CHAPITRE 1 :

RÉSUMÉ DE TÉMOIGNAGE

[1] Ce document est une traduction de la version originale en anglais du Chapitre 1 du rapport d'expertise soumis par le Professeur Peter Swire à la Haute Cour d'Irlande dans le cadre du litige où Max Schrems demande si les transferts de données à caractère personnel en vertu de Clauses contractuelles standard sont protégées de manière adéquate par le droit de l'Union européenne en matière de vie privée. En vertu des règlementations irlandaises, Swire a été désigné par Facebook en sa qualité d'expert, mais il lui a été demandé de donner son opinion personnelle concernant la législation des États-Unis, et Swire a conservé un contrôle éditorial complet sur le contenu de son témoignage. La décision de rendre le rapport public a été prise par Swire et n'était pas une décision de Facebook. Le rapport complet, ainsi que des documents explicatifs supplémentaires sont disponibles en anglais sur www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony.

INTRODUCTION

[1] Ce chapitre est un résumé de témoignage, avec beaucoup de points développés plus en détail dans les chapitres 2 à 9. Je comprends que mon devoir d'expert est d'aider la Cour sur des questions relevant de mon domaine d'expertise et cela l'emporte sur tout devoir ou obligation que je pourrais avoir envers la partie qui m'a engagé, ou envers toute partie susceptible de payer mes honoraires.

[2] Dans ce chapitre, la partie 1 contient un résumé de mon expérience sur les questions présentées devant la Cour, en tant qu'expert de la vie privée depuis plus de vingt ans, à la fois sur la législation en matière de surveillance aux États-Unis (EU) et sur la législation en matière de protection des données de l'Union européenne (UE). Il reprend l'historique de mes critiques universitaires relatives aux pratiques de surveillance américaines.

[3] La partie 2 résume le système de garanties de la législation américaine et les pratiques protégeant toutes les personnes, à la fois dans et hors des États-Unis. Ces diverses garanties sont décrites en détail dans les chapitres 3 et 4, et incluent plusieurs organes de contrôle et exigences de transparence, ainsi que l'examen judiciaire des enquêtes de renseignement étranger. Les agences de renseignement ont souvent besoin d'agir en secret afin de détecter les efforts de renseignement d'autres pays et pour des raisons impérieuses de sécurité nationale. Les États-Unis ont développé de multiples manières d'assurer la surveillance par des personnes ayant accès à des informations classifiées dans le cadre d'activités secrètes indispensables, et de créer de la transparence de manière à ne pas compromettre la sécurité nationale.

[4] Ces garanties systémiques sont abordées dans la partie 2 :

1. Le contexte historique du système législatif américain concernant les renseignements étrangers, ainsi que les garanties fondamentales s'inscrivent dans le système américain de démocratie constitutionnelle en vertu de l'état de droit ;

2. Les garanties statutaires systémiques régissant la surveillance du renseignement étranger ;

3. Les mécanismes de contrôle ;

4. Les mécanismes de transparence ; et

5. Les garanties administratives qui sont importantes dans la pratique et qui complètent les garanties législatives.

[5] À mon avis, le système américain fournit dans l'ensemble des garanties efficaces contre les abus de pouvoirs de surveillance secrète. Je suis d'accord avec l'équipe dirigée par Ian Brown, professeur à Oxford, lequel, après avoir comparé les garanties américaines par rapport à d'autres pays, a conclu que « les États-Unis constituent désormais une référence dans les normes concernant le renseignement étranger » et que le cadre juridique de la collecte de renseignements

étrangers aux États-Unis contient des règles plus claires en matière de collecte, d'utilisation, de partage et de surveillance des données relatives aux ressortissants étrangers que les législations de presque tous les États membres de l'UE.[2] En outre, comme le montre l'analyse de la Cour de Surveillance du Renseignement Étranger (Foreign Intelligence Surveillance Court) dans le chapitre 5, ces normes juridiques rigoureuses sont mises en œuvre de manière efficace dans la pratique, sous la supervision de juges indépendants bénéficiant d'un accès à des informations top-secrètes. En outre, ces garanties systémiques dans le domaine du renseignement étranger sont complétées par des garanties dans le domaine de la procédure pénale qui sont plus strictes que celles en vigueur dans les États membres de l'UE à plusieurs égards importants.

[6] La partie 3 décrit comment les individus (y compris les résidents des États membres de l'UE) ont accès à de multiples recours aux États-Unis en cas de violations de la vie privée. Elle décrit les différentes voies qu'une personne lésée aux États-Unis ou un résident d'un État membre de l'UE peut emprunter en réponse à des préoccupations concernant des violations de la vie privée :

1. J'aborde des recours judiciaires individuels contre le gouvernement des États-Unis, y compris les accords Privacy Shield (accord sur protection de la vie privée) et Umbrella Agreement (accord-cadre) récemment finalisés, ainsi que la loi Judicial Redress Act (loi sur le recours juridictionnel) récemment adoptée.

2. J'examine les recours civils et criminels disponibles dans les cas où des personnes, y compris des employés du gouvernement, violent des règles en matière d'écoute téléphonique et d'autres règles de surveillance en vertu de lois telles que la Stored Communications Act (loi sur les communications enregistrées), la Wiretap Act (loi sur les écoutes téléphoniques) et la Foreign Intelligence Surveillance Act (loi sur la surveillance du renseignement étranger).

3. Je mets en lumière trois voies de recours non-judiciaires que toute personne aux États-Unis ou dans l'UE peut choisir : le Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles), les Congressional committees (comités du Congrès), ainsi que le recours à la presse libre et à des organisations non gouvernementales de défense de la vie privée aux États-Unis.

4. J'analyse des recours individuels contre des entreprises américaines qui divulguent des informations de manière inappropriée au gouvernement des États-Unis concernant des clients ou d'autres personnes. Ces causes d'action contre des sociétés américaines peuvent être portées à la fois par des individus (ressortissants américains ou non) et par des agences administratives fédérales

[2] Ian Brown et al., *Towards Multilateral Standards for Surveillance Reform* (2015), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.

des États-Unis.

5. J'examine également les recours disponibles en vertu de la législation d'État aux États-Unis, y compris des applications par des procureurs généraux d'Etat, ainsi que des droits privés d'action, qui sont généralement beaucoup plus faciles à faire valoir aux États-Unis que dans l'UE.

[7] **Pour résumer sur les parties 2 et 3, la combinaison de garanties systémiques et de recours individuels aux États-Unis est, à mon avis, efficace et adéquate dans la protection des données à caractère personnel des personnes non américaines. Par ailleurs, la Cour de justice de l'Union européenne (CJUE) a annoncé une norme juridique d'« équivalence essentielle » pour les transferts de données à caractère personnel vers des pays tiers comme les États-Unis. D'après mon examen complet de la législation et de la pratique aux États-Unis, et mes années d'expérience en droit sur la protection des données dans l'UE, ma conclusion est que, dans l'ensemble, les États-Unis offrent de meilleures garanties sur le renseignement concernant les données à caractère personnel que les États membres de l'UE. Pour être plus précis, les garanties américaines sont au moins « essentiellement équivalentes » à celle de l'Union européenne. Par conséquent, je ne vois pas de fondement en droit ou de fait pour conclure que les États-Unis manquent de protections adéquates, en raison de ses activités de renseignement, dans le transfert de données à caractère personnel vers les États-Unis depuis l'UE.**

[8] La partie 4 traite de l'impact potentiellement très large si l'UE estimait qu'il existait un manque d'« adéquation » ou d'« équivalence essentielle ». Vous trouverez ci-dessous les principales conclusions auxquelles je parviens sur la base de l'analyse effectuée dans le présent chapitre et les chapitres associés :

1. La législation américaine définit le terme « fournisseur de services de communications électroniques » au sens large pour inclure toute entreprise fournissant un système de communication par courriel ou autre. Une conclusion d'insuffisance devrait s'appliquer à l'ensemble de ces fournisseurs de services. L'effet de cette procédure sur des entreprises ayant des activités aux États-Unis et dans l'UE pourrait donc s'avérer potentiellement très large.

2. Les garanties contre la surveillance dans la plupart ou dans tous les autres pays en dehors de l'UE sont moins étendues que celles mises en place aux États-Unis. L'effet d'une conclusion d'inadéquation semblerait donc logiquement devoir s'appliquer aux transferts vers tous les pays non membres de l'UE, à l'exception des pays où les garanties contre la surveillance sont supérieures à celles des États-Unis.

3. Une conclusion d'inadéquation concernant les clauses contractuelles types (Standard Contract Clauses, SCC) pourrait avoir des répercussions sur d'autres bases légales pour les transferts de données. Je ne fais aucune déclaration sur la question de savoir si la conclusion d'inadéquation

concernant les SCC entraînerait une conclusion d'inadéquation sur le Privacy Shield (protection de la vie privée) ou des règles d'entreprise contraignantes (Binding Corporate Rules ou BCR). La discussion soutient ici la possibilité d'une « conclusion d'inadéquation catégorique » - une conclusion d'inadéquation qui s'appliquerait non seulement aux SCC, mais également au Privacy Shield et aux BCR. Une conclusion d'inadéquation catégorique aurait des conséquences importantes sur l'ensemble des relations UE/États-Unis, affectant les relations étrangères, la sécurité nationale, les intérêts économiques et d'autres intérêts des États membres et de l'UE elle-même.

4. Ce témoignage soutient l'opinion qu'une conclusion d'inadéquation aurait des effets importants sur le bien-être de l'économie de l'UE. Les institutions de l'UE et les États membres ont clairement indiqué l'importance économique du maintien des flux de données avec les États-Unis. En outre, l'Accord général sur le commerce des services interdit la « discrimination entre les pays où des conditions similaires existent ». Un tel cas de discrimination semblerait devoir se produire si les transferts vers les États-Unis étaient exclus, malgré des garanties contre la surveillance moins étendues dans la plupart des pays non membres de l'UE et dans certains États membres eux-mêmes.

5. Une conclusion d'inadéquation pourrait également créer de grands risques pour la sécurité nationale et la sûreté publique de l'UE. Les obligations de l'OTAN et les obligations découlant d'autres traités mettent l'accent sur l'échange d'informations à des fins de sécurité nationale. L'UE a déclaré que le partage d'informations entre l'UE et les États-Unis est « essentiel dans la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris en matière de terrorisme. »

[9] Pour résumer, la combinaison de garanties systémiques et de recours individuels aux États-Unis est, à mon avis, efficace et adéquate dans la protection des données à caractère personnel des personnes non américaines. Ces actions sont nécessaires et mises en œuvre conformément à la loi. À la lumière de ces garanties et des recours mis à la disposition des citoyens de l'UE dans le cadre des données transférées vers les États-Unis, je crois et j'affirme respectueusement que la poursuite des transferts de données à caractère personnel en vertu de Clauses contractuelles types est nécessaire dans une société démocratique en vue de protéger les intérêts vitaux de l'UE, notamment la sécurité nationale, la sûreté publique et le bien-être économique.

PARTIE 1 :
Résumé biographique de Peter Swire

[10] Mon expertise globale en matière de vie privée s'est construite sur une période de 20 ans au cours de laquelle je me suis concentré principalement sur des questions de vie privée et de cybersécurité, à la fois en tant que professeur et haut fonctionnaire du gouvernement.[3] J'ai écrit

[3] Le chapitre 2 fournit plus de détails sur mon expérience et mes compétences pertinentes.

six livres et de nombreux articles universitaires, et j'ai témoigné devant une douzaine de comités du Congrès des États-Unis. Je suis le principal auteur du manuel standard utilisé pour l'examen sur la vie privée dans le secteur du droit privé de l'Association internationale des professionnels de la vie privée (International Association of Privacy Professionals, IAPP).[4] En 2015, l'IAPP, parmi ses plus de 20 000 membres, m'a décerné son Prix du leadership de la vie privée (Privacy Leadership Award).

[11] Pour le gouvernement, sous le Président Bill Clinton, j'ai eu le rôle de conseiller en chef pour la vie privée dans le Bureau de la gestion et du budget des États-Unis (US Office of Management and Budget), devenant ainsi la première personne à assumer la responsabilité de l'ensemble de l'administration américaine concernant la vie privée. Sous le président Barack Obama, j'ai été assistant spécial du Président pour la politique économique en 2009-2010. En 2013, après les premières révélations de Snowden, le Président Obama m'a nommé comme l'un des cinq membres du groupe d'étude sur les technologies de renseignement et de communication (Review Group on Intelligence and Communications Technology) (que j'appelle le « Groupe d'étude »).

[12] À ma connaissance, je suis la seule personne à avoir écrit à la fois un livre sur la législation de l'UE en matière de protection des données et un livre sur la législation américaine concernant le renseignement. Dans le chapitre 2, je mets en avant mes expériences dans ces deux domaines, y compris la façon dont ces expériences ont informé et formé mon opinion sur ces questions depuis plus de vingt ans.

[13] De mon point de vue, la pertinence globale des protections liées aux pratiques de surveillance des États-Unis a beaucoup évolué au fil du temps, à la lumière des réformes pro-vie privée que les États-Unis ont adoptées. En 2004, mon article de synthèse juridique sur « Le système législatif du renseignement étranger » a critiqué plusieurs aspects du régime américain.[5] Environ 10 recommandations issues de ce document font désormais partie du droit et de la pratique aux États-Unis, comme l'indique l'annexe au chapitre 2. De nombreuses autres réformes ont eu lieu depuis 2013, comme l'indique mon témoignage de 2015 pour l'agence belge de la vie privée (2015 Testimony for the Belgium Privacy Agency).[6] Sur la base de ces réformes et de mon étude des systèmes dans d'autres pays, mon évaluation du système américain s'est avérée conforme à celle de l'équipe d'Oxford qui estime que les États-Unis constituent une « référence » dans les principes de transparence, les procédures et le contrôle de la surveillance en matière de sécurité nationale.[7]

---

[4] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, INT'L ASSOC. OF PRIV. PROF. (2012) https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf.

[5] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004), http://peterswire.net/wp-content/uploads/Swire-the-System-of-Foreign-Intelligence-Surveillance-Law.pdf.

[6] Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, 32 Georgia Inst. Tech. Scheller College of Bus. Res. Paper No. 36 (Dec. 18, 2015), http://ssrn.com/abstract=2709619. Ce document a été présenté sous la forme d'un livre blanc à l'autorité belge en charge de la vie privée à sa demande pour son Forum sur « Les conséquences du jugement dans l'affaire Schrems. »

[7] Brown et al., *supra* note 1.

PARTIE 2 :
Garanties systémiques dans la législation et la pratique aux États-Unis

[14] Le gouvernement américain est fondé sur le principe d'équilibre contre les excès de pouvoir. Le risque d'abus est potentiellement important pour les agences de services secrets dans une société ouverte et démocratique : les personnes au pouvoir peuvent chercher à s'accrocher au pouvoir en surveillant leurs ennemis. Les États-Unis ont connu ce problème dans les années 1970, lors de l'effraction du Watergate, quartier général du Parti démocrate alors dans l'opposition. En réponse, les États-Unis ont adopté de nombreuses mesures de protection contre les abus, y compris la loi sur la surveillance du renseignement étranger (Foreign Intelligence Surveillance Act, FISA) de 1978. Au cours des dernières années, après les révélations de Snowden qui ont commencé en 2013, les États-Unis ont promulgué un ensemble complet de garanties supplémentaires contre la surveillance excessive, comme le montre la liste comprenant deux douzaines de réformes abordées dans mon témoignage de 2015 pour les organismes européens de règlementation de la vie privée (2015 Testimony for European privacy regulators),[8] ainsi que d'autres mesures de protection mises en place par la suite. Dans l'ensemble, une grande partie des protections les plus efficaces de la vie privée existent à mon avis au niveau *systémique*, plutôt que principalement sur une base rétroactive, au moyen d'un recours individuel.[9]

[15] Cette procédure évalue la pertinence des protections contre la surveillance excessive qui se produit lorsque des données à caractère personnel dans l'UE sont transférées vers les États-Unis. Lorsque le gouvernement des États-Unis effectue des écoutes téléphoniques ou autrement obtient l'accès à des données à caractère personnel aux États-Unis, l'enquête menée aux États-Unis est régie principalement par les règles en matière de renseignement étranger ou des règles pénales.[10]

[16] Je n'aborde pas en détail l'Ordre exécutif 12,333 en raison de ma compréhension de la portée de la procédure, laquelle concerne l'adéquation des garanties contre la surveillance excessive en cas de transfert de données à caractère personnel depuis l'UE vers les États-Unis. L'Ordre exécutif 12,333 est « la principale autorité de la branche exécutive pour les activités de renseignement étranger *qui n'est pas régie par le FISA* » et constitue, en effet, la « principale autorité dirigeante pour les activités de renseignement des États-Unis *à l'extérieur des États-*

[8] Swire, *US Surveillance Law*, *supra* note 5.

