ils disposent d'un large pouvoir d'appréciation pour réaliser des enquêtes, des audits et des examens des programmes, y compris en ce qui concerne les fraudes, abus ou violations de la loi. Ils peuvent également recommander des mesures correctives. Si les recommandations de l'inspecteur général ne sont pas contraignantes, ses rapports sont souvent rendus publics et toujours transmis au Congrès; il s'agit notamment de rapports de suivi lorsque des mesures correctives recommandées dans de précédents rapports n'ont pas encore été adoptées. Le Congrès est ainsi informé de tout manquement aux dispositions et peut décider d'exercer des pressions, notamment sur le plan budgétaire, pour obtenir l'adoption de mesures correctives. Différents rapports des inspecteurs généraux concernant les programmes de renseignement ont été publiés ([1]).

— Le Bureau de la protection des libertés civiles et de la vie privée (*Civil Liberties and Privacy Office*, CLPO) de l'ODNI a pour mission de veiller à ce que les services de renseignement fonctionnent de manière à assurer la sécurité nationale tout en protégeant les libertés civiles et les droits liés à la vie privée ([2]). D'autres composantes des services de renseignement possèdent leur propre agent de la protection de la vie privée.

— Le Conseil de surveillance du droit au respect de la vie privée et des libertés civiles (*Privacy and Civil Liberties Oversight Board*, PCLOB), un organe indépendant établi par voie législative, est chargé d'analyser et de contrôler les programmes et politiques de contre-terrorisme, y compris le recours au renseignement d'origine électromagnétique, afin de garantir qu'ils protègent de manière adéquate la vie privée et les libertés civiles. Il a publié plusieurs rapports sur les activités de renseignement.

— Comme nous le verrons plus en détail ci-dessous, la Cour FISA, juridiction composée de juges fédéraux indépendants, est responsable de la surveillance et de la conformité de toutes les activités de collecte de renseignements d'origine électromagnétique effectuées conformément à la FISA.

— Enfin, le Congrès américain, plus précisément les commissions du renseignement et des affaires judiciaires de la Chambre des représentants et du Sénat ont d'importantes responsabilités de surveillance à l'égard de toutes les activités du renseignement extérieur américain, y compris le renseignement d'origine électromagnétique.

En plus de ces mécanismes de surveillance formels, les services de renseignement ont également mis en place plusieurs mécanismes visant à garantir le respect, en leur sein, des limitations en matière de collecte décrites ci-dessus. Par exemple:

— Les hauts responsables ministériels sont tenus de valider chaque année leurs exigences en matière de renseignement d'origine électromagnétique.

— La NSA contrôle les cibles du renseignement d'origine électromagnétique d'un bout à l'autre afin de déterminer si les renseignements étrangers collectés correspondent aux priorités établies et met fin à la collecte dans le cas contraire. D'autres procédures assurent le contrôle périodique des critères de sélection.

([1]) Voir par exemple le rapport de l'inspecteur général du ministère américain de la justice, «A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008» (septembre 2012), disponible à l'adresse https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Voir www.dni.gov/clpo.

— Sur la base d'une recommandation d'un groupe d'étude indépendant nommé par le président Obama, le DNI a créé un nouveau mécanisme afin de contrôler la collecte et la diffusion de renseignements d'origine électromagnétique particulièrement sensibles en raison de la nature de la cible ou du moyen de collecte utilisé, afin de veiller à ce que les renseignements collectés correspondent aux objectifs des responsables politiques.

— Enfin, l'ODNI effectue une révision annuelle de l'allocation des ressources aux services de renseignement sur la base des priorités du NIPF et de la mission de renseignement dans son ensemble. Cette révision inclut l'évaluation de la valeur de tous les types de collecte de renseignements, y compris le renseignement d'origine électromagnétique, et adopte une vision à la fois rétrospective — dans quelle mesure les services de renseignement sont-il parvenus à leurs objectifs? — et prospective — de quoi auront besoin les services de renseignement à l'avenir? Ainsi, les ressources du renseignement d'origine électromagnétique sont appliquées aux priorités nationales les plus importantes.

Comme l'illustre ce panorama global, les services de renseignement ne décident pas seuls des conversations qu'ils vont écouter, ne tentent pas de tout collecter et ne sont pas exempts de tout contrôle. Leurs activités sont axées sur les priorités définies par les responsables politiques, au travers d'un processus auquel contribue le gouvernement tout entier, et sous une surveillance effectuée à la fois par la NSA, l'ODNI, le ministère de la justice et le ministère de la défense.

La PPD-28 contient également de nombreuses dispositions visant à ce que les informations à caractère personnel collectées par voie électromagnétique soient protégées, indépendamment de la nationalité de la personne concernée. Par exemple, la PPD-28 prévoit des procédures de contrôle de la sécurité, de l'accès et de la qualité des données, afin de protéger les informations à caractère personnel collectées par voie électromagnétique, ainsi qu'une formation obligatoire afin de s'assurer que le personnel comprenne sa responsabilité dans la protection de ces informations, indépendamment de la nationalité de la personne concernée. La PPD prévoit également des mécanismes supplémentaires de surveillance et de conformité, dont des audits et contrôles périodiques, par les responsables compétents en la matière, des pratiques mises en œuvre pour protéger les informations à caractère personnel contenues dans les renseignements d'origine électromagnétique. Les contrôles doivent également évaluer la conformité des agences avec les procédures de protection de ces informations.

La PPD-28 prévoit en outre que les problèmes importants de conformité relatifs à des ressortissants non américains doivent être pris en charge par les plus hautes instances gouvernementales. Les problèmes de conformité majeurs concernant les informations à caractère personnel d'un individu collectées dans le cadre d'activités de renseignement d'origine électromagnétique doivent être signalés rapidement au DNI, en plus des éventuelles autres exigences de notification. Si le problème porte sur les informations à caractère personnel d'un ressortissant non américain, le DNI décide, en consultation avec le secrétaire d'État et le directeur de la composante des services de renseignement concernée, des mesures à prendre pour notifier le gouvernement étranger concerné, en respectant la protection des sources et des méthodes et du personnel américain. Par ailleurs, conformément à la PPD-28, le Secrétaire d'État a nommé une haute fonctionnaire, la sous-secrétaire Catherine A. Novelli, afin de servir de point de contact aux gouvernements étrangers souhaitant manifester leur préoccupation au sujet d'activités de renseignement d'origine électromagnétique de la part des États-Unis. Cet engagement en faveur d'une implication au plus haut niveau illustre les efforts entrepris par le gouvernement ces dernières années afin d'instaurer la confiance dans les nombreuses protections simultanées de la confidentialité mises en place pour les informations des ressortissants et ressortissants non américains.

e) **Synthèse**

Les processus mis en place par les États-Unis pour la collecte, la conservation et la diffusion des renseignements étrangers apportent d'importantes protections de la confidentialité des informations à caractère personnel de tous les individus, quelle que soit leur nationalité. En particulier, ces processus veillent à ce que nos services de renseignement se concentrent sur leur mission de sécurité nationale en application des lois, décrets exécutifs et directives présidentielles qui les habilitent, protègent les informations contre l'accès, l'utilisation et la divulgation non autorisés et effectuent ses activités sous la supervision de plusieurs niveaux de contrôle et de surveillance, y compris par les organes parlementaires de surveillance. La PPD-28 et ses procédures d'application représentent nos efforts en vue d'étendre aux informations à caractère personnel de tous les individus, quelle que soit leur nationalité, certains principes de limitation et autres principes importants de protection des données. Les informations à caractère personnel obtenues via la collecte américaine de renseignements d'origine électromagnétique sont soumises aux principes et exigences de la législation américaine et aux directives présidentielles, y compris les protections incluses dans la PPD-28. Ces principes et exigences veillent à ce que tous les individus soient traités avec dignité et respect, quels que soient leur nationalité ou leur lieu de résidence, et reconnaissent que toute personne possède des intérêts légitimes en matière de vie privée dans le cadre du traitement de ses informations à caractère personnel.

II. LOI SUR LA SURVEILLANCE ET LES RENSEIGNEMENTS ÉTRANGERS — SECTION 702

La collecte de données au titre de la section 702 de la loi sur la surveillance et les renseignements étrangers ([1]) n'est pas «massive et indifférenciée», mais strictement orientée vers la collecte de renseignements étrangers sur la base d'objectifs légitimes déterminés au cas par cas, expressément autorisée par un mandat légal explicite, et soumise à un contrôle judiciaire indépendant ainsi qu'à une surveillance et à un examen importants de la part du pouvoir exécutif et du Congrès. La collecte au titre de la section 702 est considérée comme étant une collecte de renseignements d'origine électromagnétique soumise aux exigences de la PPD-28 ([2]).

La collecte au titre de la section 702 constitue l'une des sources les plus précieuses de renseignements en vue de protéger les États-Unis et nos partenaires européens. Des informations détaillées sur le fonctionnement et le contrôle de la section 702 sont à la disposition du public. De nombreux actes de procédures, décisions de justice et rapports de surveillance relatifs au programme ont été déclassifiés et publiés sur le site web de l'ODNI consacré à la diffusion de documents au grand public, www.icontherecord.tumblr.com. La section 702 a par ailleurs fait l'objet d'une analyse complète du PCLOB dans un rapport consultable à l'adresse https://www.pclob.gov/library/702-Report.pdf ([3]).

La section 702 a été adoptée dans le cadre de la loi de 2008 portant modification de la FISA ([4]), à l'issue d'un vaste débat public au Congrès. Elle autorise l'obtention de renseignements étrangers via le ciblage de ressortissants non américains se trouvant en dehors du territoire des États-Unis, avec l'assistance obligatoire des fournisseurs de services de communications électroniques américains. La section 702 autorise le procureur général et le DNI — deux responsables gouvernementaux nommés par le Président et approuvés par le Sénat — à soumettre des certifications annuelles à la Cour FISA ([5]). Ces certifications identifient des catégories spécifiques de renseignements étrangers à collecter, telles que des renseignements en rapport avec le contre-terrorisme ou les armes de destruction massive, qui doivent relever des catégories de renseignement étranger définies par la FISA ([6]). Comme l'a noté le PCLOB, «[c]es limitations n'autorisent *pas* la collecte illimitée d'informations sur les étrangers» ([7]).

Les certifications doivent également inclure des procédures de «ciblage» et de «limitation» à examiner et approuver par la Cour FISA ([8]). Les procédures de ciblage servent à faire en sorte que la collecte ne soit effectuée que dans les limites prévues par la législation et selon la portée définie dans les certifications; les procédures de limitation, elles, visent à limiter l'ampleur de l'obtention, de la diffusion et de la conservation de données sur les ressortissants américains, mais contiennent également des dispositions apportant une protection importante aux informations relatives aux ressortissants non américains, qui sont décrites ci-dessous. Par ailleurs, comme indiqué ci-dessus, le Président a demandé dans sa PPD-28 que les services de renseignement prévoient des mesures de protection supplémentaires en ce qui concerne les informations à caractère personnel relatives à des ressortissants non américains; ces protections s'appliquent aux informations collectées au titre de la section 702.

Une fois que la cour a approuvé les procédures de ciblage et de minimisation, la collecte au titre de la section 702 ne peut être effectuée ni en vrac, ni de façon indifférenciée, mais «consiste exclusivement à cibler des personnes spécifiques identifiées de manière individuelle», conformément au PCLOB ([9]). Le ciblage de la collecte s'effectue en utilisant des sélecteurs individuels, tels que les adresses de courrier électronique ou les numéros de téléphone, des données qui, selon

([1]) 50 U.S.C. § 1881a.

([2]) Les États-Unis peuvent également obtenir des ordonnances judiciaires au titre d'autres dispositions de la FISA relatives à la production de données, notamment de données transférées au titre du bouclier de protection des données. Voir 50 U.S.C. § 1801 et suivants. Les titres I et III de la FISA, qui autorisent respectivement la surveillance électronique et les fouilles corporelles, nécessitent une ordonnance judiciaire (sauf 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. Le titre IV de la FISA autorise l'utilisation d'enregistreurs graphiques («Pen Registers») et de dispositifs de traçage (Trap and Trace devices) dans les activités autorisées de renseignement étranger ou de contre-espionnage ou les enquêtes antiterroristes. Le titre V de la FISA autorise le FBI, sur la base d'une ordonnance d'un tribunal (sauf en cas d'urgence), d'obtenir des documents professionnels pertinents aux fins d'une activité autorisée de renseignement étranger, de contre-espionnage ou d'une enquête antiterroriste. Comme expliqué ci-dessous, la loi USA FREEDOM interdit expressément l'utilisation d'ordonnances FISA autorisant les enregistreurs graphiques et dispositifs de traçage pour la collecte en vrac de renseignements et impose l'exigence d'un «critère de sélection spécifique» afin de veiller à ce que ces pouvoirs soient utilisés de manière ciblée.

([3]) Privacy and Civil Liberties Board, «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act» (2 juillet 2014) («rapport du PCLOB»).

([4]) Voir Pub. L. No. 110-261, 122 Stat. 2436 (2008).

([5]) Voir 50 U.S.C. § 1881a(a) et (b).

([6]) Voir ibidem, § 1801(e).

([7]) Voir le rapport du PCLOB, point 99.

([8]) Voir 50 U.S.C. § 1881a(d) et (e).

([9]) Voir le rapport du PCLOB, point 111.

le personnel du renseignement américain, sont susceptibles d'être utilisées pour communiquer des renseignements étrangers du type couvert par la certification présentée à la cour ([1]). La base utilisée pour choisir la cible doit être motivée et la motivation de chaque sélecteur est ensuite contrôlée par le ministère de la justice ([2]). Le gouvernement américain a publié des informations selon lesquelles on comptait en 2014 environ 90 000 personnes ciblées au titre de la section 702, soit une infime proportion des plus de 3 milliards d'utilisateurs d'internet dans le monde entier ([3]).

Les informations collectées au titre de la section 702 sont soumises aux procédures de limitation approuvées par la cour, qui prévoient des mesures de protection pour les aux ressortissants non américains comme pour les ressortissants américains et qui ont été rendues publiques ([4]). Par exemple, les communications obtenues au titre de la section 702 sont enregistrées dans des bases de données dont l'accès est strictement contrôlé, qu'elles concernent des ressortissants américains ou non américains. Elles ne peuvent être examinées que par des agents du renseignement qui ont été formés aux procédures de limitation destinées à protéger la vie privée et qui ont reçu une autorisation d'accès spécifique pour effectuer les tâches qui leur incombent ([5]). L'utilisation des données est limitée à la détection de renseignements étrangers ou de preuves d'un crime ([6]). Conformément à la PPD-28, ces informations ne peuvent être diffusées qu'à la condition que cette diffusion présente un intérêt valable pour le renseignement étranger ou l'application de la loi; il ne suffit pas que l'une des parties à la communication ne soit pas un ressortissant américain ([7]). Par ailleurs, les procédures de limitation et la PPD-28 établissent également des limites en ce qui concerne la durée pendant laquelle des données obtenues au titre de la section 702 peuvent être conservées ([8]).