[9] *See* Swire, *The System of Foreign Intelligence Surveillance Law*, *supra* note 4. Le chapitre 2 concernant la biographie comprend une annexe montrant le grand nombre de réformes proposées dans l'article de 2004 qui sont depuis devenues la loi et la pratique aux États-Unis.

[10] Lorsque ces perquisitions ont lieu en vertu d'une ordonnance mandatoire, elles suivent généralement le régime du renseignement étranger ou celui de l'application de la loi. L'article 50 du Code des États-Unis 1802(a) autorise une collecte limitée pour une période d'un an ou moins, sur instruction du Président et avec l'approbation du procureur général, pour (1) la collecte de communications exclusivement entre ou parmi des puissances étrangères ; et (2) la collecte de renseignements techniques qui n'incluent pas des communications verbales entre individus, dans des installations sous le contrôle d'une puissance étrangère.

Unis. »[11] Pour les transferts de données, les États-Unis pouvaient logiquement collecter des informations de deux manières différentes. Premièrement, si les données à caractère personnel sont collectées à l'intérieur des États-Unis, la collecte se fait généralement en vertu d'autorités d'application des lois ou d'autorités de renseignement étranger, notamment le FISA. Deuxièmement, le gouvernement des États-Unis pourrait chercher à obtenir l'accès aux données pendant leur transfert, par exemple par le biais des câbles sous-marins. Comme cela est abordé dans le chapitre 3, la Commission de l'UE a pris en considération cette possibilité dans son avis sur le Privacy Shield et trouvé une protection adéquate.[12] En outre, ces dernières années, le cryptage renforcé est devenu la norme pour la transmission de communications de réseau social, de messagerie web, et d'autres types de communications, de sorte que toute accès hypothétique aux câbles sous-marins par une agence de renseignement serait difficile ou impossible par rapport à l'accès à des communications non cryptées.[13]

I. Garanties systémiques dans le renseignement étranger

[17] Mon témoignage résume la discussion détaillée dans le chapitre 3 des garanties systémiques dans le renseignement étranger. La partie A fournit un contexte historique du système législatif américain concernant le renseignement étranger, ainsi que les garanties fondamentales s'inscrivant dans le système américain de démocratie constitutionnelle en vertu de l'état de droit ; La partie B décrit les garanties statutaires systémiques régissant la surveillance du renseignement étranger ; La partie C décrit les mécanismes de contrôle, et la partie D les mécanismes de transparence. La partie E décrit les garanties administratives qui sont importantes dans la pratique et qui complètent les garanties législatives. Mon témoignage résume également comment ces garanties s'appliquent dans un cas d'étude, lequel est énoncé dans le chapitre 5, sur la manière dont la Cour de Surveillance du Renseignement Étranger a fourni ces garanties dans la pratique.

[18] Dans l'ensemble, à mon avis, un impressionnant système de surveillance a été mis en place concernant les pratiques de renseignement étranger des États-Unis. Comme nous l'avons vu dans le chapitre 6, je suis d'accord avec la conclusion d'une étude menée par un expert de la vie privée et le professeur d'Oxford, Ian Brown, laquelle a conclu que le système américain dispose « de règles beaucoup plus claires en matière de collecte, d'utilisation, de partage et de surveillance des données relatives aux ressortissants étrangers que les législations de presque

---

[11] See PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY 70 (Dec. 12, 2014) [hereinafter "REVIEW GROUP REPORT"], https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (souligné dans l'original) ; *see also* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CIVIL LIBERTIES AND PRIVACY OFFICE, CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE 2008 REVISION OF EXECUTIVE ORDER 12333 3 (2008, and revised in 2013) https://www.dni.gov/files/documents/CLPO/CLPO_Information_Paper_on_2008_Revision_to_EO_12333.pdf (« les informations du FISA sont soumises aux dispositions du FISA et ne peuvent pas être affectées par un Ordre exécutif. »).

[12] See Chapter 3, Section VI(B).

[13] See Peter Swire, Testimony before the US Senate Commerce Comm. on "How Will the FCC's Proposed Privacy Rules Affect Consumers and Competition?" (July 12, 2016) (discussion sur la prévalence croissante du cryptage), https://iisp.gatech.edu/sites/default/files/images/swire_commerce_fcc_privacy_comments_07_12_2016.pdf.

tous les États membres de l'UE. »[14] Une question centrale dans cette affaire est de savoir si les États-Unis disposent de garanties « adéquates » autour des informations de surveillance ; mon examen des garanties correspond à celui du professeur Brown : le système américain offre en général des règles plus claires et plus étendues que les législations équivalentes dans les États membres de l'UE. En outre, l'étude de cas sur la Cour de Surveillance du Renseignement Étranger montre à quel point ces règles sont mises en pratique aux États-Unis. À ma connaissance, il n'existe aucune preuve semblable de d'un tel niveau de protection dans la pratique au sein des États membres.

A. Les États-Unis en tant que démocratie constitutionnelle en vertu de l'état de droit

[19] L'évaluation la plus fondamentales d'« adéquation » ou d'« équivalence essentielle » consiste à déterminer si le pays protège les droits et libertés de la nation en vertu de l'état de droit. La Constitution des États-Unis a créé un système d'équilibre des pouvoirs entre les trois branches du gouvernement. Ce système, qui a fait ses preuves, fonctionne sans interruption depuis 1790. Le pouvoir judiciaire est une branche séparée de l'administration américaine. Il est composé de juges indépendants qui exercent le pouvoir de révision judiciaire.[15] La Constitution des États-Unis énumère les droits fondamentaux qui servent de contrôle systémique contre les abus, puisque les juges peuvent annuler l'action du gouvernement s'ils l'estiment inconstitutionnelle le cas échéant.[16]

[20] Pour la protection contre l'accès par le gouvernement à des données à caractère personnel, le Quatrième amendement de la Constitution des États-Unis, qui interdit les recherches non motivées contre leur « personne, domicile, papiers et effets », joue un rôle particulièrement important.[17] Les recherches de renseignement étranger sur une personne américaine ou non-américaine sont toujours soumises au Quatrième amendement, dans la mesure où ces recherches doivent satisfaire à l'ensemble des dispositions du Quatrième amendement pour être jugées « raisonnables ».[18] Ces garanties constitutionnelles s'appliquent aux recherches menées aux États-Unis (y compris concernant les données transférées aux États-Unis).[19] Comme

---

[14] Brown et al., *supra* note 1, at 3.

[15] En ce qui concerne les garanties d'indépendance des juges, voir Chapter 3, Section I(B). Le pouvoir judiciaire a l'autorité pour s'engager dans la révision judiciaire depuis 1803 et l'affaire de la Cour suprême *Marbury c. Madison*, 5 U.S. 137 (1803).

[16] *Voir* Chapter 3, Section I(C).

[17] *Voir* U.S. CONST. amend. IV, traité plus en détail dans le chapitre 3, article I, paragraphe C.

[18] *In re Sealed Case*, 310 F.3d 717 (F.I.S.C.R. 2002), http://law.justia.com/cases/federal/appellate-courts/F3/310/717/495663/. Pour une discussion plus approfondie du Quatrième amendement dans le contexte de la surveillance, *voir le* chapitre 3, article II, paragraphe A.

[19] Dans certains écrits européens traitant de la législation américaine, il existe une confusion au sujet de l'effet d'affaires traitées par la Cour suprême des États-Unis définissant la portée de la protection offerte par le Quatrième amendement, comme dans l'affaire *États-Unis c. Verdugo-Urquidez*, 494 U.S. 1092 (1990). [Le Quatrième amendement s'applique aux recherches au sein des États-Unis, lorsque le non-résident dispose de « connexions volontaires importantes » avec les États-Unis, telle qu'une présence physique dans le pays. La Cour suprême n'a pas abordé la question de savoir si le Quatrième amendement s'appliquait à la fouille de données de non-ressortissants lorsque les données sont situées à l'intérieur des États-Unis, mais qu'il n'existe aucune « connexion volontaire importante » aux États-Unis. [Note au lecteur : La discussion de *Verdugo* dans cette note de bas de page est l'un des

cela est abordé ci-dessous, le pouvoir judiciaire joue un rôle clé dans le contrôle de la surveillance menée aux États-Unis et lui impose le respect de normes constitutionnelles.

B. Garanties statutaires sur la surveillance du renseignement étranger

[21] En plus de contrôles constitutionnels, des garanties majeures du système judiciaire américain sur le renseignement étranger sont codifiées dans un certain nombre de lois. Les branches du pouvoir élues démocratiquement aux États-Unis ont autorisé la surveillance afin de protéger la sécurité nationale. Elles ont également réagi devant des preuves de surveillance excessive en établissant des lois limitant les pouvoirs de surveillance.[20]

[22] Plus particulièrement, en 1978, le Congrès des États-Unis a adopté le Foreign Intelligence Surveillance Act (FISA).[21] Les premiers changements majeurs apportés au FISA ont eu lieu dans le USA PATRIOT Act, à la suite des attentats du 11 septembre 2001. Comme beaucoup d'autres, j'ai avancé que ces changements étaient trop étendus.[22] De nombreuses réformes pro-vie privée ont été mises en place depuis 2001. Par exemple, à la suite des divulgations de Snowden, le Congrès a renforcé, dans le USA Freedom Act (loi sur la liberté) de 2015, des aspects importants du FISA, tout en mettant un terme à la collecte en masse autorisée par l'article 215 du PATRIOT Act.[23]

[23] En vertu du FISA et de la législation de la Cour suprême, les juges conservent leur pouvoir de contrôle sur toutes les surveillances électroniques effectuées à l'intérieur des États-Unis. Une perquisition est soit (a) menée dans un contexte criminel, auquel cas le juge doit approuver un mandat indiquant une cause probable de crime ; ou (b) menée dans le contexte du renseignement étranger, auquel cas la Cour de Surveillance du Renseignement Étranger doit autoriser la surveillance en vertu du FISA et sous réserve des exigences raisonnables du Quatrième amendement. Ce sont les principaux moyens utilisés pour effectuer légalement une recherche dans les communications électroniques aux États-Unis.[24]

---

deux endroits précis où Swire a complété ou modifié le témoignage original sur la base de l'examen du témoignage des autres experts dans cette affaire. L'autre endroit est la note de bas de paragraphe 72 du présent chapitre.]

[20] Le chapitre 3, article II retrace les événements historiques ayant conduit à des lois importantes en vigueur aujourd'hui, y compris le mouvement des droits civils, les enquêtes menées à la suite de l'affaire du Watergate, les attaques du 11 septembre 2001, et les révélations de Snowden.

[21] *Voir* 50 U.S.C. § 1801 *et seq.*, les discussions plus détaillées au chapitre 3.

[22] *Voir* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. 107-56 (2001). J'aborde le PATRIOT Act dans le chapitre 3, sections II(paragraphe C) et III(paragraphe B), ainsi qu'un ensemble de dix réformes dans l'annexe du chapitre 2.

[23] *Voir* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. No. 114-23 (2015). Les réformes introduites par le USA FREEDOM Act sont décrites tout au long des chapitres 3 et 5.

[24] Certains accès du gouvernement à des informations n'atteignent pas le niveau de « recherche » en vertu du Quatrième amendement. Par exemple, en vertu de ce qu'on appelle la « doctrine de troisième partie », l'accès par le gouvernement à des métadonnées téléphoniques détenues par un « tiers » (la société de téléphone) est autorisé constitutionnellement sans mandat approuvé par le juge. *Smith v. Maryland*, 442 U.S. 735 (1979). En réponse, le Congrès a créé, dans la Loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act ou ECPA) de 1986, des protections statutaires concernant les métadonnées téléphoniques, lesquelles exigent un ordre judiciaire par la loi plutôt qu'une exigence par la Constitution. L'ECPA est abordée dans le chapitre 4.

[24] Cette section traite de trois garanties légales systémiques que les États-Unis ont mises en place concernant le renseignement étranger : (1) la Cour de Surveillance du Renseignement Étranger ; (2) la collecte de métadonnées en vertu de l'article 215 ; et (3) la collecte des communications en vertu de l'article 702.

1. La Cour de Surveillance du Renseignement Étranger

[25] Depuis l'adoption du FISA, la Cour de Surveillance du Renseignement Étranger (Foreign Intelligence Surveillance Court, FISC) a joué un rôle central dans la régulation du renseignement étranger aux États-Unis. Le FISA accorde au FISC la compétence exclusive pour émettre des ordonnances pour toutes les surveillances étrangères/de renseignement effectuées aux États-Unis.[25] Cela comprend notamment des ordonnances pour la surveillance individuelle, ainsi que pour le contrôle de programmes de renseignement à plus grande échelle.

[26] Au sein du FISC, des juges indépendants et de haute qualité nommés à vie à la magistrature fédérale disposent d'un accès à des informations top-secrètes, et exercent une autorité constitutionnelle dans l'application des limites légales sur les activités de renseignement.[26] Les juges du FISC sont sélectionnés par le juge en chef de la Cour suprême des États-Unis, et appuyés par un ensemble de procureurs jouissant d'une habilitation de sécurité et d'une expertise juridique en matière de sécurité nationale.[27]

[27] Récemment, le FISC et l'administration Obama ont déclassifié de nombreux actes de procédure, ordonnances et document connexes du FISC. Afin de déterminer comment le FISC a mis en pratique les garanties identifiées dans le présent témoignage, je consacre le chapitre 5 à un examen détaillé des documents déclassifiés. Selon moi, les documents viennent étayer les conclusions suivantes :

> *Le FISC offre aujourd'hui un contrôle indépendant et efficace de la surveillance menée par l'administration américaine, soutenu par des procédures d'examen approfondies et une autorité judiciaire constitutionnelle*.[28] Les procédures standard du FISC soumettent les applications de surveillance du gouvernement à un examen attentif, et les décisions du FISC montrent que le tribunal exige que le gouvernement se soumette à des séries d'informations, de réunion, de questions, ainsi qu'à des auditions. Dans ses évaluations de surveillance proposée, le FISC se concentre sur la conformité du gouvernement avec les ordonnances existantes ou similaires du FISC. Au cours des dernières années, le nombre d'applications de surveillance que le FISC a modifiées ou rejetées a considérablement augmenté, et le FISC a exercé son pouvoir constitutionnel de faire cesser des surveillances qu'il juge illégales.

---

[25] *Voir* 50 U.S.C. § 1804(a).

[26] Les juges fédéraux sont nommés à la Court de Surveillance du Renseignement Étranger pour un mandat de sept ans. Pour une discussion approfondie de la structure institutionnelle du FISC et de ses ressources dans la surveillance du renseignement étranger aux États-Unis, *voir* Chapter 3, Section III(A)(1).

[27] *Voir id.*

[28] Les documents à la base de cette conclusion sont discutés en détail dans le chapitre 5, article I.