La surveillance de la section 702 est étendue et assurée par les trois branches de l'État américain. Les agences qui mettent en œuvre la législation disposent de plusieurs niveaux de contrôle interne, notamment par des inspecteurs généraux indépendants, ainsi que de contrôles technologiques de l'accès aux données. Le ministère de la justice et l'ODNI examinent et contrôlent minutieusement l'utilisation faite de la section 702 afin de s'assurer du respect des règles de droit. Les agences ont également une obligation indépendante de signaler les cas de non-conformité potentiels. Ces incidents font l'objet d'une enquête et tous les cas de non-conformité sont signalés à la Cour FISA, au conseil de surveillance du renseignement (Intelligence Oversight Board) auprès du Président et au Congrès, et les mesures correctives nécessaires sont prises ([9]). À ce jour, aucun incident relatif à une tentative volontaire de violation du droit ou de contournement des dispositions légales n'a été enregistré ([10]).

La Cour FISA joue un rôle important dans la mise en œuvre de la section 702. Elle se compose de juges fédéraux indépendants qui y sont nommés pour sept ans, mais qui, comme tous les juges fédéraux, sont nommés en tant que juges à vie. Comme mentionné ci-dessus, la Cour doit examiner les certifications annuelles et les procédures de ciblage et de limitation afin de s'assurer qu'elles sont conformes à la loi. En outre, comme également indiqué ci-dessus, les pouvoirs publics sont tenus de signaler immédiatement à la Cour tout cas de non-conformité ([11]); de fait, plusieurs avis de la Cour ont été déclassifiés et publiés afin de démontrer le niveau exceptionnel de contrôle judiciaire et d'indépendance dont elle dispose pour examiner ces infractions.

Les procédures rigoureuses de la Cour ont été décrites par son ancien président dans une lettre adressée au Congrès qui a été rendue publique ([12]). Par ailleurs, à la suite de l'adoption de la loi USA FREEDOM, décrite ci-dessous, la Cour est désormais expressément autorisée à nommer un juriste externe en tant que défenseur indépendant de la vie privée dans les cas qui présentent des difficultés juridiques nouvelles ou importantes ([13]). Un tel degré d'implication d'une instance judiciaire indépendante dans les activités de renseignement étranger d'un pays, ciblant des personnes qui n'en sont pas ressortissantes et qui ne résident pas sur son territoire est inhabituel, voire inédit, et contribue à garantir que les collectes au titre de la section 702 ne dépassent pas les limites juridiques adéquates.

([1]) Ibidem.

([2]) Ibidem. au point 8; 50 U.S.C. § 1881a(l); voir également NSA Director of Civil Liberties and Privacy Report, «NSA's Implementation of Foreign Intelligence Surveillance Act Section 702» (ci-après le «rapport de la NSA») p. 4, disponible à l'adresse http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Director of National Intelligence 2014 Transparency Report, disponible à l'adresse http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Les procédures de limitation sont disponibles aux adresses suivantes: http://www.dni.gov/files/documents/ppd-28/2014 %20NSA%20702%20Minimization%20Procedures.pdf («procédures de limitation de la NSA»); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; et http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Voir le rapport de la NSA, p. 4.

([6]) Voir par exemple les procédures de limitation de la NSA, p. 6.

([7]) Les procédures des agences de renseignement au titre de la PPD-28 sont disponibles à l'adresse http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Voir les procédures de limitation de la NSA et la PPD-28, section 4.

([9]) Voir 50 U.S.C. § 1881(l); voir également le rapport du PCLOB, p. 66 à 76.

([10]) Voir l'évaluation semestrielle du respect des procédures et lignes directrices conformément à la section 702 de la loi sur la surveillance du renseignement étranger, publiée par le procureur général et le Directeur du renseignement national, p. 2 et 3, disponible à l'adresse http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Règle 13 du règlement de procédure de la Cour FISA, disponible à l'adresse http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) 29 juillet 2013 — Lettre de M. Reggie B. Walton à M. Patrick J. Leahy, disponible à l'adresse http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Voir la section 401 de la loi USA FREEDOM, P.L. 114-23.

Le Congrès exerce une surveillance par le biais de rapports requis par la loi et transmis aux commissions du renseignement et des affaires judiciaires, ainsi que de fréquents briefings et auditions. Parmi ces rapports figurent un rapport semestriel du procureur général motivant l'utilisation de la section 702 ainsi que les éventuels cas de non-conformité ([1]); une évaluation semestrielle distincte du procureur général et du DNI étayant le respect des procédures de ciblage et de limitation, y compris la conformité avec les procédures visant à garantir que la collecte répond à un objectif valable de renseignement étranger ([2]); ainsi qu'un rapport annuel des directeurs des composantes des services de renseignement assurant notamment que les collectes au titre de la section 702 continuent à produire des renseignements étrangers ([3]).

En résumé, la collecte au titre de la section 702 est autorisée par la loi, soumise à plusieurs niveaux de contrôle, de surveillance et de supervision judiciaires et, comme la Cour FISA l'a indiqué dans un avis récemment déclassifié, elle n'est «pas effectuée en vrac ou de façon indifférenciée», mais. «sur la base […] de décisions de ciblage distinctes pour les différents canaux [de communication]» ([4]).

III. LA LOI USA FREEDOM

La loi USA FREEDOM (Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), promulguée en juin 2015, a modifié en profondeur les pouvoirs de surveillance et autres pouvoirs en rapport avec la sécurité nationale aux États-Unis et amélioré la transparence publique de l'utilisation de ces pouvoirs et des décisions de la Cour FISA, comme expliqué ci-dessous ([5]). Cette loi confère à nos professionnels du renseignement et de l'application de la loi les compétences nécessaires pour protéger la Nation tout en veillant à ce que la vie privée des individus soit suffisamment protégée dans le cadre de leur exercice. Elle améliore le respect de la vie privée et des libertés civiles tout en renforçant la transparence.

Cette loi interdite la collecte en vrac d'archives, qu'ils concernent des ressortissants américains ou non américains, au titre de différentes dispositions de la FISA ou via l'utilisation de lettres de sécurité nationale, une forme d'injonction administrative autorisée par la loi ([6]). Cette interdiction inclut spécifiquement les métadonnées téléphoniques relatives aux appels entre des personnes sur le territoire américain et des personnes hors du territoire américain et concerne également la collecte d'informations relevant du bouclier de protection des données effectuée dans l'exercice de ces compétences. Cette loi exige des pouvoirs publics qu'ils fondent toute demande d'archives, dans l'exercice de ces compétences, sur un «critère de sélection spécifique» — un critère qui identifie précisément une personne, un compte, une adresse ou un dispositif personnel d'une manière qui limite la portée des informations recherchées dans la plus grande mesure raisonnablement possible ([7]). Cela garantit également que la collecte d'informations à des fins de renseignement est précisément orientée et ciblée.

La loi USA FREEDOM a également modifié de manière substantielle les procédures devant la Cour FISA, en en améliorant la transparence et en apportant des garanties supplémentaires quant à la protection de la vie privée. Comme indiqué ci-dessus, il a permis la création d'un comité permanent d'avocats possédant une habilitation de sécurité et disposant d'une expertise en matière de protection de la vie privée et des libertés civiles, de collecte de renseignements, de technologies de communication ou d'autres domaines pertinents, qui peuvent être appelés à plaider devant la cour à titre d'amicus curiae dans les cas nécessitant une interprétation approfondie ou inédite du droit. Ces avocats sont habilités à présenter des arguments légaux en vue de défendre la protection de la vie privée et des libertés civiles, et peuvent accéder à toutes les informations, y compris classifiées, que la cour juge nécessaire à l'exercice de leurs fonctions ([8]).

Cette loi se base également sur la transparence sans précédent dont le gouvernement a fait preuve en matière de renseignement en exigeant du DNI, en consultation avec le procureur général, qu'il déclassifie ou publie un résumé non classifié de chaque décision, ordonnance ou avis rendu par la Cour FISA ou la Cour d'appel pour la surveillance du renseignement étranger (Foreign Intelligence Surveillance Court of Review) impliquant une interprétation élaborée d'une disposition de droit.

([1]) Voir 50 U.S.C. § 1881f.
([2]) Voir 50 U.S.C. § 1881a(l)(1).
([3]) Voir 50 U.S.C. § 1881a(l)(3). Certains de ces rapports sont classifiés.
([4]) Mem. Opinion and Order at 26 (FISC 2014), disponible à l'adresse http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Voir la loi USA FREEDOM de 2015, Pub. L. No. 114-23, § 401, 129 Stat. 268.
([6]) Voir ibidem, §§ 103, 201, 501. Les lettres de sécurité nationale sont autorisées par différentes dispositions législatives. Elles permettent au FBI d'obtenir des informations figurant dans des rapports de solvabilité, des états financiers et certains documents de transactions et d'abonnements électroniques de certains types de sociétés, uniquement dans un but de protection contre le terrorisme international ou les activités de renseignement clandestines. Voir 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u et 1681v; 18 U.S.C. § 2709. Les lettres de sécurité nationale sont généralement utilisées par le FBI pour rassembler des informations essentielles ne portant pas sur le contenu lors des phases initiales des enquêtes antiterroristes et de contre-espionnage — comme l'identité d'un abonné à un compte qui pourrait avoir été en communication avec les membres d'un groupe terroriste comme l'EI. Les destinataires d'une lettre de sécurité nationale ont le droit de la contester devant un tribunal. Voir 18 U.S.C. § 3511.
([7]) Voir ibidem.
([8]) Voir ibidem § 401.

La loi USA FREEDOM prévoit par ailleurs des divulgations à grande échelle d'informations sur les activités de collecte au titre de la FISA et sur les demandes de lettres de sécurité nationale. Les États-Unis doivent communiquer chaque année au Congrès et au public, entre autres informations, le nombre d'ordonnances et de certifications FISA demandées et obtenues, une estimation du nombre de ressortissants américains et non américains ciblés et concernés par la surveillance et le nombre de désignations d'*amici curiae* ([1]). La loi USA FREEDOM exige également des pouvoirs publics qu'ils communiquent publiquement le nombre de demandes de lettres de sécurité nationale relatifs aux ressortissants et ressortissants non américains ([2]).

En ce qui concerne la transparence des entreprises, la loi offre à ces dernières plusieurs moyens de déclarer publiquement le nombre total d'ordonnances et directives FISA ou de lettres de sécurité nationale qu'elles reçoivent de la part des pouvoirs publics, ainsi que le nombre de comptes clients ciblés par ces ordonnances ([3]). Plusieurs entreprises ont déjà communiqué des informations en ce sens, qui ont révélé que les demandes de renseignements concernaient peu de clients.

Ces rapports de transparence des entreprises prouvent que les demandes de renseignements des États-Unis n'affectent qu'une infime partie des données. Par exemple, le rapport de transparence récemment publié par une grande société montre que les requêtes de sécurité nationale (au titre de la FISA ou de lettres de sécurité nationale) qui lui ont été adressées ont concerné moins de 20 000 comptes alors qu'elle possédait au moins 400 millions d'abonnés. En d'autres termes, l'ensemble des requêtes de sécurité nationale américaines déclarées par cette société représentaient moins de 0,005 % de ses abonnés. Quand bien même l'une de ces requêtes aurait porté sur des données relevant de la sphère de sécurité, ce qui n'est bien entendu pas le cas, il est évident que les requêtes sont ciblées et d'une ampleur appropriée et qu'elles ne sont effectuées ni en vrac, ni de façon indifférenciée.

Enfin, alors que les dispositions législatives qui autorisent les lettres de sécurité nationale limitaient déjà les circonstances dans lesquelles le destinataire d'un tel courrier pouvait se voir interdire de le divulguer, la loi USA FREEDOM précise que ces exigences de non-divulgation doivent être périodiquement réexaminées, exige que les destinataires de ces courriers soient prévenus lorsque l'obligation de non-divulgation n'est plus fondée et prévoit des procédures codifiées pour les destinataires souhaitant contester une exigence de non-divulgation ([4]).

En résumé, les modifications importantes apportées par la loi USA FREEDOM aux compétences du renseignement américain illustrent clairement les efforts notables déployés par les États-Unis pour placer la protection des informations à caractère personnel, de la vie privée, des libertés civiles et de la transparence au centre de toutes les pratiques du renseignement américain.

IV. TRANSPARENCE

En plus de la transparence exigée par la loi USA FREEDOM, les services de renseignement américains fournissent au public de nombreuses informations supplémentaires, montrant ainsi l'exemple au niveau de la transparence de leurs activités de renseignement. Les services de renseignement ont rendu publics un grand nombre de leurs politiques, procédures, décisions de la Cour FISA et autres documents déclassifiés, assurant ainsi un niveau de transparence extraordinaire. En outre, les services de renseignement ont considérablement renforcé leur communication de statistiques sur l'utilisation faite par les pouvoirs publics de ses compétences en matière de collecte de renseignements à des fins de sécurité nationale. Le 22 avril 2015, les services de renseignement ont publié leur deuxième rapport annuel, qui présente des statistiques sur la fréquence du recours par les pouvoirs publics à ces compétences importantes. L'ODNI a également publié, sur son site web ainsi que sur le site *IC On the Record*, une série de principes concrets en matière de transparence ([5]) et un plan de mise en œuvre transposant les principes en initiatives concrètes et mesurables ([6]). En octobre 2015, le directeur du renseignement national a demandé à chaque agence de renseignement de désigner au sein de sa direction un responsable de la transparence en matière de renseignement afin de favoriser la transparence et de diriger les initiatives dans ce domaine ([7]). Le responsable de la transparence travaillera en étroite collaboration avec le responsable de la protection de la vie privée et des libertés civiles de chaque agence de renseignement, afin de veiller à ce que la transparence et le respect de la vie privée et des libertés civiles demeurent prioritaires.

([1]) Voir ibidem § 602.
([2]) Voir ibidem.
([3]) Voir ibidem § 603.
([4]) Voir ibidem §§ 502(f) à 503.
([5]) Disponible à l'adresse http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Disponible à l'adresse http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Voir ibidem.

Une illustration de ces efforts est la publication, par le responsable en chef de la protection de la vie privée et des libertés civiles de la NSA, de plusieurs rapports déclassifiés au cours des dernières années, dont des rapports sur des activités au titre de la section 702, du décret exécutif 12333 et de la loi USA FREEDOM ([1]). Les services de renseignement travaillent par ailleurs en étroite collaboration avec le PCLOB, le Congrès et les services de défense de la vie privée aux États-Unis en vue d'accroître la transparence des activités du renseignement américain, dans la mesure du possible et d'une manière qui ne nuise pas à la protection des sources et méthodes de renseignement sensibles. Dans leur ensemble, les activités de renseignement des États-Unis sont aussi transparentes, voire plus, que celles des autres nations du monde et sont aussi transparentes que ne le permet la protection des sources et méthodes sensibles.

Voici quelques exemples de la transparence accrue qui préside aux activités du renseignement américain:

— Les services de renseignement ont rendu public et mis en ligne des milliers de pages d'avis judiciaires et de procédures des agences décrivant les procédures et exigences spécifiques de nos activités de renseignement. Nous avons également publié des rapports sur le respect des restrictions applicables par les agences de renseignement.