Le FISC surveille la conformité avec ses ordonnances, et a sanctionné sévèrement les cas de non-conformité.[29] La juridiction du FISC s'étend au contrôle et à l'application de ses ordonnances. Un système de règles de déclaration, de vérifications par des tiers des agences de surveillance, et des rapports périodiques fournit au FISC des notifications concernant les incidents de conformité. Lorsque le FISC a rencontré des cas de non-conformité, il a imposé des sanctions importantes, parfois en refusant l'accès aux données de renseignement à la NSA et en menaçant de mettre fin à l'ensemble des programmes de surveillance à moins que des changements ne soient mis en œuvre.

Au cours des dernières années, le FISC a ainsi, sur sa propre initiative, considérablement accru la transparence tout en mettant en place de nouvelles lois.[30] Les procédures du FISC sont secrètes et les décisions du FISC ont habituellement été classées. Cependant, au cours des dernières années, le FISC a lui-même commencé à publier un plus grand nombre d'opinions et de procédures personnelles, et le USA FREEDOM Act exige désormais que les décisions importantes du FISC soient publiées. En outre, les litiges réglés par le FISC ont entraîné des droits en matière de transparence des rapports d'entreprise que le USA FREEDOM Act a par la suite codifiés et élargis.

Le FISC reçoit aujourd'hui et continuera de bénéficier d'informations contradictoires provenant de parties non-gouvernementales dans des affaires importantes.[31] Au cours de la période post-2001, le rôle du FISC s'est étendu de l'approbation de chacune des ordonnances d'écoute téléphonique au contrôle de l'intégralité des programmes de renseignement étranger, et il a été de plus en plus reconnu que le FISC pourrait bénéficier de présentations contradictoires sur des questions complexes. Dans certains cas, le FISC a commencé à recevoir de telles informations sur sa propre initiative, à la fois de la part d'experts de la vie privée et de fournisseurs de services de communication. Aujourd'hui, le USA FREEDOM Act a créé un panel de six experts de la vie privée qui aura accès à des informations classifiées et participera à d'importants travaux du FISC via des briefings et des plaidoiries orales.

2. Collecte de métadonnées en vertu de l'article 215

[28] Il est possible que le changement le plus spectaculaire opéré dans les lois sur la surveillance américaine depuis 2013 concerne les réformes de l'article 215 du USA PATRIOT Act, lequel a fourni au gouvernement des pouvoirs étendus dans l'obtention de « documents et d'autres choses tangibles. »[32] Après les attentats du 11 septembre, l'article 215 a été utilisé comme base pour la collecte de métadonnées sur un grand nombre d'appels téléphoniques effectués aux États-Unis.[33]

---

[29] *Voir id.*, Section II.
[30] *Voir id.*, Section III.
[31] *Voir id.*, Section IV.
[32] *Voir* USA PATRIOT Act § 215 Les préoccupations et les réformes concernant l'article 215 du PATRIOT Act sont discutées en détail dans le chapitre 3, article III, paragraphe B.
[33] Le chapitre 3, article III, paragraphe B traite de la collecte de métadonnées post-11 septembre en vertu de l'article 215.

[29] Le USA FREEDOM Act abolit la collecte en masse en vertu de l'article 215 et de deux autres pouvoirs. Ces limites sur la collecte s'appliquent à la fois aux personnes américaines et non américaines. Une autorité beaucoup plus restreinte existe désormais, basée sur des sélecteurs personnalisés associés au terrorisme et à l'examen judiciaire de chaque sélecteur proposé.[34]

3. Collecte de communications en vertu de l'article 702

[30] L'article 702 du FISA s'applique aux collectes qui ont lieu à l'intérieur des États-Unis, et autorise uniquement l'accès aux communications de personnes ciblées, à des fins de renseignement étranger précis.[35] Après avoir reçu des informations classées sur l'article 702, le Conseil de surveillance de la vie privée et des libertés civiles indépendant est parvenu à la conclusion suivante :

> Dans l'ensemble, le Conseil a constaté que les informations collectées dans le cadre du programme ont été précieuses et efficaces dans la protection de la sécurité nationale et dans la production de renseignements étrangers utiles. Le programme a fonctionné en vertu d'une loi qui a été l'objet d'un débat public, et le texte de la loi décrit la structure de base du programme. Le fonctionnement de l'article 702 du programme a fait l'objet d'un contrôle judiciaire et d'une surveillance interne importante, et le Conseil n'a trouvé aucune preuve d'abus intentionnel.[36]

[31] Le chapitre 3 sur les garanties systémiques pour le renseignement étranger et le chapitre 5 concernant le FISC fournissent des détails sur les programmes PRISM et Upstream mis en place en vertu de l'article 702. Le malentendu concernant le programme PRISM remonte à l'histoire originale et désormais révisée du Washington Post, lequel a déclaré que « [l]'Agence nationale de sécurité (National Security Agency) et le FBI se servent *directement* sur les serveurs de neuf grandes sociétés Internet américaines » pour extraire toute une gamme d'informations.[37] Cette déclaration était inexacte. Dans la pratique, le PRISM fonctionne au titre d'une directive judiciairement approuvée et supervisée, en vertu de laquelle le gouvernement envoie une demande à un fournisseur de services basé aux États-Unis pour la collecte de sélecteurs « ciblés », telle qu'une adresse électronique.

---

[34] Ces réformes sont codifiées dans le chapitre 50 du Code des États-Unis, paragraphe 1861 et sont expliquées plus en détail dans le chapitre 3, article III, paragraphe B).

[35] L'article 702 est codifié dans l'article 50 du Code des États-Unis, paragraphe 1881a. Une discussion détaillée de l'historique, de la structure et des opérations de l'article 702 est contenue dans le chapitre 3, article III, paragraphe B).

[36] PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 2 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

[37] *Voir* Barton Gellman, *U.S. intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (Jun. 6, 2013) (soulignement ajouté), https://www.engadget.com/2013/06/06/washington-post-nsa-fbi-tapping-directly-into-servers-of-9-lea/. L'histoire a été révisée afin d'expliquer qu'un document qui avait fuité indiquait l'existence d'un accès direct ; en fait, comme expliqué dans le chapitre 3, article III, paragraphe C(2), le document était trompeur ou inexact ; l'article 702 n'autorise pas un accès direct.

[32] Il y a également eu des préoccupations au sujet d'Upstream en tant que programme de collecte de masse.[38] En réalité, l'administration américaine reçoit des communications à la fois en vertu des programmes Upstream et PRISM sur la base de sélecteurs ciblés, avec des actions effectuées en vertu de chaque programme et qui sont soumises à l'examen du FISC. Concernant l'échelle, un avis déclassifié du FISC a constaté que plus de 90 % des communications Internet obtenues par la NSA en 2011 en vertu de l'article 702 provenaient en fait du programme PRISM, avec moins de 10 % provenant du programme Upstream.[39] La communauté du renseignement américain publie désormais un Rapport annuel de transparence statistique,[40] dont les statistiques sont soumises au contrôle du Congrès, des inspecteurs généraux, du FISC, du Conseil de surveillance de la vie privée et des libertés civiles, et d'autres.[41] En 2015, il y a eu 94 368 « cibles » en vertu des programmes de l'article 702, chacune ayant été ciblée suite à la constatation d'une raison de renseignement étranger.[42] Il s'agit d'une toute petite fraction d'utilisateurs Internet américains, européens ou mondiaux. Au lieu d'une surveillance de masse ou incontrôlée, les statistiques documentés montrent la faible probabilité des communications acquises sur des citoyens ordinaires.[43]

[33] J'ai affirmé précédemment qu'à mon avis, l'article 702 constitue une réponse raisonnable à l'évolution de la technologie, énoncée dans une loi qui a été débattue en public avant son adoption.[44] Les documents désormais déclassifiés du FISC, ainsi que des rapports sur l'article 702 du Conseil de surveillance de la vie privée et des libertés civiles et du Groupe d'étude, montrent un ensemble de mesures beaucoup plus ciblées et limitées légalement en vertu de l'article 702 que la presse ne l'avait suggéré dans un premier temps.[45]

C. Contrôle des activités de surveillance

---

[38] Le chapitre 3, article III, paragraphe C(3) contient une description plus détaillée de la collecte par Upstream.
[39] *Voir [Caption Redacted]*, No. [Redacted], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011), at 30, 33-34, https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[40] Les rapports de transparence ont été publiés chaque année depuis 2013 : OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013*, IC ON THE RECORD (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.
[41] Pour obtenir une liste des différentes entités de contrôle, *voir* REVIEW GROUP REPORT, *supra* note 10, Appendix C at 269.
[42] Les rapports statistiques définissent le terme de « cible » en détail et mon évaluation est que le nombre de personnes visées est inférieur au nombre indiqué.
[43] Le rapport de transparence statistique 2016 réaffirme la nature ciblée de la surveillance : « L'article 702 autorise uniquement le ciblage des personnes non-américaines dont on pense raisonnablement qu'elles sont situées en dehors des États-Unis en vue d'obtenir des informations de renseignement étranger. » *Voir, e.g.*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD at "Response to PCLOB Recommendation 9(5)" (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.
[44] *Voir* Swire, *US Surveillance Law*, *supra* note 5.
[45] *Voir* Chapter 3, Section III(C)(1).

[34] En plus de la codification des garanties systémiques, les États-Unis ont créé plusieurs mécanismes d'examen et de contrôle liés au renseignement étranger. À la suite des divulgations de Snowden, j'ai fait partie des cinq membres du Groupe d'étude sur les technologies de renseignement et de communication que le président Obama a créé afin de mener un examen complet des programmes de surveillance américains. Nous avons reçu des informations top-secrètes et remis au Président notre rapport de plus de 300 pages en décembre 2013.[46] En janvier 2014, l'administration Obama nous a informés que 70 pour cent de nos 46 recommandations avaient été adoptées dans la lettre ou dans l'esprit, et d'autres avaient été adoptées depuis.

[35] À l'avenir, plusieurs institutions ayant chacune accès à des informations classifiées exerceront des responsabilités de contrôle sur les activités de renseignement étranger :[47]

1. *Inspecteurs généraux de l'agence exécutive (Inspectors General, IG)*. Par la loi, les bureaux des IG sont établis au sein d'agences américaines afin de surveiller de manière indépendante la légalité des activités de l'agence, et de recevoir des rapports sur des activités illégales d'employés du gouvernement.[48] Toutes les agences de renseignement, y compris la NSA, disposent d'un bureau des IG.

2. *Comités de surveillance du Congrès*. Tant le Sénat que la Chambre des représentants disposent de comités de surveillance du renseignement, lesquels ont un pouvoir d'assignation ainsi qu'un accès à des informations classifiées.[49] Les lois concernant les lanceurs d'alerte prévoient que les employés et les prestataires du gouvernement puissent signaler directement aux deux comités des problèmes sérieux liés à la surveillance.[50]

3. *Conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, « PCLOB »)*. Le PCLOB est un organisme indépendant sur la vie privée disposant d'importants pouvoirs d'enquête sur des activités classifiées de renseignement étranger.[51] Les rapports publiés par le PCLOB ont donné lieu à des changements importants dans les pratiques de surveillance américaines.[52]

---

[46] REVIEW GROUP REPORT, *supra* note 10, at 179.
[47] Pour une discussion plus approfondie sur chaque organisme de contrôle, voir Chapter 3, Section IV.
[48] *Voir en général* Inspector General Act of 1978, codified at 5 U.S.C. App. 1 §§ 1-13.
[49] *Voir en général U.S. Senate Select Committee on Intelligence*, Senate.gov, http://www.intelligence.senate.gov/. Pour une discussion plus détaillée des comités de surveillance du Congrès, *voir* Chapter 3, Section IV(B).
[50] *Voir* Intelligence Community Whistleblower Protection Act of 1998, 50 U.S.C. § 403q. chapitre 3, article IV, paragraphe B qui aborde les procédures de signalement des violations des comités du Congrès.
[51] *Voir* 42 U.S.C. § 2000ee. Les objectifs, la structure et les pouvoirs du PCLOB sont discutés en détail dans le chapitre 3, article IV, paragraphe C.
[52] À ce jour, le PCLOB a publié deux rapports sur la collecte visée par article 215 et les programmes visés par l'article 702. Les deux rapports, y compris les modifications apportées à la suite des recommandations du PCLOB, sont discutés dans le chapitre 3, article IV, paragraphe C.

4. *Bureaux sur la vie privée dans les agences exécutives.* Le Président Obama a récemment publié un décret stipulant la fondation du Conseil fédéral sur la vie privée, lequel est responsable de la mise en œuvre de la politique relative à la vie privée dans toutes les agences gouvernementales américaines.[53] Les agences de renseignement américaines disposent désormais des bureaux internes consacrés à la vie privée et aux libertés civiles.[54] Le Bureau national de la sécurité chargé du renseignement du Ministère de la Justice a établi une section de surveillance.[55] Un vaste système de surveillance permet également de signaler les incidents de conformité avec la Cour de Surveillance du Renseignement Étranger.[56]

D. Garanties de transparence

[36] Le système juridique américain en matière de renseignement étranger a depuis longtemps dû répondre à des obligations de transparence, telles que des rapports statistiques sur le nombre d'ordonnances judiciaires émises. Depuis 2013, de nombreux changements ont eu lieu dans le sens de la transparence, tout en reconnaissant l'atteinte à la sécurité nationale pouvant découler de la divulgation d'informations classifiées, telles que sur les sources et méthodes des activités de renseignement. Les garanties de transparence viennent compléter le contrôle exercé par le FISC et les autres mécanismes de contrôle que nous venons d'aborder. La transparence est appropriée lorsqu'elle est compatible avec la sécurité nationale, et un contrôle supplémentaire est effectué par les juges et d'autres personnes habilitées top-secret lorsque la transparence n'est pas appropriée.

[37] Comme cela est abordé plus en détail dans les chapitres suivants,[57] les garanties de transparence aux États-Unis comprennent :

1. *Rapports sur les interprétations juridiques.* Le USA FREEDOM Act inclut une nouvelle règle concernant les risques d'une loi secrète. Lorsque le FISC émet une décision contenant « une construction ou interprétation importante de toute disposition de la loi », le USA FREEDOM Act exige désormais que le gouvernement des États-Unis rende publique la décision du FISC dans toute la mesure du possible.[58]

---

[53] *Voir* Exec. Order No. 13719, Establishment of the Federal Privacy Council, 81 Fed. Reg. 29, 7685-89 (Feb. 9, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-12/html/2016-03141.htm.
[54] Le chapitre 3, article IV, paragraphe D traite des bureaux de la vie privée au sein de la communauté du renseignement des États-Unis, tel que le Bureau des libertés civiles et de la vie privée de la NSA.
[55] DEP'T OF JUSTICE, *Office of Intelligence* (July 23, 2014), https://www.justice.gov/nsd/office-intelligence.
[56] Chapter 5, Section II(A).
[57] Chapter 3, Section IV and Chapter 5, Section III.
[58] 50 U.S.C. § 1872(b), https://casetext.com/statute/50-usc-1872-declassification-of-significant-decisions-orders-and-opinions. Si l'opinion ne peut pas être déclassifiée pour des raisons de sécurité nationale, le gouvernement devra malgré tout publier un résumé non classifié.

2. *Rapports de transparence du gouvernement.* Les USA FREEDOM Act donnaient beaucoup plus de détails qu'auparavant sur les demandes du gouvernement en informations de renseignement étranger, y compris le Rapport annuel de transparence statistique aux États-Unis.[59]

3. *Rapports de transparence des entreprises.* Le USA FREEDOM Act a codifié et étendu la capacité des entreprises à la fourniture d'informations granulaires dans leurs rapports concernant la transparence des ordres auxquels elles ont répondu.[60] Par exemple, les entreprises peuvent désormais déclarer la portée des ordonnances du FISA pour le contenu et le non contenu (par ex. 0-1 000 ; 1 001-2 000), ainsi que le nombre de sélecteurs de client ciblés dans le cadre de l'ordre. Pertinents dans le cadre des plaintes pour surveillance de masse et aveugle, ces rapports montrent la très petite fraction d'utilisateurs ayant été concernés par l'article 702 et d'autres demandes effectuées auprès d'entreprises.[61]

4. *Mesures supplémentaires du gouvernement en matière de transparence.* Au-delà des exigences légales, le gouvernement des États-Unis a depuis 2013 pris plusieurs mesures en matière de transparence, notamment : la déclassification de nombreuses décisions du FISC ;[62] un nouveau site web consacré à l'accès du public à des informations de la communauté du renseignement ;[63] les premiers « Principes de transparence du renseignement pour la communauté du renseignement » ;[64] et la publication des politiques des agences de

[59] Les rapports de transparence ont été publiés chaque année depuis 2013 : OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014*, IC ON THE RECORD (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013*, IC ON THE RECORD (Jun. 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

[60] Chapter 3, Section V(E).