— Les hauts responsables du renseignement évoquent souvent publiquement les rôles et activités de leur organisation, notamment en décrivant les régimes et garanties de conformité qui régissent leur travail.

— Les services de renseignement ont publié de nombreux autres documents sur leurs activités, conformément à la FISA.

— Le Président a publié la PPD-28, qui établit publiquement des limitations supplémentaires de nos activités de renseignement, tandis que l'ODNI a publié deux rapports libres d'accès sur l'application de ces limitations.

— Les services de renseignement sont désormais légalement tenus de publier les avis juridiques importants rendus par la Cour FISA, ou à tout le moins des résumés de ceux-ci.

— Les pouvoirs publics sont tenus de rendre compte annuellement de l'ampleur de l'utilisation qu'ils font de certaines compétences en matière de sécurité nationale et les entreprises y sont également autorisées.

— Le PCLOB a publié plusieurs rapports détaillés sur les activités de renseignement et continuera de le faire.

— Les services de renseignement fournissent un grand nombre d'informations classifiées aux organes parlementaires de surveillance.

— Le DNI a publié des principes de transparence visant à régir les activités des services de renseignement.

Cette grande transparence se maintiendra. Toutes les informations rendues publiques seront bien entendu accessibles au ministère du commerce et à la Commission européenne. L'examen annuel de la mise en œuvre du bouclier de protection des données, réalisé par le ministère américain du commerce et la Commission européenne, sera l'occasion pour la Commission européenne d'aborder les questions éventuellement soulevées par les informations nouvellement publiées, ainsi que toute autre question relative au bouclier de protection des données et à son fonctionnement. Nous avons été informés que le ministère pourrait, à sa discrétion, inviter les représentants d'autres acteurs, y compris les services de renseignement, à participer à cet examen. Celui-ci vient bien entendu s'ajouter au mécanisme de la PPD-28 donnant aux États membres de l'Union européenne la possibilité de signaler leurs inquiétudes en matière de renseignement à un représentant ministériel désigné.

V. RECOURS

Le droit américain met plusieurs moyens de recours à la disposition des individus qui ont fait l'objet d'une surveillance électronique illégale pour les besoins de la sécurité nationale. En vertu de la FISA, le droit de saisir les tribunaux américains n'est pas limité aux ressortissants américains. Toute personne ayant qualité pour agir dispose de moyens de

([1]) Disponible aux adresses: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

recours lui permettant de contester les actes de surveillance électronique illégaux menés au titre de la FISA. Celle-ci permet par exemple aux personnes faisant l'objet d'une surveillance électronique illégale de poursuivre des responsables du gouvernement américain à titre personnel en vue d'obtenir une réparation financière, y compris des dommages-intérêts et le remboursement des frais d'avocat. Voir 50 U.S.C. § 1810. Les personnes ayant qualité pour agir peuvent également introduire une procédure civile en vue d'obtenir une réparation financière, y compris le remboursement des frais de procédure, contre les États-Unis lorsque des informations les concernant obtenues dans le cadre d'une surveillance électronique au titre de la FISA ont été volontairement et illégalement utilisées ou divulguées. Voir 18 U.S.C. § 2712. Si les pouvoirs publics ont l'intention de divulguer des informations obtenues ou dérivées de la surveillance électronique concernant une personne lésée aux termes de la FISA ou de les utiliser contre cette personne dans une procédure judiciaire ou administrative aux États-Unis, il doit faire connaître au préalable son intention à la juridiction compétente et à la personne concernée, qui peut alors contester la légalité de la surveillance et réclamer la suppression des informations. Voir 50 U.S.C. § 1806. Enfin, la FISA prévoit également des sanctions pénales à l'encontre des personnes qui participent volontairement à une surveillance électronique illégale sous couvert de la loi ou qui utilisent ou divulguent volontairement des informations obtenues grâce à une surveillance illégale. Voir 50 U.S.C. § 1809.

Les citoyens de l'Union européenne disposent d'autres moyens pour poursuivre en justice des responsables de l'administration américaine en cas d'utilisation ou d'accès illégal des pouvoirs publics à des données, y compris en cas de violation de la loi par des agents publics dans le cadre d'un accès ou d'une utilisation illégale d'informations sous couvert d'intérêt de sécurité nationale. La loi relative à la fraude et aux abus informatiques (Computer Fraud and Abuse Act) interdit l'accès intentionnel non autorisé (ou l'abus d'un accès autorisé) aux informations d'une institution financière, à un système informatique de l'administration américaine ou à un ordinateur via l'internet, ainsi que les menaces d'endommagement d'ordinateurs protégés à des fins d'extorsion ou de fraude. Voir 18 U.S.C. § 1030. Toute personne victime d'une perte ou d'un préjudice à la suite d'une violation de cette loi peut, quelle que soit sa nationalité, poursuivre en justice le coupable (y compris s'il s'agit d'un agent public) afin d'obtenir une indemnisation ou des mesures de redressement par voie d'injonction ou de toute autre mesure équitable au titre de la section 1030(g), que des poursuites pénales aient été ou non engagées et pour autant que la violation implique au moins l'une des circonstances énoncées dans la législation. La loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act, ECPA) réglemente l'accès du gouvernement aux communications électroniques enregistrées et aux archives de transactions et abonnements électroniques détenus par des fournisseurs de communications tiers. Voir 18 U.S.C. §§ 2701 à 2712. L'ECPA autorise les personnes lésées à poursuivre en justice les représentants du gouvernement ayant accédé illégalement à des données enregistrées. L'ECPA s'applique à tous les individus, quelle que soit leur citoyenneté. Les personnes lésées peuvent se voir accorder des dommages-intérêts ainsi que le remboursement de leurs frais d'avocat. La loi relative au droit à la confidentialité financière (*Right to Financial Privacy Act*, RFPA) limite l'accès du gouvernement américain aux dossiers bancaires et boursiers des clients. Voir 12 U.S.C. §§ 3401 à 3422. Au titre de la RFPA, un client d'une banque ou d'un service boursier a le droit de poursuivre le gouvernement américain afin d'obtenir des dommages-intérêts préétablis, réels et punitifs lors de l'obtention illégale d'un accès à son dossier; en outre, la constatation d'un caractère volontaire à cet accès illégal entraîne automatiquement une enquête en vue d'une éventuelle poursuite disciplinaire contre les employés gouvernementaux concernés. Voir 12 U.S.C. § 3417.

Enfin, la loi sur la liberté d'information (FOIA) donne à toute personne la possibilité de demander l'accès aux archives d'une agence fédérale relatives à des sujets soumis à certaines catégories de dérogations. Voir 5 U.S.C. § 552(b). Il s'agit notamment de limitations de l'accès à des informations classifiées sur la sécurité nationale, aux informations à caractère personnel d'autres personnes et aux informations relatives aux enquêtes liées à l'application de la loi. Elles sont comparables aux limitations imposées par les pays qui possèdent leur propre législation sur l'accès aux informations. Ces restrictions s'appliquent tout autant aux citoyens américains qu'aux ressortissants d'autres pays. Les litiges relatifs à la communication d'archives demandées au titre de la FOIA peuvent être portés devant une juridiction administrative, puis devant un tribunal fédéral. Le tribunal est alors amené à déterminer de novo si l'accès aux archives en question a été refusé à juste titre [5 U.S.C. § 552(a)(4)(B)]. Il peut obliger les pouvoirs publics à accorder l'accès aux archives en question. Il est arrivé que les tribunaux donnent tort à des déclarations du gouvernement selon lesquelles l'accès aux informations devait être refusé car elles étaient classifiées ([1]). Bien qu'aucune réparation financière ne puisse être obtenue, les tribunaux peuvent accorder le remboursement des frais d'avocat.

VI. CONCLUSION

Les États-Unis reconnaissent que toute personne, quels que soient sa nationalité ou son lieu de résidence, doit être traitée avec dignité et respect dans le cadre de leurs activités de renseignement d'origine électromagnétique et autres activités de renseignement, quelle que soit sa nationalité ou son lieu de résidence, et que toute personne possède des intérêts légitimes en matière de vie privée dans le cadre du traitement de ses informations à caractère personnel. Les États-Unis n'utilisent le renseignement d'origine électromagnétique que dans le but d'assurer leur sécurité nationale, de défendre leurs intérêts de politique étrangère et de protéger du danger leurs citoyens et ceux de leurs alliés et partenaires. En résumé, les services de renseignement ne soumettent personne, encore moins les citoyens européens ordinaires, à une surveillance indifférenciée. La collecte de renseignements d'origine électromagnétique n'intervient que lorsqu'elle est dûment autorisée et dans des conditions strictement conformes aux limitations susmentionnées, après examen de la

([1]) Voir:New York Times v. Department of Justice, 756 F.3d 100 (2d Cir. 2014); American Civil Liberties Union v. CIA, 710 F.3d 422 (D.C. Cir. 2014).

disponibilité d'autres sources de renseignement, y compris diplomatiques et publiques, et en privilégiant les solutions de substitution appropriées et praticables. En outre, dans la mesure du possible, la collecte de renseignements d'origine électromagnétique est uniquement orientée vers des cibles ou des sujets spécifiques du renseignement étranger, à l'aide de discriminants.

La politique des États-Unis à cet égard a été clarifiée dans la PPD-28. Dans le cadre ainsi décrit, les agences de renseignement américaines n'ont ni le pouvoir légal, ni les ressources, ni la capacité technique, ni le désir d'intercepter toutes les communications effectuées dans le monde entier. Ces agences ne lisent pas les courriers électroniques de tous les citoyens américains, ni ceux de tout un chacun dans le reste du monde. Conformément à la PPD-28, les États-Unis offrent de solides protections concernant les informations à caractère personnel de ressortissants non américains collectées par le renseignement d'origine électromagnétique. Dans la mesure du possible et en fonction des besoins de la sécurité nationale, ces protections incluent des politiques et procédures destinées à limiter la conservation et la diffusion d'informations à caractère personnel concernant des ressortissants non américains comparables aux protections accordées aux ressortissants américains. Par ailleurs, comme nous l'avons vu ci-dessus, le régime de surveillance approfondie des pouvoirs conférés par la section 702 de la FISA est unique au monde. Enfin, les profondes modifications apportées à la loi américaine sur le renseignement par la loi FREEDOM et les initiatives menées par l'ODNI en vue de favoriser la transparence au sein des services de renseignement améliorent remarquablement le respect de la vie privée et des libertés civiles de toute les personnes concernées, quelle que soit leur nationalité.

Veuillez agréer, Messieurs, l'expression de ma considération distinguée.

Robert S. Litt

Le 21 juin 2016

M. Justin S. Antonipillai
Conseiller
Ministère américain du commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

M. Ted Dean
Sous-secrétaire adjoint
International Trade Administration (administration du commerce international)
1401 Constitution Avenue, N.W.
Washington, DC 20230

Monsieur Antonipillai, Monsieur Dean,

Cette lettre a pour but de fournir de plus amples informations sur la façon dont les États-Unis procèdent à la collecte en vrac de renseignements d'origine électromagnétique. Comme expliqué dans la note 5 de bas de page de la directive présidentielle nº 28 (PPD-28), on entend par collecte «en vrac» l'acquisition d'un volume relativement important d'informations ou de données issues du renseignement d'origine électromagnétique dans des conditions où les services de renseignement ne peuvent pas utiliser d'identifiant associé à une cible spécifique (tels que l'adresse électronique ou le numéro de téléphone de la cible) pour orienter la collecte. Toutefois, il ne s'agit pas pour autant d'une collecte «massive» ou «indifférenciée». En effet, PPD-28 exige également que «[l]es activités de renseignement d'origine électromagnétique sont aussi adaptées aux besoins que possible». Dans le cadre de ce mandat, les services de renseignement veillent à ce que, même lorsqu'il n'est pas possible d'utiliser des identifiants spécifiques pour cibler la collecte, les données à collecter soient susceptibles de contenir des renseignements étrangers qui répondront aux exigences définies par les responsables politiques américains, conformément à la procédure expliquée dans ma lettre précédente, et limitent la quantité d'informations non pertinentes collectées.

À titre d'exemple, les services de renseignement peuvent être amenés à acquérir des renseignements d'origine électromagnétique sur les activités d'un groupe terroriste opérant dans une région du Proche-Orient, dont on suppose qu'il planifie des attaques contre des pays d'Europe occidentale, mais sans connaître les noms, numéros de téléphone et adresses électroniques ou autres identifiants des individus associés à ce groupe terroriste. Nous pourrions choisir de cibler ce groupe en collectant des communications à destination et en provenance de cette région, qui seront ensuite passées au crible et analysées afin de déterminer les communications qui se rapportent à ce groupe. Ce faisant, les services de renseignement chercheraient à réduire autant que possible le champ de la collecte. Cette activité serait considérée comme une collecte «en vrac», puisque l'utilisation de discriminants n'est pas possible, mais il ne s'agirait pas d'une collecte «massive» ou «indifférenciée»: au contraire, elle serait orientée aussi précisément que possible.

Ainsi, même lorsqu'un ciblage au moyen de sélecteurs spécifiques n'est pas possible, les États-Unis ne collectent pas l'ensemble des communications provenant de l'ensemble des installations de communication existant dans le monde, mais ils appliquent des filtres et d'autres outils techniques pour orienter cette collecte vers les canaux de communication susceptibles de d'avoir une valeur en termes de renseignement étranger. De cette manière, les activités américaines de renseignement d'origine électromagnétique ne touchent qu'une fraction des communications transitant sur le réseau internet.

De plus, comme indiqué dans ma lettre précédente, du fait que la collecte «en vrac» comporte un plus grand risque de collecter des communications non pertinentes, la PPD-28 limite à six finalités spécifiques l'utilisation que les services de renseignement peuvent faire des renseignements d'origine électromagnétique collectés de cette façon. La PPD-28, et les politiques des agences qui la mettent en œuvre, imposent également des restrictions à la conservation et à la diffusion d'informations à caractère personnel acquises par le renseignement d'origine électromagnétique, indépendamment du mode de collecte — en vrac ou ciblée — et de la nationalité des personnes concernées.

Par conséquent, la collecte «en vrac» pratiquée par les services de renseignement n'est pas une collecte «massive» ou «indifférenciée», mais implique l'utilisation de méthodes et d'outils de filtrage afin d'orienter la collecte sur le matériel qui répondra aux exigences définies par les responsables politiques américains en matière de renseignement étranger, tout en

réduisant autant que possible la collecte d'informations non pertinentes et en prévoyant des règles strictes pour protéger les informations non pertinentes qui pourraient être acquises. Les stratégies et les procédures décrites dans la présente lettre s'appliquent à tous les types de collecte en vrac de renseignements les signaux d'origine électromagnétique, y compris la collecte en vrac de communications à destination et en provenance de l'Europe, sans que cette lettre ne confirme ni l'infirme la réalité d'une telle collecte.

Vous avez également demandé un complément d'information sur le Conseil de surveillance de la vie privée et des libertés civiles *(Privacy and Civil Liberties Oversight Board*, PCLOB) et les inspecteurs généraux, et sur leurs compétences. Le PCLOB est une agence indépendante au sein de l'exécutif américain. Les cinq membres de ce conseil bipartite sont nommés par le Président des États-Unis et confirmé par le Sénat ([1]). Chaque membre du conseil a un mandat de six ans. Les membres et les effectifs du PCLOB bénéficient des habilitations de sécurité leur permettant de s'acquitter pleinement de leurs tâches et de leurs responsabilités statutaires ([2]).