[61] Le chapitre 3, article V, paragraphe E examine les rapports de transparence Facebook et Google les plus récents, et conclut que, tout au plus, environ 0,001 % des utilisateurs de Google sont potentiellement affectés par des demandes d'informations des États-Unis.

[62] *Voir* U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, *Public Filings*, http://www.fisc.uscourts.gov/public-filings; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Declassified: Release of FISC Question of Law and FISCR Opinion*, IC ON THE RECORD (Aug. 22, 2016), https://icontherecord.tumblr.com/tagged/declassified.

[63] *Voir* IC ON THE RECORD, https://icontherecord.tumblr.com/.

[64] *Voir* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY (2015), https://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

renseignement en vertu des autorités de renseignement, y compris l'Ordre exécutif 12 333.[65]

E. Garanties de l'exécutif

[38] Depuis 2013, l'exécutif américain a mis en place plusieurs garanties permettant de compléter les garanties législatives décrites ci-dessus. Mon expérience au sein du Groupe d'étude et en général me permet de conclure, comme cela est détaillé dans l'article VI, paragraphe A du chapitre 3, que ces garanties de l'exécutif présentent une grande importance dans la pratique.

[39] Au premier rang des nouvelles garanties de la banche de l'exécutif figure la Directive de politique présidentielle 28 (Presidential Policy Directive 28, PPD-28), laquelle exige que les agences de surveillance américaines fassent en sorte que la vie privée soit intégrée dans la planification des transmissions de renseignements.[66] La PPD-28 exige que les agences privilégient des sources alternatives de renseignements, telles que des sources diplomatiques, par rapport au renseignement sur les transmissions.[67] Lorsque la surveillance est utilisée, elle doit être « aussi individualisée que possible », en procédant via des sélecteurs tels que les adresses de courriel chaque fois que cela est possible.[68] La collecte en masse ne peut pas être utilisée, sauf pour détecter et contrer des menaces sérieuses, comme dans le cadre du terrorisme, de l'espionnage ou de la prolifération nucléaire.[69] Les données concernant des citoyens de l'UE ne peuvent pas être diffusées, à moins que cela puisse être fait avec des données comparables sur des personnes américaines.[70] Bien que la PPD-28 n'utilise pas des termes utilisés dans la législation européenne tels que « nécessaire » et « proportionné », le fait de privilégier des solutions alternatives à la surveillance, l'exigence d'une collecte individualisée et les limites d'utilisation constituent des exemples de la mise en œuvre de garanties spécifiques pour répondre à ces préoccupations.

[40] En outre, les récents accords entre l'UE et les États-Unis contraignent la branche de l'exécutif des États-Unis à protéger les données à caractère personnel des citoyens de l'UE. L'Umbrella Act UE-États-Unis protège les données à caractère personnel transférées vers des agences américaines à des fins d'application de la loi, restreignant ainsi les transferts et les utilisations autorisées, tout en fournissant aux ressortissants de l'UE des droits d'accès et de

---

[65] *Voir* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *IC on the Record Statement Accompanying Posting of EO 12333 Table of Guidelines*, IC ON THE RECORD (July 20, 2016), https://icontherecord.tumblr.com/post/147708188298/ic-on-the-record-statement-accompanying-posting-of.

[66] Le chapitre 3, article VI, paragraphe B contient une discussion détaillée de six garanties importantes figurant dans la PPD-28. *Voir Presidential Policy Directive 28, Signals Intelligence Activities* (PPD-28) (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[67] *Voir* PPD-28, § 1(d).

[68] *Voir id.*

[69] *Voir id.* § 2.

[70] *Voir id.* § 4(a)(i).

correction.[71] La Privacy Shield contient des engagements du gouvernement des États-Unis à agir rapidement et efficacement pour répondre aux préoccupations de protection des données de l'UE, et soumet les performances du Privacy Shield à un processus d'examen annuel.[72] Ces engagements et examens fournissent à l'Union européenne et à ses autorités un mécanisme continu de protection des données à caractère personnel transférées vers les États-Unis, y compris les données traitées à des fins de sécurité nationale.

II. Garanties systémiques dans l'application de la loi

[41] En plus du renseignement étranger, les États-Unis ont établi un système de garanties protégeant les individus dans le cadre d'enquêtes criminelles. Tel que mentionné ci-dessus, la collecte par le gouvernement de communications électroniques aux États-Unis est effectuée soit en vertu de l'application de la loi, soit en vertu d'autorités légales de renseignement étranger. Pour les collectes aux États-Unis, toute autre autorité telle que l'Ordre exécutif 12 333 ne s'applique pas.[73] Cette partie de mon témoignage décrit les garanties systémiques en place pour la collecte aux États-Unis de communications électroniques dans le cadre d'enquêtes criminelles.

[42] En réaction à l'expérience coloniale américaine avec les monarques anglais, la Constitution des États-Unis énonce plusieurs droits fondamentaux permettant de contrôler les intrusions du gouvernement dans les affaires criminelles.[74] Aux États-Unis, ces droits ont donné lieu à des garanties de procédure pénale plus strictes dans de multiples domaines que dans d'autres pays, y compris dans de nombreux pays de l'UE :

1. *Contrôle judiciaire strict*.[75] Des huissiers de justice indépendants supervisent les demandes de mandats visant à effectuer des recherches et à recueillir des preuves. La « cause probable », qui constitue une exigence pour la délivrance

[71] *Voir* L'accord entre l'Union européenne et les États-Unis d'Amérique sur la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de la prévention, de la recherche, de la détection ou de la poursuite des infractions pénales (version de paraphe), UE-EU, 2 juin 2016, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf [ci-après désigné « Umbrella Agreement »].
[72] *Voir The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.
[73] Pour être explicite, mon hypothèse en écrivant ce témoignage était que la Cour examine le caractère adéquat de la protection des données transférées vers les États-Unis, et non pas des données qui restent dans l'UE. Sur la base de cette hypothèse, je concentre mon analyse sur les règles juridiques s'appliquant aux transferts de données. En revanche, l'Ordre exécutif 12 333 s'applique aux données collectées à l'extérieur des États-Unis. [Il existe une exception d'« autorité de transit » à l'application de l'Ordre exécutif 12 333. Si je comprends bien, l'autorité de transit s'appliquerait, par exemple, à un courriel provenant de l'étranger, à travers le réseau de télécommunications à l'intérieur des États-Unis sans avoir de destination aux États-Unis, et qui s'est ensuite rendu vers une destination étrangère. Pour obtenir une discussion de l'autorité de transit, voir https://www.lawfareblog.com/understanding-deeper-history-fisa-and-702-charlie-savages-power-wars-fiber-optic-cables-and- transit.] [Note au lecteur : La discussion de l'autorité de transit dans cette note de bas de page est l'un des deux endroits précis où Swire a complété ou modifié le témoignage original sur la base de l'examen du témoignage des autres experts dans cette affaire. L'autre endroit est la note de bas de page 18 du présent chapitre.]
[74] Le chapitre 4, article I traite des différents droits énoncés dans la Déclaration des droits de la Constitution américaine en réponse à l'expérience coloniale avec l'Angleterre.
[75] Le chapitre 4, article II, paragraphes A, B et E fournit une discussion détaillée de la surveillance judiciaire et de la cause probable.

d'un mandat de perquisition, est une exigence relativement stricte concernant les recherches numériques.[76]

2. *Contrôle plus strict pour les interceptions*. Les écoutes téléphoniques et autres interceptions en temps réel font même l'objet d'exigences plus strictes, telles que des cycles successifs d'examen par l'agence, la réduction au minimum des garanties pour les non-cibles et des exigences pour épuiser d'autres sources d'information.[77]

3. *Sanctions en cas de perquisitions illégales*. La « règle d'exclusion » empêche les preuves obtenues au moyen d'une fouille illégale d'être utilisées au cours de procès criminels,[78] tandis que la doctrine du « fruit de l'arbre empoisonné » annule les autres preuves découlant de la perquisition illégale.[79] Les officiers qui mènent des perquisitions illégales sont passibles de poursuites en dommages et intérêts.[80]

4. *Les ordres permettant des contestations judiciaires*. La législation américaine exige que les ordonnances de tribunal indiquent clairement la base juridique d'un mandat ou d'une demande d'information, ce qui permet au destinataire de déterminer s'il existe un fondement pour contester l'ordonnance.[81]

5. *Aucune conservation de données obligatoire*. La législation américaine n'exige aucune conservation de données concernant des communications sur Internet, telles que des courriels.[82] Pour les communications téléphoniques, la législation américaine exige une conservation limitée des enregistrements nécessaires permettant de résoudre des litiges en matière de facturation.[83]

6. *Cryptage renforcé*. Les États-Unis autorisent l'utilisation d'un cryptage renforcé, une technologie de préservation de la vie privée qui a été largement adoptée par les entreprises basées aux États-Unis.[84]

[43] Dans une large mesure, la création même des États-Unis dérive d'une insistance sur la protection des droits des personnes dans le système de justice pénale. Bien qu'il soit compliqué d'évaluer précisément dans quels domaines les États-Unis et l'UE fournissent des garanties plus

---

[76] *Voir, e.g., United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), https://scholar.google.com/scholar_case?case=11707608375476732 55&hl=en&as_sdt=6&as_vis=1&oi=scholarr.
[77] *Voir* 18 U.S.C. § 2518, discussed in Chapter 4, Section II(C).
[78] *Voir Mapp v. Ohio*, 367 U.S. 643 (1961). La règle d'exclusion et d'autres sanctions pour des perquisitions illégales sont discutées dans le chapitre 4, article II, paragraphe D.
[79] *Voir Wong Sun v. U.S.*, 371 U.S. 471 (1963).
[80] *Voir* 42 U.S.C. §1983; *Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971).
[81] *Voir* 18 U.S.C. § 2703(b).
[82] Pour une comparaison plus approfondie entre les pratiques de conservation des données dans l'UE et les règles de conservation limitée des données aux États-Unis, *voir* le chapitre 4, article II, paragraphe G.
[83] *Voir* 47 C.F.R. § 42.6.
[84] *Voir* Chapter 4, Section II(H); *voir également* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416 (2012).

strictes en matière d'enquêtes criminelles, les États-Unis disposent d'importantes garanties, souvent constitutionnelles, qui font souvent défaut au sein de l'UE. À mon avis, une comparaison équitable de l'adéquation des deux systèmes devrait examiner soigneusement ces facteurs supplémentaires.

III. Conclusion sur les garanties systémiques

[44] Les agences de renseignement agissent souvent en secret afin de détecter les efforts de renseignement d'autres pays et pour des raisons de sécurité nationale. Les États-Unis ont développé de multiples façons d'assurer la surveillance par des personnes ayant accès à des informations classifiées dans le cadre d'activités secrètes indispensables, et de créer de la transparence de manière à ne pas compromettre la sécurité nationale. À mon avis, le système américain propose des contrôles efficaces contre les abus de pouvoirs de surveillance secrète. Je suis d'accord avec l'équipe dirigée par Ian Brown, professeur à Oxford, lequel, après avoir comparé les garanties américaines avec d'autres pays, a conclu que « les États-Unis constituent désormais une référence dans les normes concernant le renseignement étranger » et que le cadre juridique de la collecte de renseignements étrangers aux États-Unis contient des règles beaucoup plus claires concernant l'autorisation et les limites en matière de collecte, d'utilisation, de partage et de surveillance des données relatives aux ressortissants étrangers que les législations équivalentes de presque tous les États membres de l'UE.[85] En outre, comme le montre l'étude détaillée de la Cour de Surveillance du Renseignement Étranger (Foreign Intelligence Surveillance Court), ces normes juridiques rigoureuses sont mises en œuvre de manière efficace dans la pratique, sous la supervision de juges indépendants bénéficiant d'un accès à des informations top-secrètes.

PARTIE 3 : Recours individuels dans la législation américaine en matière de vie privée

[45] Aux États-Unis, un ressortissant de l'UE ou d'autres personnes disposent de multiples recours disponibles en cas de violation de la vie privée. Ces recours individuels fonctionnent en tandem avec les garanties systémiques que nous venons d'aborder. Pour la plupart des problèmes impliquant la surveillance secrète par des agences, j'estime que les garanties systémiques sont souvent très efficaces. Aux États-Unis, les organes de contrôle tels que le FISC, les inspecteurs de l'agence, le PCLOB, les inspecteurs généraux de l'agence, le Sénat et les comités du renseignement intérieur, et le Groupe d'étude du Président dont j'ai fait partie ont accès à des informations classifiées. Cet accès permet à ces contrôleurs de détecter des problèmes de vie privé et de prendre des mesures pour les corriger. Par contraste, certaines raisons exigent la prudence concernant la divulgation de secrets de sécurité nationale à des individus ou dans le cadre d'audience publique, lorsque l'acte de divulgation lui-même peut présenter de nouveaux risques de sécurité.

[46] Le système américain renforce ces garanties systémiques avec une approche concertée des recours individuels. J'ai parfois entendu dans l'UE et ailleurs que les États-Unis manquaient généralement de recours en cas de violation de la vie privée, ou que les recours ne sont

[85] Brown et al., *supra* note 1, at 3.

disponibles qu'aux ressortissants des États-Unis. Ce n'est pas exact. En tant qu'auteur principal du manuel utilisé pour l'examen juridique sur la vie privée dans le secteur privé de l'Association internationale des professionnels de la vie privée (IAPP), j'ai écrit une présentation des lois de protection de la vie privée aux États-Unis qui s'appliquent au secteur privé, y compris les mécanismes de mise en application, laquelle présentation comprend à elle seule près de 200 pages et 11 chapitres. [86] L'annexe 1 du chapitre 7 de mon témoignage fournit un organigramme de cette combinaison de garanties systémiques et de recours individuels afin de donner un aperçu global du régime juridique en matière de vie privée aux États-Unis. Il vient compléter les explications détaillées fournies concernant chaque aspect de ce régime dans les chapitres 3, 4 et 7.

[47] La grande quantité des lois sur la vie privée aux États-Unis conduit parfois à une autre critique de l'UE arguant que les recours aux États-Unis sont « fragmentés » et peuvent, pour cette raison, ne pas être adéquats selon les normes de l'UE. J'espère que cette explication des recours américains en matière de vie privée pourra démontrer comment s'articulent les différents rouages de la législation des États-Unis. La complexité de la législation des États-Unis découle en partie de sa culture juridique pro-application, avec pour résultat que plusieurs agents chargés de la protection de la vie privée peuvent chacun avoir la capacité juridique d'intenter une action. Cette division de l'autorité peut s'avérer bénéfique pour la protection de la vie privée, dans la mesure où elle permet aux experts en la matière de mettre en application dans leurs domaines d'expertise, permet à différentes agences de mobiliser leurs ressources pour contrôler les catégories d'activités au nom des personnes concernées, et octroie également aux personnes des droits privés d'action.

[48] Pour expliquer le système d'application de protection de la vie privée aux États-Unis, je donne un aperçu des voies qu'une personne lésée aux États-Unis ou dans l'Union européenne peut choisir pour réagir à des préoccupations concernant des violations de la vie privée, comme cela est expliqué plus en détail au chapitre 7 : Recours individuels dans la législation américaine en matière de vie privée Premièrement, j'aborde des recours judiciaires individuels contre le gouvernement des États-Unis, y compris les accords Privacy Shield (accord sur protection de la vie privée) et l'Umbrella Agreement (accord-cadre) récemment finalisés, ainsi que la loi Judicial Redress Act (loi sur le recours juridictionnel) récemment adoptée. Ensuite, j'examine les recours civils et criminels disponibles lorsque des personnes, y compris des employés du gouvernement, violent des règles en matière d'écoute téléphonique et d'autres règles de surveillance en vertu de lois telles que la Stored Communications Act (loi sur les communications enregistrées), la Wiretap Act (loi sur les écoutes téléphoniques) et la Foreign Intelligence Surveillance Act (loi sur la surveillance des renseignements étrangers). Après quoi, je mets en lumière trois voies de recours non-judiciaires que des personnes peuvent choisir : le PCLOB, les comités du Congrès, ainsi que le recours à la presse libre et des organisations non gouvernementales de défense de la vie privée aux États-Unis. Ensuite, je discute des recours individuels contre des sociétés

[86] PETER SWIRE & KENESA AHMAD, U.S. PRIVATE SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS, INT'L ASSOC. OF PRIV. PROF. (2012) https://iapp.org/media/pdf/certification/cippus-us-private-sector-ch3.pdf. La même année, nous avons publié un livre proposant une introduction à la vie privée à l'échelle internationale. PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES, INT'L ASSOC. OF PRIV. PROF. (2012).

américaines qui divulguent de manière inappropriée à l'administration américaine des informations concernant des clients. Ces causes d'action contre des sociétés américaines peuvent être portées à la fois par des individus (ressortissants américains ou non) et par des agences administratives fédérales des États-Unis. J'examine également les recours disponibles en vertu de la loi d'État aux États-Unis et des droits privés d'action, y compris leur application par des procureurs généraux d'État.

[49] Je fournis également dans cette partie une réponse à certaines des préoccupations soulevées dans l'affidavit du commissaire irlandais chargé de la protection dans cette affaire. Plus précisément, je réponds aux préoccupations de l'affidavit concernant les recours fragmentés dans la législation américaine, les restrictions possibles sur la disponibilité des recours et les préoccupations relatives à la doctrine de l'intérêt à agir en vertu de la législation américaine. Cette partie explique comment l'ensemble du système juridique américain répond à ces préoccupations, et comment des réformes spécifiques, tel que le mécanisme de médiation dans le cadre du Privacy Shield, ont une incidence sur ces préoccupations.

[50] La partie 3 conclut par une mise en garde : les recours individuels sont parfois difficiles à fournir dans le cadre du renseignement, en raison du risque de révélation d'informations classifiées à des acteurs hostiles. L'attrait des différentes voies de recours dans les systèmes de renseignement repose donc sur les avantages à fournir un recours individuel contre les risques inhérents à la divulgation d'informations classifiées. Pour utiliser la langue de l'article 8 de la Convention européenne des Droits de l'homme, l'attrait des différentes voies de recours individuel dans les systèmes de renseignement dépend de la manière dont l'application du droit est jugée avec la nécessité dans une société démocratique de protéger d'autres intérêts, notamment celui de la sécurité nationale et de la sûreté publique.

I. Recours individuels contre le Gouvernement des États-Unis

[51] Il existe des recours contre le gouvernement des États-Unis en cas de violations de la vie privée en vertu de lois civiles aussi bien que criminelles.

A. Recours judiciaires civils aux États-Unis

[52] Les personnes admissibles, y compris des ressortissants de l'UE, peuvent engager des poursuites civiles contre le gouvernement des États-Unis pour des violations du droit pouvant entraîner des dommages-intérêts pécuniaires et des injonctions contre des activités ou programmes gouvernementaux illégaux en cours. Les recours de ce genre existent en vertu des lois suivantes : le Judicial Redress Act ; le EU-US Privacy Shield ; l'Umbrella Agreement ; le Stored Communications Act (SCA) ; le Wiretap Act ; et le Foreign Intelligence Surveillance Act (FISA).

[53] Pris ensemble, le EU-US Privacy Shield, le Judicial Redress Act et l'Umbrella Agreement fournissent d'importantes voies de recours individuels aux ressortissants de l'UE qui

pensent avoir été victimes de préjudices dans le domaine de la vie privée.[87] Le EU-US Privacy Shield a créé de nouveaux recours contre le gouvernement des États-Unis mis à disposition des ressortissants de l'UE. Le Privacy Shield crée une médiation au sein du Département d'État américain qui peut entendre les plaintes de ressortissants concernés de l'UE dans le cadre d'actions du gouvernement des États-Unis.[88] Cette médiation fonctionne indépendamment des services de sécurité nationale des États-Unis, et les protections s'appliquent aux transferts de données en vertu de Clauses contractuelles types : le médiateur (Ombudsman) a le pouvoir d'examiner les « requêtes d'accès par la sécurité nationale à des données transmises depuis l'UE vers les États-Unis en vertu du Privacy Shield, des clauses contractuelles types [et] des règles d'entreprise contraignantes (BCR). »[89] Le Privacy Shield permet également aux personnes d'invoquer, à titre gracieux, un autre organisme indépendant de règlement des litiges pour traiter les plaintes contre des entreprises américaines participant au Privacy Shield.[90]

[54] En vertu du Judicial Redress Act de 2016,[91] les États-Unis ont explicitement étendu le droit à une action civile contre le gouvernement des États-Unis en vue d'obtenir des réparations à l'égard de divulgations volontaires ou intentionnelles d'enregistrements couverts en violation du Privacy Act ou lorsqu'une agence désignée du gouvernement des États-Unis refuse de modifier l'enregistrement d'une personne en réponse à une demande individuelle.[92] Le Judicial Redress Act répond directement à une préoccupation qui avait été précédemment exprimée par des responsables de l'UE : que les citoyens de l'UE ne bénéficiaient pas de garanties en vertu du Privacy Act. Bien que les États membres de l'UE n'aient pas à ce jour finalisé leur participation en vertu du Judicial Redress Act, je crois comprendre que l'UE et les États-Unis envisagent de le faire.

[55] Le Privacy Act permet aux États-Unis et à des personnes non-américaines de poursuivre une agence fédérale des États-Unis pour une mauvaise gestion d'enregistrements couverts, pour obtenir des injonctions ou des dommages-intérêts pécuniaires et d'examiner, de copier et de

---

[87] Pour une discussion plus détaillée de ces documents, y compris les critères d'admissibilité des personnes en vertu de la loi, *voir* Chapter 7, Section I(A)(1).

[88] European Commission Press Release MEMO16/434, *EU-U.S. Privacy Shield: Frequently Asked Questions*, (Feb. 29, 2016), http://europa.eu/rapid/press-release_MEMO-16-434_en.htm. Veuillez noter qu'à ce jour, ce mécanisme est toujours en cours d'organisation et n'est pas encore disponible. *Voir* PRIVACY SHIELD FRAMEWORK, *How to Submit a Request Relating to U.S. National Security Access to Data*, https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data

[89] European Commission, Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C(2016) 4176 final (July 12, 2016) at 52, http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf, [Ci-après les annexes]. Veuillez noter que le médiateur peut également examiner les requêtes présentées en réponse à des transmissions de données depuis l'UE vers les États-Unis en vertu de dérogations et d'éventuelles futures dérogations.

[90] *Annexes*, *supra* note 88 at 19, http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf; European Commission Directorate General for Justice and Consumers, *Guide to the EU-U.S. Privacy Shield* (2016), http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf.

[91] Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015), https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

[92] *Id.* at § 2(a).

demander des modifications dans leurs enregistrements.[93] Un particulier peut engager une poursuite en vertu de la loi lorsque l'agence omet volontairement ou intentionnellement de se conformer au Privacy Act d'une manière ayant « un impact négatif sur [la] personne. »[94] Une personne pourra également engager une poursuite si l'agence décide de ne pas modifier l'enregistrement de la personne suite à une demande, ne fournit pas un examen approprié sur la base d'une demande ou refuse de se conformer à une demande.[95] Comme cela est abordé de manière plus approfondie dans le chapitre 7, il existe des exceptions à l'applicabilité du Privacy Act.

[56] L'Umbrella Agreement prévoit des recours pour des personnes concernées de l'UE dont les données sont transférées à des autorités d'application de la loi des États-Unis. Les personnes peuvent accéder à ces informations personnelles, sous réserve de certaines restrictions équivalentes auxquelles doivent également faire face les citoyens américains, et les personnes concernées de l'UE peuvent demander une correction ou rectification.[96] Si une agence d'application de la loi rejette une demande d'accès ou de rectification, elle devra expliquer le motif de son refus « sans retard indu ». Les personnes concernées de l'UE peuvent, conformément au cadre juridique américain, demander une révision administrative et judiciaire de ce refus, ou demander un examen judiciaire de toute allégation de divulgation illégale volontaire ou intentionnelle d'informations personnelles.[97] Si besoin, le tribunal peut exiger l'accès à ces informations personnelles ou leur rectification, et peut accorder des dommages-intérêts compensatoires concernant d'autres violations.[98] Ces capacités sont accordées en partie par le Judicial Redress Act, dont l'adoption était due en partie à une exigence de l'Umbrella Agreement.[99]

[57] Le Stored Communications Act prévoit un recours à la fois pour les citoyens américains et européens en cas d'accès ou d'utilisation illégale de données de communications enregistrées par un agent gouvernemental non autorisé ou une agence américaine.[100] Les règles permettant d'avoir accès légalement à des données stockées dépendent du type de données. Concernant le contenu des communications, comme un courriel, un juge indépendant applique la règle constitutionnelle du Quatrième amendement, laquelle exige une cause probable de crime.[101]

---

[93] 5 U.S.C. § 552a(g)(1) ; cf. aussi *id.* au § 2(h)(4) (définissant des « enregistrements couverts » de la même manière qu'un enregistrement au titre de l'article 5 U.S.C., paragraphe 552a(a)(4)).
[94] *Id.*
[95] *Id.*
[96] *Voir* Proposal for a Council Decision on the conclusion, on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, at 10-12, COM (2016) 237 final (Apr. 29, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476055815798&uri=CELEX:52016PC0237.
[97] *Id.*
[98] *Id.*
[99] *Voir Press Release – Questions and Answers on the EU-US data protection "Umbrella Agreement"*, EUROPEAN COMMISSION (Sep. 8, 2015), http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[100] Pour obtenir une discussion plus détaillée du Stored Communications Act, veuillez vous reporter au chapitre 7, article I(A)(2).
[101] La loi elle-même applique différentes normes pour l'accès au contenu d'un courriel, en fonction de facteurs tels que le fait de savoir si le courriel a été ouvert et quelle est son ancienneté. Article 18 du Code des États-Unis, paragraphe 2703. Sur la base du Quatrième amendement, cependant, une cour d'appel fédérale a jugé dans la

L'accès aux métadonnées[102] oblige le gouvernement à certifier à un juge que les informations susceptibles d'être obtenues sont pertinentes dans le cadre d'une enquête criminelle en cours.[103] Une entreprise peut divulguer volontairement des renseignements de base sur les abonnés (basic subscriber information, BSI), et le gouvernement peut obliger l'accès à des BSI par le biais d'autres processus judiciaires tels qu'une citation à comparaître devant un grand jury.[104] Une personne concernée dont les données sont illégalement consultées peut engager des poursuites en vertu du SCA contre des agents individuels et des agences américaines si la violation était « intentionnelle ».[105] Le succès de poursuites contre des agents individuels peut donner lieu à des dommages-intérêts pécuniaires d'au moins 1 000,00 USD, une compensation équitable ou jugement déclaratoire, des honoraires d'avocat, des frais de justice, et/ou des dommages-intérêts punitifs.[106] Tout employé gouvernemental jugé pour avoir volontairement ou intentionnellement violé la loi peut également faire l'objet de mesures disciplinaires.[107] Des poursuites contre une agence américaine peuvent entraîner des dommages-intérêts compensatoires ou 10 000 USD, selon la somme la plus élevée, plus les dépens.[108]

[58] Le Wiretap Act octroie un droit d'action similaire pour les personnes contre le gouvernement des États-Unis.[109] En vertu du Wiretap Act, le gouvernement doit démontrer à la fois la cause probable et un certain nombre d'autres normes, y compris un crime suffisamment grave[110] et une explication de la raison pour laquelle les informations ne peuvent pas être obtenue par d'autres moyens.[111] Les écoutes téléphoniques ne sont autorisées que pour une durée limitée et spécifique,[112] doivent réduire au minimum la quantité d'informations non pertinentes interceptées,[113] et toute surveillance menée en dehors de ces limites est considérée comme

---

grande affaire *Warshak* que les gens peuvent espérer une certaine confidentialité dans le contenu d'un courriel, et que la norme de cause probable relativement stricte soit appliquée. *U.S. v. Warshak*, 631 F.3d 266, 274 (6th Cir. 2014). Le gouvernement des États-Unis a déclaré publiquement chercher le contenu d'un courriel en vertu de cette norme de cause probable. *ECPA (partie 1) : Lawful Access to Stored Content: Hearing before the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 113th Cong., 14 (2013) (déclaration d'Elana Tyrangiel, Sous-procureur général, Bureau de la politique juridique, Ministère de la Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.

[102] Les métadonnées incluent la numérotation, le routage, l'adressage et les informations de signalisation liées à une communication électronique.

[103] 18 U.S.C. §§ 3121-22.

[104] *Id.* §§ 2702-03.

[105] *Id.* § 2520. La disposition civile exigeant une violation « intentionnelle » comporte des exceptions relatives à la bonne foi des ordonnances de tribunal, aux citations à comparaître devant un grand jury, aux autorisations législatives, aux autorisations statutaires, ou à une requête valide émanant d'un agent d'enquête ou d'application de la loi. Article 18 du Code des États-Unis, paragraphe 2520(d). De même, il n'existe pas de violation « intentionnelle » lorsque l'individu ou l'agence poursuivi(e) a déterminé de bonne foi que l'action alléguée était valide en vertu de l'ECPA. *Id.*

[106] 18 U.S.C. § 2707(c).

[107] *Id.* § 2707(d).

[108] *Id.* § 2712(a).

[109] Pour obtenir une discussion plus détaillée du Wiretap Act, veuillez vous reporter à Chapter 7, Sections I(A)(2) and III(A)(2).

[110] 18 U.S.C. § 2518(3)(a).

[111] *Id.* § 2518(3)(c).

[112] *Id.* § 2518(4)(d).