La mission du PCLOB est de veiller à ce que les efforts déployés par le gouvernement fédéral pour lutter contre le terrorisme soient mis en balance avec la nécessité de protéger la vie privée et les libertés civiles. Le Conseil assume deux responsabilités essentielles: la surveillance et le conseil. Il définit lui-même son programme de travail et détermine quelles activités de surveillance ou de conseil il souhaite mener.

Dans le cadre de sa fonction de *surveillance*, le PCLOB passe en revue et analyse les mesures prises par l'exécutif pour protéger la nation contre le terrorisme, en veillant à ce que la nécessité de ces mesures soit mise en balance avec la nécessité de protéger la vie privée et les libertés civiles ([3]). La revue la plus récente dans ce domaine que le PCLOB ait mené à terme était centrée sur les programmes de surveillance mis en place en vertu de la section 702 de la FISA ([4]). Il procède actuellement à un examen des activités de renseignement menées en vertu du décret présidentiel 12333 ([5]).

Dans le cadre de sa *fonction consultative*, le PCLOB veille à ce que les enjeux dans le domaine des libertés soient dûment pris en compte lors de l'élaboration et de la mise en œuvre des lois, réglementations et politiques liées aux efforts déployés pour protéger la nation du terrorisme ([6]).

Afin de remplir sa mission, le Conseil est habilité par la législation à accéder à l'ensemble des archives, rapports, audits, réexamens, documents, notes, recommandations et autre matériel des agences, y compris les informations classifiées en conformité avec la loi ([7]). En outre, la Conseil peut interroger, prendre la déposition ou le témoignage public de tout agent ou employé du pouvoir exécutif ([8]). De plus, le Conseil peut demander par écrit que le procureur général délivre, en son nom, des citations à comparaître contraignant les parties n'appartenant pas à l'exécutif à fournir des informations requises ([9]).

Enfin, le PCLOB est statutairement soumis à des exigences de transparence à l'égard du public. Il s'agit notamment de tenir le public informé de ses activités en organisant des séances publiques et en rendant ses rapports accessibles au public, et ce, dans toute la mesure du possible, en conformité avec la protection des informations classifiées ([10]). Par ailleurs, le PCLOB est tenu de signaler les cas où une agence du pouvoir exécutif refuse de suivre ses conseils.

Les inspecteurs généraux (IG) au sein des services de renseignement (*Intelligence Community*, IC) effectuent des audits, des inspections et des réexamens de programmes et d'activités dans ce secteur pour identifier et traiter les risques systémiques, les faiblesses et les lacunes. En outre, les IG enquêtent en cas de plaintes ou d'allégations de violations de la

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) Voir, sur un plan général, https://www.pclob.gov/library.html#oversightreports.
([5]) Voir, sur un plan général, https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); Voir également le document du PCLOB décrivant ses stratégies et procédures pour la fonction consultative (PCLOB Advisory Function Policy and Procedure, Policy 2015-004), disponible à l'adresse https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

législation ou de la réglementation, ou de mauvaise gestion; de gaspillage massif de fonds; d'abus de pouvoir; ou de menace concrète et spécifique pour la santé et la sécurité publiques découlant de programmes ou d'activité des services de renseignement. L'indépendance est la pierre angulaire de l'objectivité et de l'intégrité de chaque rapport, conclusion et recommandation émise par un IG. Le processus de nomination et de révocation des IG, la séparation des compétences opérationnelles, budgétaires et en matière de personnel; et la double exigence de rapport aux directeurs des agences de l'exécutif et au Congrès, entre autres aspects, forment la clé de voûte sur laquelle repose l'indépendance des IG.

Le Congrès a mis en place un bureau indépendant des IG dans chaque agence relevant du pouvoir exécutif, y compris dans chaque composante des services de renseignement ([1]). Depuis l'adoption de la loi d'habilitation des services de renseignement pour l'exercice 2015 (*Intelligence Authorisation Act for Fiscal Year 2015*), presque tous les IG exerçant une surveillance sur une composante des services de renseignement — y compris le ministère de la justice, l'Agence centrale de renseignement, l'Agence de sécurité nationale et les services de renseignement — sont nommés par le Président des États-Unis et entérinés par le Sénat ([2]). En outre, ces fonctionnaires ont un poste permanent, n'appartiennent à aucun parti et ne peuvent être révoqués que par le Président. Alors que la constitution des États-Unis dispose que le Président a le pouvoir de révoquer les IG, cette compétence a rarement été exercée; en pareil cas, le Président est tenu de présenter au Congrès une justification écrite dans un délai de 30 jours avant la révocation ([3]). Ce processus de nomination garantit que les agents de l'exécutif ne s'immiscent pas dans la sélection, la désignation ou la révocation d'un IG.

D'autre part, les IG disposent d'importances compétences statutaires pour effectuer des audits, des enquêtes et des réexamens concernant les programmes et les activités du pouvoir exécutif. Outre les enquêtes et examens de surveillance prévus par la loi, les IG ont toute latitude pour exercer leurs compétences de surveillance en passant en revue les programmes et activités de leur choix ([4]). Dans l'exercice de ces compétences, la loi garantit aux IG la fourniture de ressources indépendantes pour s'acquitter de leurs obligations, y compris le pouvoir d'engager leur propre personnel et de motiver séparément leurs demandes de crédits budgétaires au Congrès ([5]). La loi garantit aux IG l'accès aux informations nécessaires à l'exécution de leurs tâches. Ils ont notamment autorité pour avoir directement accès à l'ensemble des archives des agences et à tous les documents détaillant les programmes et activités d'une agence, quelle que soit leur classification; pour ordonner la production d'informations et de documents; et de faire prêter serment ([6]). Dans des cas limités, le directeur d'une agence relevant de l'exécutif peut interdire l'activité d'un IG si, par exemple, l'audit ou l'enquête menés par celui-ci portaient sensiblement atteinte aux intérêts nationaux des États-Unis. Là encore, l'exercice de cette compétence est extrêmement rare et, dans ce cas, le directeur de l'Agence devrait en notifier la motivation dans les 30 jours au Congrès ([7]). D'ailleurs, le directeur du renseignement national n'a jamais fait usage de cette compétence limitative à l'encontre des activités d'aucun IG.

Par ailleurs, les IG ont pour tâche de garder tant les directeurs des agences relevant du pouvoir exécutif que le Congrès pleinement et constamment informés, au moyen de rapports, des fraudes et autres problèmes graves, abus et irrégularités décelés dans les programmes et activités du pouvoir exécutif ([8]). L'obligation de double rapport renforce l'indépendance des IG, en assurant la transparence de leurs procédures de surveillance et en offrant aux directeurs des agences la possibilité de mettre en œuvre leurs recommandations avant que le Congrès ne puisse arrêter des mesures législatives. Ainsi, les IG sont légalement tenus de rédiger des rapports semestriels pour décrire les problèmes rencontrés ainsi que les mesures correctives adoptées jusque-là ([9]). Les agences relevant du pouvoir exécutif prennent les constatations et les

---

([1]) Sections 2 et 4 de la loi relative aux inspecteurs généraux (Inspector General Act) de 1978, telle que modifiée; section 103H(b) et (e) de la loi sur la sécurité nationale (National Security Act) de 1947, telle que modifiée; section 17(a) de la loi relative à l'Agence centrale de renseignement (Central Intelligence Act).