[113] *Id.* § 2518(5).

illégale.[114] Les applications effectuées en vertu du Wiretap Act doivent également être approuvées au plus haut niveau du Ministère de la Justice avant de pouvoir être soumises à un juge pour examen. À l'image du SCA, le Wiretap Act permet également à des personnes lésées, y compris des ressortissants de l'UE, d'engager des poursuites lorsque leurs communications ont été interceptées illégalement par le gouvernement des États-Unis.[115] Si un individu a « intentionnellement » violé la loi,[116] la personne concernée pourra obtenir une « réparation appropriée »,[117] y compris une injonction sur toute écoute en cours, des dommages-intérêts pécuniaires et des dommages-intérêts punitifs.[118]

[59] Le FISA fournit également des recours individuels pour les personnes concernées par des actes illégaux d'agents du gouvernement.[119] Toute surveillance d'une personne concernée effectuée sans autorisation statutaire ou présidentielle, l'usage détourné d'informations de surveillance, ou la divulgation illégale d'informations de surveillance par un agent en particulier fera que l'agent pourra faire l'objet de poursuites devant un tribunal des États-Unis.[120] Les personnes concernées parvenant à poursuivre ces agents pourront recevoir des dommages-intérêts compensatoires supérieurs ou égaux à 1 000,00 USD, des dommages-intérêts préétablis de 100,00 USD par jour de surveillance illégale, et éventuellement des dommages-intérêts punitifs et des frais d'avocats, le cas échéant.[121] Une personne concernée de l'UE peut engager des poursuites en vertu du FISA, pour autant qu'elle ne soit pas une « puissance étrangère » ou un « agent d'une puissance étrangère ».[122]

B. Recours judiciaires criminels aux États-Unis

[60] Le Ministère de la Justice des États-Unis peut engager des poursuites pénales pour violation du SCA, de l'ECPA et du FISA.[123] Une attention particulière aux violations de la vie privée est conforme à l'engagement des États-Unis dans l'application efficace des lois de protection de la vie privée, tel que le démontre le Judicial Redress Act, l'Umbrella Agreement et

---

[114] *Id.* § 2518(5) (« Chaque ordonnance . . .devra être menée de manière à minimiser l'interception de communications qui ne sont pas autrement visées par une interception en vertu du présent chapitre »).
[115] *Voir* 18 U.S.C. §§ 2510(6), 2510(11) (définissant une « personne » et une « personne lésée » au sens de la loi) ; *voir également Suzlon Energy v. Microsoft*, 671 F.3d 726, 731 (9th Cir. 2011) (« Le ECPA protège les communications nationales de non-citoyens »). Dans la mesure où le Wiretap Act est codifié en vertu de l'ECPA, *Suzlon* s'applique également aux recours disponibles en vertu de l'article 18 du Code des États-Unis, paragraphe 2520.
[116] 18 U.S.C. § 2511(1)(a).
[117] *Id.* § 2520.
[118] *Id.* § 2520(b). Contrairement au SCA, le Wiretap Act ne prévoit pas explicitement d'accorder une renonciation à l'immunité de juridiction en cas de poursuites contre des agences américaines, mais permet plutôt des poursuites uniquement contre des agents ayant intentionnellement violé la loi. Article 18 du Code des États-Unis, paragraphe 2511(1).
[119] Pour obtenir une discussion plus détaillée du FISA, veuillez vous reporter au chapitre 7, article I(A)(4).
[120] 50 U.S.C. §§ 1801, 1810.
[121] *Id.* § 1810. Veuillez noter que la personne pourra soit recevoir des dommages-intérêts compensatoires minimum de 1 000,00 USD, soit des dommages-intérêts s'élevant à 100,00 USD par jour de surveillance, mais pas les deux.
[122] *Id.* §§ 1801(a)-1801(b).
[123] Pour obtenir des informations plus détaillées sur les sanctions pénales concernant de telles violations, veuillez vous reporter à Chapter 7, Section I(B).

le EU-US Privacy Shield Framework.[124] Par exemple, l'article du EU-US Privacy Shield Framework consacré aux recours, à l'application et à la responsabilité comprend un engagement stipulant que la FTC devra « donner la priorité aux cas de non-conformité avec les principes du Ministère et des autorités des États membres de l'UE. »[125]

[61] De plus, si le gouvernement des États-Unis tentait d'utiliser des informations acquises illégalement contre une personne concernée dans une procédure pénale, les personnes concernées, y compris des ressortissants de l'UE, disposeraient de deux droits importants. Premièrement, la règle d'exclusion permet aux personnes concernées de supprimer l'utilisation de preuves obtenues illégalement devant un tribunal.[126] Les tribunaux des États-Unis rejettent non seulement les preuves obtenues illégalement, mais rejettent également les preuves acquises à la suite de perquisition ou de saisie illégale.[127] Si une telle demande est refusée au cours d'un procès, la personne concernée sera en droit d'interjeter appel de cette décision.[128]

[62] Le Classified Information Procedures Act (CIPA) fournit également un mécanisme permettant aux défendeurs dans une affaire criminelle d'accéder à des documents classifiés au cours du procès qui pourraient être utile à la défense.[129] Le CIPA fournit des procédures protégeant la sécurité des informations classifiées tout en permettant aux défendeurs dans une affaire criminelle d'exiger la production de preuves relatives à leur défense.[130] En résumé, le CIPA protège à la fois l'intérêt du gouvernement des États-Unis à garder secrètes des données classées et le droit à un procès équitable pour les défendeurs dans une affaire criminelle.

II. Recours individuels non-judiciaires aux États-Unis contre le gouvernement des États-Unis

[63] En plus des recours judiciaires, il existe des canaux administratifs, législatifs et publiques importants pour les personnes concernées leur permettant de demander réparation en cas de préjudices porté à la vie privée par le gouvernement des États-Unis. La partie 2 de ce témoignage traite des garanties systémiques fournies par le PCLOB et les comités du Congrès sur le renseignement. Le PCLOB et les comités permettent également à des personnes de soumettre des préoccupations relatives aux pratiques du renseignement américain, pour des ressortissants américains aussi bien qu'européens.

---

[124] *Voir* Umbrella Agreement, *supra* note 70; PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY; Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2015).
[125] PRIVACY SHIELD FRAMEWORK, *Recourse, Enforcement and Liability*, https://www.privacyshield.gov/article?id=7-RECOURSE-ENFORCEMENT-AND-LIABILITY.
[126] *Voir* Chapter 3 ; *voir également* 18 U.S.C. § 2518(10)(a); *United States v. Warshak*, 631 F.3d at 282-89 (6th Cir. 2010) (jugeant qu'une preuve acquise en vertu du Stored Communications Act sans mandat est soumise à la règle d'exclusion).
[127] *Wong Sun v. United States*, 371 U.S. 471 (1963).
[128] FED. R. EVID. 103 (Expliquant comment une partie peut conserver le droit d'interjeter appel d'une décision d'admettre ou d'exclure des éléments de preuve au cours d'un procès).
[129] 18 U.S.C. App III §§ 1-16. Pour obtenir une discussion plus détaillée du CIPA, veuillez vous reporter au chapitre 8, article IV.
[130] *Id.*

[64] La presse libre américaine peut servir de recours à des personnes lésées par la surveillance des États-Unis. Contrairement aux lois sur les secrets officiels d'autres pays, le Premier amendement de la Constitution des États-Unis a été interprété de manière à respecter strictement la liberté des journalistes américains à soulever des questions de sécurité nationale comme la surveillance. Il protège également contre l'utilisation excessive de la diffamation et de la calomnie en exigeant des preuves strictes dans le cadre de ces poursuites.[131] Le Premier amendement prévoit également une protection contre la restriction d'emblée de la liberté de parole, y compris la censure d'articles proposés,[132] et il offre la possibilité de publier librement des informations confidentielles, même si elles ont été obtenues illégalement et/ou partagées avec le journaliste.[133]

[65] Des organisations non gouvernementales de défense de la vie privée aux États-Unis utilisent leur expertise et leurs ressources pour poursuivre le changement systémique et les recours au nom de personnes lésées.[134] Par exemple, le Centre de l'information du secret électronique (Electronic Privacy Information Center, EPIC), lequel participe à cette procédure, s'engage dans de nombreuses activités de protection de la vie privée, notamment des pétitions présentées au FTC concernant des torts individuels.[135] L'Union américaine pour les libertés civiles (American Civil Liberties Union), le Centre pour la démocratie et la technologie (Center for Democracy and Technology), la Fondation de la frontière électronique (Electronic Frontier Foundation), l'Institut de la technologie ouverte (Open Technology Institute) et de nombreuses autres organisations non-gouvernementales mènent des actions similaires, y compris l'évaluation et la compilation de documents gouvernementaux obtenus en vertu de la Loi sur l'accès à l'information (Freedom of Information Act).[136] Les personnes soucieuses de leurs droits à la vie privée peuvent solliciter une ou l'ensemble de ces organisations, ou toute autre organisation non-gouvernementale étrangère similaire pouvant travailler avec ces organisations américaines, ou qui peuvent travailler de manière indépendante ou de concert afin d'utiliser leurs ressources et leur influence pour remédier à une injustice individuelle ou influencer des changements dans les politiques ou les procédures américaines. La valeur de la liberté de la presse et des organisations non-gouvernementales aux États-Unis représente une voie importante pour les personnes recherchant des recours en matière de vie privée.

---

[131] U.S CONST. amend. I, *New York Times Co. v. Sullivan*, 376 U.S. 254, 727 (1964) (nécessitant une preuve de « malveillance réelle » pour accorder des dommages-intérêts en cas de diffamation dans des actions intentées par des agents publics contre les critiques de leur conduite officielle. »).

[132] *Voir New York Times Co. v. United States*, 403 U.S. 713, 717 (1971) (« L'histoire autant que la langue du Premier amendement soutient l'opinion que la presse doit être laissée libre de publier des informations, quelle qu'en soit la source, sans censure, injonctions, ou restrictions préalables. »).

[133] *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (« Nous pensons qu'il est évident qu'un raisonnement parallèle exige de conclure que la conduite illégale d'un étranger ne suffit pas à retirer le droit de garder le silence du Premier amendement concernant une question d'intérêt public. »).

[134] COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008) (analysant des groupes de défense de la vie privée aux États-Unis).

[135] ELECTRONIC PRIVACY INFORMATION CENTER, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.ORG, https://epic.org/apa/comments/.

[136] AMERICAN CIVIL LIBERTIES UNION, *Section 215 Documents*, https://www.aclu.org/foia-collection/section-215-documents.

III. Recours supplémentaires en matière de vie privée prévus par la législation fédérale

[66] Des personnes peuvent demander réparation pour des préjudices causés par des entreprises privées, tels que des fournisseurs de services de messagerie web et de réseaux sociaux, et qui divulguent des informations de manière inappropriée au gouvernement des États-Unis.[137] Ces fournisseurs de services sont fortement incités à respecter la loi et leurs propres politiques d'entreprise, dans la mesure où des violations pourraient entraîner des mesures répressives, des procès coûteux et d'importants dommages à la réputation de l'entreprise. Le SCA et le Wiretap Act notamment permettent des poursuites contre des entreprises privées qui partagent illégalement des données clients, lesquelles poursuites peuvent entraîner des dommages-intérêts coûteux.[138] Ces risques donnent forme aux informations que les entreprises sont disposées à partager avec le gouvernement et en vertu de quels processus.

[67] Les agences fédérales administratives agissent en tant que régulateurs et agents d'application des droits à la vie privée des personnes concernées pour les entreprises sous la juridiction de chaque agence, y compris en cas de divulgation inappropriée de communications électroniques par des entreprises au gouvernement. Ces agences agissent en tant qu'agents d'application de la loi dans leurs domaines de compétence respectifs, lesquels peuvent éventuellement se chevaucher. Le chapitre 7 présente cinq de ces agences : la Commission fédérale du commerce (Federal Trade Commission, FTC), la Commission fédérale des communications (Federal Communications Commission, FCC) ; le Bureau de protection financière des consommateurs (Consumer Financial Protection Bureau, CFPB) ; la Commission des opérations de bourse (Securities and Exchange Commission, SEC) ; et le Ministère de la Santé et des services sociaux (Department of Health and Human Services, HHS). Je mets l'accent sur le rôle de la FTC et son autorité en vertu, sans doute, de « l'élément le plus important de la législation américaine en matière de vie privée »[139] dans l'application d'actes ou de pratiques inéquitables ou malhonnêtes dans le secteur du commerce.[140]

[68] En vertu de la loi sur la FTC et d'autres pouvoirs, la FTC a assumé le rôle de contrôleur d'application de la loi en matière de protection de la vie privée contre des pratiques déloyales et trompeuses telles que des violations de déclaration de confidentialité d'entreprise,[141] le partage involontaire de courriels d'abonnés, [142] des déclarations trompeuses concernant les pratiques en matière de sécurité des données, [143] l'usage détourné et la collecte de données d'enfants[144] et des pratiques de spam indésirables.[145] La FTC commence souvent des enquêtes liées à l'application de la loi en réponse à des plaintes déposées directement auprès de l'agence, à des rapports de

[137] Pour obtenir une discussion plus détaillée sur ces recours, veuillez vous reporter au chapitre 7, article III(A).
[138] Une explication détaillée des dommages-intérêts disponibles en vertu du SCA et du Wiretap Act est disponible dans le chapitre 7, article III(A).
[139] *Voir* SWIRE AND AHMAD, *supra* note 3, at 14.
[140] 15 U.S.C. § 45.
[141] *Voir* SWIRE AND AHMAD, *supra* note 3, at 17 (traitant *de l'affaire GeoCities, Inc.*).
[142] *Id.* (traitant *de l'affaire Eli Lilly & Co.*).
[143] *Id.* (traitant *de l'affaire Microsoft Corp.*).
[144] *Id*. at 14 (Traitant de l'autorité de la FTC en vertu du Children's Online Privacy Protection Act.
[145] *Id.* (traitant de l'autorité de la FTC en vertu du Controlling the Assault of Non-Solicited Pornography and Marketing Act (Loi de contrôle des assauts de pornographie et de publicité non sollicitée).

presse ou des plaintes de concurrents commerciaux, ou à des recherches internes de la FTC.[146] La FTC peut, après une enquête, décider de former un recours administratif devant un juge administratif dont la décision peut faire l'objet d'un appel devant un tribunal fédéral de district des États-Unis.[147] En pratique, la FTC règle souvent ces actions par des décrets de consentement et des ordonnances par consentement associées[148] qui peuvent inclure des amendes et des engagements d'entreprises à améliorer leurs politiques et procédures, ainsi qu'à soumettre des vérifications futures et à revoir les pratiques en matière de vie privée.[149] Ces décrets sont des documents publics qui peuvent servir à établir des pratiques d'excellence et des protections minimales de référence chez les entreprises afin d'éviter de futures mesures d'application.[150] En effet, les Professeurs Daniel Solove et Woodrow Hartzog affirment qu'« aujourd'hui, la jurisprudence de la FTC en matière de vie privée est la force de réglementation la plus vaste et la plus influente sur la protection de la vie privée aux États-Unis »[151] et que « la compétence tentaculaire de la FTC dans l'application des lois en matière de vie privée » couvre des domaines qui sembleraient autrement non réglementés dans le commerce aux États-Unis.[152] Des effets similaires existent pour les activités d'application et de réglementation d'autres agences, comme cela est abordé dans le chapitre 7.

IV. Application en vertu de la législation des États-Unis et des droits privés d'action

[69] La loi d'État et les procureurs généraux d'État fournissent des mesures de protection supplémentaires en matière de vie privée pour les consommateurs tant à l'intérieur qu'à l'extérieur des États-Unis. Comme l'a abordé le professeur Danielle Citron, ces procureurs généraux se sont avérés être les principaux agents d'application des lois en matière de vie privée aux États-Unis. Le chapitre 7 propose une étude de cas détaillée du droit californien et de son application afin d'illustrer ce point.[153] La prévalence des avocats des plaignants et des droits privés d'action, ainsi que les dommages-intérêts importants octroyés dans ces actions, ont encouragé les entreprises à se conformer strictement à la loi applicable. Point important, les procureurs généraux d'État sont autorisés à examiner les demandes de toute personne, y compris des ressortissants de l'UE.

---

[146] *Id.* at 15.
[147] *Id.*
[148] *Voir id.*; FEDERAL TRADE COMMISSION, *Cases and Proceedings*, https://www.ftc.gov/enforcement/cases-proceedings.
[149] *Voir* SWIRE & AHMAD at 15.
[150] *Voir* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV. 583, 676 (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
[151] *Id.* at 587.
[152] *Id.* at 588. Dans son verdict du 29 août 2016 dans l'affaire *Federal Trade Commission c. AT&T Mobility LLC* la neuvième cour d'appel a observé des restrictions sur la juridiction d'application de la FTC concernant des entreprises classées comme des transporteurs publics, y compris des fournisseurs de services Internet. *Voir FTC v. AT&T Mobility*, No. 15-16585, 2016 WL 4501685 (9th Cir. Aug. 29, 2016), https://cdn.ca9.uscourts.gov/datastore/opinions/2016/08/29/15-16585.pdf Bien que cette décision actuelle puisse limiter la capacité de la FTC à engager des poursuites contre des entreprises offrant un service de transporteur, je crois que la décision de la cour était incorrecte, et elle fait aujourd'hui l'objet d'un appel vigoureux. Pour de plus amples informations sur la FTC et d'autres mesures administratives d'application, veuillez vous reporter à Chapter 7, Section III(B).
[153] *Voir* Chapter 7, Section IV.

V. Préoccupations dans les recours en matière de vie privée aux États-Unis dans l'affidavit du Commissaire irlandais chargé de la protection

[70] Le Commissaire irlandais chargé de la protection des données (Data Protection Commissioner, DPC) a déposé un affidavit dans cette affaire (l'« Affidavit du DPC ») fournissant un résumé des conclusions concernant les recours aux États-Unis.[154] La partie suivante cite brièvement des déclarations pertinentes de l'Affidavit du DPC, puis indique où la Cour peut trouver les passages où j'aborde ces questions dans mon témoignage.

[71] L'Affidavit DPC conclut que « les recours prévus par la législation des États-Unis sont fragmentés, et sont soumis à des limites ayant une incidence sur leur efficacité dans une certaine mesure. »[155] La chapitre 7 reconnaît que certains recours aux États-Unis puissent apparaître fragmentés, et décrit comment s'articulent les nombreuses voies par lesquelles la législation des États-Unis permet à des personnes de remédier à des violations de la vie privée. La complexité de la législation américaine peut s'expliquer en partie par le fait que plusieurs sources d'application des lois peuvent exister pour chaque question de vie privée. Cette division de l'autorité peut être bénéfique, car elle offre des droits privés d'action aux personnes, tout en permettant à plusieurs agences de définir les catégories d'activités au nom des personnes concernées.

[72] L'affidavit du DPC affirme que les recours aux États-Unis « surviennent uniquement dans des circonstances factuelles particulières », telles que des violations intentionnelles, et ne sont « pas d'une portée suffisamment large pour garantir un recours dans chaque situation dans laquelle existe une interférence avec [] des données personnelles. »[156] Comme nous l'avons vu dans le chapitre 7, articles I et III(A), certains recours aux États-Unis - comme les lois criminelles en général - exigent l'intention de montrer une violation. La portée de chaque recours aux États-Unis est traitée dans les chapitres 7 et 8.

[73] Le DPC a suggéré, en tant que développement positif, que les recours aux États-Unis puissent être réévalués « dans le contexte du » mécanisme de médiation du Privacy Shield.[157] Le chapitre 7, article I(A)(1) traite de la manière dont les ressortissants de l'UE peuvent désormais déposer des plaintes auprès d'un médiateur indépendant du gouvernement des États-Unis concernant la collecte de données, indépendamment du fait qu'ils aient été informés que les données personnelles ont été collectées, et sans avoir besoin de démontrer l'intention ou un préjudice réel. Le chapitre 7 traite également des voies de recours contre les entreprises qui violent les droits à la vie privée, établissant les recours disponibles spécifiquement pour les

---

[154] *Voir* Affidavit of John V. O'Dwyer, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed July 4, 2016) (H.C.) [ci-après « DPC Affidavit"].

[155] *Id.* para. 91.

[156] *Id.* para. 92.

[157] *Voir* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd.*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), para. 6(1). Le DPC affirme « qu'il ne pouvait avoir tenu compte de la Décision du Privacy Shield pour en arriver à la Décision provisoire dans la mesure où elle n'avait pas encore été mise en œuvre à la date d'adoption de la Décision provisoire. » *Id.*

citoyens de l'UE (Annexe 1) et les montants substantiels que les demandeurs ont obtenus dans le cadre du règlement de litiges en matière de vie privée aux États-Unis (Annexe 2).

[74] L'Affidavit du DPC affirme que les « exigences d'admissibilité de l'intérêt à agir des tribunaux fédéraux fonctionnent comme une contrainte sur toutes les formes de réparation disponibles. »[158] Le chapitre 7, article V fournit des détails concernant le développement d'affaires aux États-Unis depuis *Clapper c. Amnesty International USA Clapper*,[159] mentionnée dans la Décision provisoire du DPC. Le chapitre 7 traite plus généralement des voies offertes par la législation des États-Unis aux personnes pour remédier à des violations à la vie privée, y compris : recours judiciaires (chapitre 7, articles I et III(A)) ; recours non-judiciaires tels que le PCLOB et la presse libre (chapitre 7, article II) ; recours par des agences administratives via des agences telles que la Federal Trade Commission et la Federal Communications Commission (chapitre 7, article III(B)) ; et le mécanisme de médiation du Privacy Shield (chapitre 7, article I(A)(1)). La doctrine de l'intérêt à agir affecte potentiellement les recours judiciaires, et le chapitre 8 analyse les raisons pour lesquelles les tribunaux des États-Unis et de l'UE ont fait preuve de prudence dans la divulgation des secrets de sécurité nationale en audience publique. Les solutions comme la médiation, le PCLOB et la FTC ne sont pas soumises à de telles limitations de l'intérêt à agir.

[75] L'Affidavit du DPC cite également un certain nombre de conclusions concernant la loi de surveillance énoncée dans les rapports de la Commission européenne publiés le 27 novembre 2013.[160] Ces rapports de la Commission sont antérieurs aux recommandations de réforme du Groupe d'étude, ainsi que pratiquement toutes les réformes de l'après Snowden dans les pratiques de renseignement étranger des États-Unis que mon rapport aborde. J'aurais tendance à renvoyer la Cour au chapitre 3 (Garanties systémiques pour le renseignement étranger), 5 (la Cour de Surveillance du Renseignement Étranger), 6 (l'évaluation Oxford des lois de surveillance post-Snowden aux États-Unis) et 7 (Recours individuels aux États-Unis) pour obtenir une vue d'ensemble des pratiques actuelles du renseignement étranger aux États-Unis.

VI. Conclusions sur les recours individuels, avec une réserve

[76] La partie 3 de ce résumé du témoignage a exposé les multiples voies que des personnes peuvent suivre, y compris les citoyens de l'UE, pour exercer des recours aux États-Unis en cas de violations de la vie privée. Avant de passer à la partie 4, j'aborde brièvement une réserve concernant les recours individuels dans le cadre du renseignement. L'attrait des différentes voies de recours dans les systèmes doit être pondéré avec les risques inhérents à la divulgation d'informations classifiées. Dans les termes utilisés dans l'article 8 de la Convention européenne

[158] DPC Affidavit, *supra* note 153, para. 93.
[159] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).
[160] *Voir* DPC Affidavit, *supra* note 153, paras. 48-52 (citant la Commission européenne, *Communication from the Commission to the European Parliament and the Council*: *Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 (Nov. 27, 2013); et la Commission européenne, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM(2013) 847 (Nov. 27, 2013)).

des Droits de l'homme,[161] la disponibilité du droit individuel à la vie privée est évaluée par rapport à la nécessité dans une société démocratique de protéger les intérêts de sécurité nationale et de sûreté publique.

[77] Le domaine de la cybersécurité fournit une analogie pour décider quels sont les types de recours dont les personnes pourraient disposer en ce qui concerne le traitement de leurs informations par des agences de surveillance. Beaucoup d'entre nous sont aujourd'hui au moins un peu familiarisés avec trois types de précautions sur la cybersécurité : (1) ne pas cliquer sur des liens dans des courriels, dans la mesure où il pourrait s'agir d'attaques d'hameçonnage ; (2) mise à jour de votre logiciel anti-virus, de sorte que les virus n'infectent pas votre ordinateur ; et (3) disposer d'un bon pare-feu, de sorte que les attaquants ne puissent pas pénétrer dans votre système. L'idée que je propose est simple, mais utile à mon avis : être prudent sur la création d'un nouveau vecteur d'attaque, tels que des recours individuels, dans un système protégé.

[78] Un exemple simple illustre le type de préjudice pour la sécurité nationale qui pourrait résulter de l'accès direct par des personnes à leurs données détenues par une agence de renseignement. Supposons qu'un acteur hostile, tel qu'un service étranger de renseignement, veuille sonder la NSA ou l'agence de renseignement d'un État membre. L'acteur hostile peut avoir Alice qui utilise un service de messagerie SMS, Bob un service de messagerie électronique et Carlos un service de messagerie instantanée (chat). Ils déposent ensuite des demandes d'accès, et seul Bob obtient un fichier. Dans ce cas, l'acteur hostile a appris quelque chose de précieux : le service de messagerie électronique est sous surveillance, mais les services de SMS et de chat semblent ne pas l'être. Dans cet exemple, les recours possibles constituent une forme de cyberattaque hostile : l'acteur peut sonder les secrets de l'agence et apprendre ses sources et méthodes.

[79] Le chapitre 8 sur les acteurs hostiles et les considérations de sécurité nationale décrit comment une agence de renseignement hostile ou d'autres menaces persistantes et évoluées pourraient utiliser des recours individuels comme une forme de cyberattaque. Il souligne également que les attaques contre les agences de renseignement ne sont pas hypothétiques : elles sont menées quotidiennement par les adversaires les plus capables dans le monde. En bref, l'accès restreint aux secrets d'une agence de renseignement peut être considéré comme un dispositif de sécurité, en même temps qu'un bogue pour la vie privée.

[80] Le chapitre développe un point connexe important : les tribunaux européens et américains ont déjà créé des doctrines permettant d'éviter ce genre d'attaque. Aux États-Unis, les tribunaux reconnaissent dans certains cas ce que l'on appelle la « doctrine des secrets d'état », de sorte que les juges (tout en maintenant la surveillance générale sur une affaire) prennent soin de ne pas laisser les litiges individuels devenir une voie d'attaque sur les secrets de sécurité nationale. Les

[161] Dans mes discussions de l'article 8 de la Convention, je suis conscient des parties liées des autres instruments juridiques, surtout les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne. *Voir* Charter of Fundamental Rights of the European Union, 2000 O.J. C364/01 (Dec. 7, 2000) http://www.europarl.europa.eu/charter/pdf/text_en.pdf ; *voir également* Explanations relating to the Charter of Fundamental Rights, [2007] O.J. C303/17, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2007.303.01.0017.01.ENG.

décisions judiciaires similaires semblent être la norme en Europe, avec des juges protégeant contre la divulgation ou l'utilisation d'informations de sécurité nationale dans le cadre de procédures publiques. En d'autres termes, la loi établie reconnaît les limites des recours individuels dans le domaine du renseignement étranger.

[81] En tant qu'avocat américain, je ne tente pas d'affirmer dans mon rôle d'expert comment ces considérations concernant des attaques d'acteur hostile seraient jugées en vertu de la législation de l'UE. Je propose toutefois quelques observations fondées sur mon expérience du droit européen. Comme je l'ai indiqué dans le chapitre 2, j'ai beaucoup travaillé dans les années 1990 sur le droit d'accès dans l'UE, notamment en prenant la tête d'une délégation américaine qui s'est rendue dans six pays de l'UE pour étudier comment le droit d'accès était interprété dans la pratique. L'article 12 de la directive 95/46/CE dispose d'un droit d'accès en des termes généraux, sans préciser d'exceptions. Néanmoins, notre recherche a révélé des dizaines d'exceptions dans la pratique.

[82] Cette expérience éclaire mes opinions concernant l'applicabilité de l'article 8 de la Convention européenne des Droits de l'homme, et des articles 7, 8 et 47 de la Charte des droits fondamentaux de l'UE. Comme nous venons de le voir, l'article 8 de la Convention évalue la disponibilité du droit individuel à la vie privée par rapport à la nécessité dans une société démocratique de protéger les intérêts de sécurité nationale et de sûreté publique. Les décisions de l'Union européenne et des États-Unis limitant la divulgation de secrets de sécurité nationale que nous venons d'aborder reflètent l'évaluation judiciaire sur la manière de protéger à la fois la vie privée et la sécurité nationale.

[83] Contrairement à l'article 8 de la Convention, le droit à la vie privée et familiale énoncé dans l'article 7 de la Charte et le droit à la protection des données dans l'article 8 de la Charte ne stipulent pas que les droits sont assortis de dérogations pour des raisons de sécurité nationale, de sûreté publique, ou pour d'autres raisons. Il me semblerait cependant étonnant de considérer que les articles 7 et 8 ne disposent pas de dérogations, en considération de la sécurité nationale et d'autres droits et intérêts probants. De même, l'article 47 de la Charte stipule, sans dérogation, que « [t]oute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. » Il me semblerait logique que les juges de l'UE examinent la nécessité de sécurité nationale, de sûreté publique et d'autres facteurs d'intérêt public dans la détermination de l'étendue des recours individuels en vertu de l'article 47.

[84] En résumé, sur l'ensemble des recours individuels, la partie 3 de ce chapitre et le chapitre 7 décrivent les nombreux recours individuels disponibles aux États-Unis pour les violations de la vie privée, y compris pour des violations de la vie privée de citoyens de l'UE. Ces recours individuels existent en plus de l'ensemble fortement renforcé de garanties systémiques en vigueur aux États-Unis en raison de réformes mise en œuvre depuis 2001, et surtout depuis 2013. Dans l'examen des recours individuels, j'ai ajouté une réserve concernant la portée des recours individuels dans les systèmes de renseignement, en raison des risques découlant de la divulgation d'informations classifiées.

[85] Je passe maintenant à la partie 4, laquelle s'intéresse à d'autres considérations. La combinaison de garanties systémiques, de recours individuels et d'autres considérations devrait informer toute évaluation de l'adéquation de la protection des données transférées depuis l'UE vers les États-Unis.

PARTIE 4 :
L'ampleur potentielle de la décision et évaluation de l'adéquation des protections sur les transferts vers les États-Unis.

[86] La partie 4 de ce résumé de témoignage porte sur cinq considérations :

1. L'effet étendu, en vertu de la législation des États-Unis, d'une conclusion que les protections contre la surveillance excessive sont inadéquates ;

2. L'effet étendu pour les transferts transfrontaliers de telles conclusions, y compris pour les pays du BRIC (Brésil, Russie, Inde et Chine) ;

3. L'effet possible d'une conclusion d'inadéquation concernant les Clauses contractuelles standard pour d'autres mécanismes légaux de transfert de données vers des pays en dehors de l'UE ;

4. Les effets négatifs potentiellement importants sur le bien-être économique de l'UE d'une telle conclusion, comme l'ont indiqué les institutions européennes et les États membres, et requis en vertu du droit commercial international ; et

5. Les effets négatifs potentiellement importants sur la sécurité nationale et la sûreté publique de l'UE d'une telle conclusion, comme indiqué par les institutions européennes, et contraires à l'objectif de protection de la sécurité mutuelle de l'OTAN.

I. La vaste définition américaine de « prestataires de services » affectée par une décision

[87] Cette procédure serait plus simple à certains égards si les effets d'une conclusion d'inadéquation s'appliquaient uniquement à une ou quelques entreprises. Comme nous l'avons cependant vu dans le chapitre 9, la législation pertinente des États-Unis s'applique à grande échelle. Toute affirmation que l'article 702 ne s'appliquerait qu'à un ensemble restreint d'entreprises telles que Facebook est inexacte.

[88] L'article 702 s'applique à la collecte de données auprès de « fournisseurs de services de communications électroniques », un terme qui est défini de façon large dans le cadre de la législation des États-Unis.[162] Les tribunaux américains ont interprété les définitions pertinentes

[162] 50 U.S.C. § 1881 (définissant le terme « fournisseur de services de communications électroniques » pour englober la définition énoncée dans l'Electronic Communications Privacy Act, article 18 du Code des États-Unis, 2510). Je remarque que la discussion du chapitre 9 traite de cas qui ont examiné l'ECPA et pas le FISA. Je ne

afin d'inclure toute entreprise fournissant à ses employés un courriel professionnel ou une autre capacité d'envoyer et de recevoir des communications électroniques. Une conclusion d'inadéquation de la protection s'appliquant à l'article 702 pourrait ainsi s'appliquer à presque n'importe quelle entreprise menant des activités à la fois au sein de l'UE et aux États-Unis. Il n'existe aucune exception ou interprétation législative qui pourrait limiter le potentiel d'application de la conclusion d'inadéquation au regard de l'article 702. Avoir cette impression serait ne pas tenir compte de l'ampleur d'une telle décision.