([2]) Voir Pub. L. No. 113-293, 128 Stat. 3990, (19 décembre 2014). Seuls les IG pour l'Agence du renseignement militaire (Defense Intelligence Agency) et l'Agence nationale de renseignement géospatial (National Geospatial-Intelligence Agency) ne sont pas nommés par le Président; cependant, les IG du ministère de la défense et des services de renseignement disposent de compétences partagées pour ces agences.

([3]) Section 3 de l'Inspector General Act de 1978, telle que modifiée; section 103H(c) de la National Security Act; et section 17(b) de la Central Intelligence Act.

([4]) Voir sections 4(a) et 6(a)(2) de l'Inspector General Act de 1947; section 103H(e) et (g)(2)(A) de la National Security Act; section 17(a) et (c) de la Central Intelligence Act.

([5]) Sections 3(d), 6(a)(7) et 6(f) de l'Inspector General Act; sections 103H(d), (i), (j) et (m) de la National Security Act; sections 17(e)(7) et (f) de la Central Intelligence Act.

([6]) Section 6(a)(1), (3), (4), (5), et (6) de l'Inspector General Act; sections 103H(g)(2) de la National Security Act; section 17(e)(1), (2), (4), et (5) de la Central Intelligence Act.

([7]) Voir, par exemple, sections 8(b) et 8E(a) de l'Inspector General Act; section 103H(f) de la National Security Act; section 17(b) de la Central Intelligence Act.

([8]) Section 4(a)(5) de l'Inspector General Act; section 103H(a)(b)(3) et (4) de la National Security Act; section 17(a)(2) et (4) de la Central Intelligence Act.

([9]) Section 2(3), 4(a), et 5 de l'Inspector General Act; section 103H(k) de la National Security Act; section 17(d) de la Central Intelligence Act. Les rapports que l'inspecteur général du ministère de la justice a rendus publics sont disponibles à l'adresse http://oig.justice.gov/reports/all.htm. De même, l'inspecteur général des services de renseignement met ses rapports semestriels à la disposition du public à l'adresse https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

recommandations des IG au sérieux et il n'est pas rare que les IG mettent en avant l'acceptation et l'application, par les agences, de leurs recommandations dans les rapports semestriels ou autres soumis au Congrès, et parfois communiqués au grand public ([1]). Outre cette activité de double rapport, les IG sont également chargés d'accompagner les lanceurs d'alerte au sein du pouvoir exécutif lorsqu'ils décident de divulguer aux commissions de surveillance compétentes du Congrès des fraudes, gaspillages ou abus dans les programmes et activités du pouvoir exécutif. Ceux qui se manifestent ainsi ont la garantie que leur identité ne sera pas divulguée au pouvoir exécutif, ce qui les met à l'abri d'éventuelles mesures de représailles interdites, d'ordre professionnel ou touchant à leur habilitation de sécurité, pour avoir communiqué des informations aux IG ([2]). Étant donné que les lanceurs d'alerte sont souvent à l'origine des enquêtes menées par les IG, la possibilité de faire part de leurs préoccupations au Congrès sans interférence du pouvoir exécutif accroît l'efficacité de la surveillance réalisée par les IG. En raison de cette indépendance, les IG peuvent favoriser le progrès de l'économie, de l'efficacité et la responsabilisation dans les agences relevant du pouvoir exécutif en toute objectivité et intégrité.

Pour finir, le Congrès a mis en place un conseil des inspecteurs généraux en faveur de l'intégrité et de l'efficacité (*Council of Inspectors General on Integrity and Efficiency*). Ce conseil, entre autres activités, élabore des normes pour les audits, les enquêtes et les réexamens des IG; encourage la formation; et a compétence pour se pencher sur les allégations d'action fautive des IG, exerçant ainsi un regard critique sur ces instances chargées de surveiller toutes les autres ([3]).

J'espère que ces informations pourront vous être utiles.

Sincères salutations,
Robert S. Litt
Conseiller général

([1]) Section 2(3), 4(a), et 5 de l'Inspector General Act; section 103H(k) de la National Security Act; section 17(d) de la Central Intelligence Act. Les rapports que l'inspecteur général du ministère de la justice a rendus publics sont disponibles à l'adresse http://oig.justice.gov/reports/all.htm. De même, l'inspecteur général des services de renseignement met ses rapports semestriels à la disposition du public à l'adresse https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Section 7 de l'Inspector General Act; section 103H(g)(3) de la National Security Act; section 17(e)(3) de la Central Intelligence Act.

([3]) Section 11 de l'Inspector General Act.

ANNEXE VII

Lettre de M. Bruce Swartz, sous-procureur général adjoint et conseiller aux affaires internationales (ministère américain de la justice)

Le 19 février 2016

M. Justin S. Antonipillai
Conseiller
Ministère américain du commerce
1401 Constitution Ave., NW
Washington, DC 20230

M. Ted Dean
Sous-secrétaire adjoint
International Trade Administration (administration du commerce international)
1401 Constitution Ave., NW
Washington, DC 20230

Monsieur Antonipillai, Monsieur Dean,

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]). Ces procédures légales 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 autocertifiées au titre du cadre du bouclier de protection des données États-Unis/UE, sans distinction de nationalité de la personne concernée. En outre, les sociétés qui font l'objet d'une procédure légale de leurs données aux États-Unis peuvent contester celui-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 protégés dans leurs personne, résidence, papiers et effets contre toute perquisition et saisie présentant un caractère déraisonnable est inviolable, et aucun mandat ne peut être délivré, si ce n'est pour de sérieux motifs appuyés par serment ou déclaration, ni sans qu'il décrive avec précision le lieu à fouiller et les personnes ou objets 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). Lorsque l'obligation de mandat n'est pas applicable, le quatrième amendement soumet 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.

Autorités répressives en matière pénale:

Les procureurs fédéraux, qui sont des agents 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

([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) 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]) Le présent document a pour objet les pouvoirs réglementaires et répressifs octroyés au titre du droit fédéral; les violations du droit des États sont examinées par les États concernés et poursuivies devant les juridictions d'État. Les autorités d'État chargées de l'application de la loi 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 au titre de la constitution 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.

pénale en utilisant plusieurs types de procédures juridiques contraignantes, dont des citations à comparaître devant un grand jury («grand jury subpoenas»), des injonctions administratives et des 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 de comparution relatives à 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 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 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 de comparution, 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 compagnies de téléphone fournissant un accès internet et d'autres fournisseurs de services tiers, conformément au titre II de l'ECPA, également appelée loi sur les communications enregistrées (*Stored Communications Act*, 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 fournisseurs de services internet 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, 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.

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 2522. 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 — 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. Voir l'amendement IV de la Constitution américaine (abordé plus en détail ci-dessus), Fed. R. Crim. P. 41. La personne concernée par un mandat de perquisition peut chercher à faire annuler celui-ci au motif qu'il est trop large, qu'il est vexatoire ou qu'il a été obtenu de manière illégale. De même, les parties lésées ayant la qualité pour agir peuvent réclamer la suppression des preuves obtenues lors d'une fouille illégale. Voir Mapp v. Ohio, 367 U.S. 643 (1961).

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 Federal Bureau of Investigation (FBI) (septembre 2008) (Attorney General's Guidelines for Domestic Federal Bureau of Investigation Operations, ci-après «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 impact 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 les 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(DIOG). 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 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.

Compétences civiles et réglementaires (intérêt public):

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. Partie X. Les autres sociétés peuvent invoquer la *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 la loi sur le droit à la confidentialité financière (*Right to Financial Privacy Act*), 12 U.S.C. §§ 3401 à 3422. 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 du 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.

Veuillez agréer, Messieurs, l'expression de ma considération distinguée.

Bruce C. Swartz

Sous-procureur général adjoint et conseiller aux affaires internationales