[89] Le régime juridique de l'UE tel qu'il s'applique au consentement dans le contexte des employés signifie que l'application large de l'article 702 pourrait avoir une incidence particulièrement importante sur les activités de ressources humaines telles que la communication interne, la gestion du personnel ou des salaires. Les autorités chargées de la protection des données de l'UE ont été sceptiques sur le fait que les employés puissent donner leur consentement volontaire aux transferts de leurs données personnelles en dehors de l'UE.[163] Les entreprises opérant dans l'UE pourraient par conséquent faire face à des défis importants pour obtenir le consentement effectif d'un employé de l'Union européenne au transfert de leurs données personnelles vers d'autres pays, y compris vers les États-Unis. Ainsi, en cas de conclusion d'inadéquation de la protection aux États-Unis pour les Clauses contractuelles standard, le consentement individuel dans le contexte de l'emploi pourrait ne pas fournir de base alternative pratique aux transferts.

II. Les États-Unis bénéficient de garanties systémiques plus fortes que les pays du BRIC

[90] Je procède ensuite à quelques comparaisons de base sur les garanties contre la surveillance aux États-Unis par rapport aux importants pays constituant le BRIC : Brésil, Russie, Inde et Chine. La comparaison est pertinente en raison de la nature de l'enquête concernant l'adéquation aux États-Unis : lorsque des données personnelles sont transférées depuis l'UE vers les États-Unis, existe-t-il des garanties suffisantes contre la surveillance par le gouvernement américain ? Mon témoignage a fourni des détails sur les nombreuses garanties systémiques et les recours individuels en vigueur contre les excès de la surveillance liée à la sécurité nationale concernant les données transférées vers les États-Unis.

---

connais aucune raison de croire que l'utilisation de ce terme dans l'article 702 est différente. Je ne suis pas non plus au courant de toute opinion déclassifiée du FISC énonçant ce point précis.

[163] Le Groupe de travail Article 29 a indiqué que lorsque des transferts de données des ressources humaines avaient lieu sous la forme d'une « conséquence nécessaire et inévitable de la relation de travail », il serait considéré comme « trompeur » pour les employeurs d'utiliser le consentement comme base dans la mesure où « [s']il n'est pas possible pour l'employé de refuser, il ne s'agit pas d'un consentement. » Ainsi, un « consentement ne pourra normalement pas constituer un moyen de légitimer [des données] dans le contexte de l'emploi. » *Voir* Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (WP 48), 13 September 2001, at 3, 23, 28, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf Si le consentement est considéré comme une base pour les transferts, il peut être librement retiré, ce qui peut obliger les employeurs à respecter la volonté des employés qui souhaitent conserver les données au sein de l'UE. *Voir id.* au point 4 (« Les employeurs seraient mal avisés de se fier uniquement au consentement autrement que dans les cas où, si le consentement est retiré par la suite, cela ne sera pas une source de problèmes. »).

[91] Le point fondamental est simple : supposons que les garanties contre la surveillance dans les pays du BRIC sont plus faibles que les garanties en vigueur aux États-Unis. Si les mesures américaines sont jugées inadéquates, il semblerait donc logique que les garanties mises en place dans les pays où les garanties sont plus faibles soient également insuffisantes. En d'autres termes, si les garanties offertes par les États-Unis sont jugées inadéquates, il semblerait donc que les transferts de données à caractère personnel ne disposeraient d'une protection adéquate que dans les pays offrant des *garanties plus solides* qu'aux États-Unis.

[92] Mon analyse montre que les garanties des pays du BRIC sont clairement moins étendues que celles des États-Unis.[164] En commençant par la Chine, il existe un contraste évident entre la surveillance généralisée et le contrôle des informations accompagnant le « Grand pare-feu de Chine » et le système d'équilibre des pouvoirs prévu par la Constitution des États-Unis. Une étude récente a décrit l'approche chinoise comme une « surveillance illimitée » et a indiqué que « le gouvernement chinois a un grand appétit pour la surveillance Internet et les installations technologiques permettant d'espionner de manière indétectable. »[165] Une étude réalisée par des experts européens de la protection des données a analysé certaines lois protégeant la vie privée dans le contexte commercial, mais elle n'a pas fait état de toutes garanties importantes contre l'accès du gouvernement à des communications de personnes.[166]

[93] Le manque de garanties contre la surveillance en Russie a été documenté en détail par la Cour européenne des Droits de l'homme en 2015 dans l'affaire *Zakharov*.[167] Cette affaire impliquait le système de surveillance SORM en Russie, lequel donne un accès direct et câblé à des communications électroniques à de nombreuses agences gouvernementales : le Service de sécurité fédérale, la Police fiscale, le Ministère de l'intérieur, les Garde-frontières, le Comité des douanes, le Service de sécurité du Kremlin, le Service de sécurité présidentielle, les Services de sécurité parlementaire et le Service de renseignement étranger.[168] Dans l'affaire *Zakharov* , la CEDH a estimé que l'accès illimité du programme SORM à des communications téléphoniques sans autorisation judiciaire préalable violait l'article 8 de la Convention européenne des Droits

---

[164] Je fonde mes déclarations ici en partie sur des voyages en Inde en 2011 et en Russie en 2016. Dans les deux cas, j'ai rencontré des hauts fonctionnaires chargés des questions de vie privée et de cybersécurité, et j'ai mené des recherches approfondies sur les systèmes nationaux. Mes déclarations ici concernant les quatre pays sont fondées sur mon étude des questions de surveillance internationale et de protection de la vie privée au cours des vingt dernières années, y compris sur des discussions avec des experts de chacun des pays lors de conférences et à d'autres occasions.

[165] Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 854, 893 (2013), http://digitalcommons.pace.edu/lawfaculty/922.

[166] Paul de Hert & Vagelis Papakonstantinou, European Parliament Directorate General for Internal Policies, *The Data Protection Regime in China: In-Depth Analysis for the LIBE Committee*, PE 536.472 EN, (Oct. 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

[167] *Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. 2015), Grand Chamber (Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324 *Voir également* GLOBALVOICES, *As Russia insulates itself from human rights bodies, state surveillance decision looms* (Dec. 17, 2015), https://advox.globalvoices.org/2015/12/18/as-russia-insulates-itself-from-human-rights-bodies-state-surveillance-decision-looms/ [ci-après « *As Russia Insulates Itself"*].

[168] *Voir* WORLD POLICY INSTITUTE, *Russia's Surveillance State*, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance; *New powers for the Russian surveillance system SORM-2*, SECURITY AFFAIRS (Aug. 18, 2014), http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html.

de l'homme.[169] Comme indiqué dans le Rapport spécial sur les intérêts privés *de Privacy International : En observant l'Asie centrale*, « l'accès direct mandaté en vertu du modèle SORM représente un départ des protocoles légaux d'interception des données d'Amérique du Nord et d'Europe, ainsi qu'un défi considérable pour la protection des droits de la personne. »[170]

[94] Les systèmes juridiques de l'Inde et du Brésil se situent entre ceux de la Chine et de la Russie, d'une part, et l'ensemble des garanties systémiques et des recours individuels en vigueur aux États-Unis. L'Inde a un système juridique complexe, avec des lois qui varient considérablement entre ses 29 états. Les pratiques de surveillance des indiens après Snowden démontrent un « état actuel d'opacité » avec relativement peu de documents publics sur les pratiques de surveillance des communications.[171] Il y a peu de raison de croire que l'Inde dispose d'un système aussi robuste de garanties systémiques que celui des États-Unis : « [L]a surveillance des communications continue d'être le domaine exclusif de la branche exécutive du gouvernement » et « il n'existe aucune disposition de contrôle judiciaire ou public du processus de surveillance. »[172] Ce manque de contrôle judiciaire ou autre, et le manque de transparence, contrastent nettement, par exemple, avec les actions de la Cour de Surveillance du Renseignement Étranger des États-Unis, comme l'aborde le chapitre 5.

[95] Une étude détaillée de 2015 sur les pratiques de surveillance du Brésil montre un système qui semble plus proche des visions européennes et américaines que ceux des trois autres pays du BRIC.[173] Pour accéder à l'application des lois, le Brésil dispose d'une surveillance de la justice et de rapports statistiques, ainsi que d'exigences en matière de conservation de données pour les communications de métadonnées. L'étude exprime des préoccupations indiquant que la surveillance est « limitée en théorie mais vaste dans la pratique. »[174] Pour la surveillance du renseignement et de la sécurité nationale, « on sait peu de choses » sur les « opérations des agences concernées au Brésil. De plus, il n'existe presque aucune information sur la surveillance

---

[169] *Zakharov v. Russia*, App. No. 47143/06 (Eur. Ct. H.R. 2015), http://hudoc.echr.coe.int/eng?i=001-159324; *voir également As Russia Insulates Itself*, *supra* note 166.

[170] PRIVACY INT'L, *Privacy Interests: Monitoring Central Asia* (Nov. 2014), https://www.privacyinternational.org/sites/default/files/Private%20Interests%20with%20annex_0.pdf.

[171] WORLD WIDE WEB FOUNDATION, INDIA'S SURVEILLANCE STATE: COMMUNICATIONS SURVEILLANCE IN INDIA (non daté, mais le contenu indique une publication après les divulgations de Snowden de juin 2013), http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf [ci-après « INDIA'S SURVEILLANCE STATE"] ; Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (July 10, 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india; *voir également* CENTER FOR DEMOCRACY AND TECHNOLOGY, *National Security Standards by Country* (2013), https://govaccess.cdt.info/standards-ns-country.php [ci-après « *National Security Standards by Country*"]; VODAFONE, *Law Enforcement Disclosure Report: Legal Annex* (June 2014), http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf [ci-après « *Vodafone Law Enforcement Report*"].

[172] INDIA'S SURVEILLANCE STATE, *supra* note 170, at 49.

[173] DENNY ANTONIALLY AND JACQUELINE DE SOUZA ABREU, STATE SURVEILLANCE OF COMMUNICATIONS IN BRAZIL AND THE PROTECTION OF FUNDAMENTAL RIGHTS, ELECTRONIC FRONTIER FOUNDATION, 13 (Dec. 2015), https://www.eff.org/files/2015/12/17/brazil-en-dec2015_0.pdf [ci-après « STATE SURVEILLANCE IN BRAZIL »] ; *voir également National Security Standards by Country*, *supra* note 170, and *Vodafone Law Enforcement Report*, *supra* note 170.

[174] STATE SURVEILLANCE IN BRAZIL, *supra* note 172, at 22.

exercée par la Commission mixte du Congrès national. »[175] En se fondant sur ce manque de transparence et de contrôle, il semble difficile de démontrer que les garanties systémiques pour la surveillance de la sécurité nationale sont plus fortes au Brésil qu'aux États-Unis.

[96] Les quatre pays du BRIC sont de grandes nations et des partenaires commerciaux importants de l'UE. Tous témoignent d'activités de surveillance avec moins de transparence et de contrôle, et dans l'ensemble moins de garanties systémiques et de recours individuels que les États-Unis.[176]

[97] La relative absence de garanties est remarquable pour au moins deux raisons. Premièrement, j'ai entendu dire que les transferts depuis l'UE vers les États-Unis devraient être interdits, en raison des lois de surveillance américaines, en exprimant dans le même temps l'avis que les transferts depuis l'UE vers d'autres pays, comme la Chine, seraient autorisés. Cette référence à la Chine m'a conduit à examiner les implications des garanties chinoises contre la surveillance, lesquelles sont moins étendues que les garanties américaines.

[98] Deuxièmement, mon expérience en matière de droit de protection des données à l'échelle mondiale m'amène à conclure que l'absence relative de garanties dans les pays du BRIC prévaut dans la plupart des autres pays en dehors de l'UE. Le rôle des États-Unis en tant que « référence » dans les garanties contre la surveillance et la relative absence de garanties dans la plupart des pays non membres de l'UE, a des conséquences importantes : s'il est jugé que les États-Unis manquent de garanties appropriées contre la surveillance, ce manque devrait alors logiquement être observé dans les pays BRIC et dans de nombreux autres pays. Seuls les pays dont les garanties sont manifestement plus fortes que celles des États-Unis semblent bénéficier d'une base légale pour recevoir des données à caractère personnel provenant de l'UE. L'importation logique de cette conclusion devrait semble-t-il supprimer la base légale pour des parties importantes des flux transfrontaliers de données en provenance de l'UE.

III. La conclusion d'une inadéquation concernant les SCC pourrait avoir des répercussions sur d'autres bases légales pour les transferts de données

[99] La procédure actuelle concerne spécifiquement le fait de savoir si les Clauses contractuelles standard (SCC) fournissent une protection adéquate par rapport aux pratiques de surveillance américaines. La Décision provisoire du Commissaire chargé de la protection des données indiquait qu'elle se considérait comme « liée par le jugement » dans l'affaire *Schrems* de 2015 pour s'engager dans les procédures juridiques actuelles.[177] Je comprends par cette déclaration que le Commissaire voit un lien entre le traitement juridique d'une base pour le transfert juridique (Safe Harbour ou Sphère de sécurité) et d'une autre base pour transfert légal

[175] *Id.* at 39.
[176] Une analyse effectuée en vertu de l'article 47 de la Charte semble démontrer que ces pays manquent de « recours efficaces » et d'examen des demandes requis par un « tribunal indépendant et impartial. » *Voir* Art. 47, Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[177] *Voir* Plaintiff's Reply to the Defence of the First Named Defendant, *Data Protection Comm'r v. Facebook Ireland Ltd*, No. 2016/4809P (filed Sept. 30, 2016) (H.C.), para. 65

(SCC). Si un tribunal devait reconnaître ce lien, il existerait donc une possibilité qu'un jugement dans la présente procédure ait des implications sur d'autres bases pour un transfert légal.

[100] Il existe plusieurs façons pour qu'une conclusion juridique concernant une base juridique pour un transfert soit pertinente ou non dans une conclusion juridique à propos d'une base juridique différente. Pour commencer, j'estime que la présente procédure est une occasion de développer un dossier factuel beaucoup plus détaillé que celui qui avait été présenté devant la CJUE en 2015 dans l'affaire *Schrems*. Mon témoignage présente différents aspects de la législation et des pratiques des États-Unis qui n'étaient pas présentes dans le dossier de l'affaire de 2015. Comme nous l'avons vu tout au long de mon témoignage, il existe de bonnes raisons de conclure que le système de garanties des États-Unis pour les enquêtes de renseignement étranger est plus strict et plus efficace dans la pratique que les systèmes mis en place dans les pays de l'UE. Le dossier détaillé présenté devant la Cour dans le cadre de la présente procédure illustre ainsi comment une décision judiciaire concernant l'adéquation d'une base légale de transfert (Safe Harbor) peut s'avérer compatible avec une autre décision judiciaire concernant une autre base légale du transfert (SCC).

[101] Si la Cour devait conclure à une inadéquation dans la présente procédure, cette perspective de différentes conclusions d'inadéquation pourrait logiquement avoir lieu en vertu d'autres bases légales, telles que le Privacy Shield ou les Règles d'entreprise contraignantes (BCR). Il existe des similitudes entre les SCC, le Privacy Shield et les BCR, telle que l'annonce dans le Privacy Shield que les procédures de médiation s'appliqueront aux données transférées en vertu de l'une quelconque de ces bases légales.[178] De plus, pour les données stockées aux États-Unis, pour autant que je sache, les mêmes règles s'appliquent en vertu de l'article 702 du FISA et d'autres autorités juridiques, que le transfert ait eu lieu en vertu des SCC, du Privacy Shield ou des BCR. D'autre part, des considérations importantes peuvent exister dans la législation de l'UE quant à savoir pourquoi un jugement sur une adéquation en vertu des SCC pourrait conduire à un autre résultat qu'une adéquation dans le cadre d'autres méthodes de transfert, comme le Privacy Shield ou les Règles d'entreprise contraignantes. Je ne fais aucune déclaration sur la question juridique de l'UE, concernant l'effet, le cas échéant, que pourrait avoir une conclusion d'adéquation dans la présente procédure sur le Privacy Shield ou les BCR.

[102] Ceci dit, l'impact de la présente procédure varierait considérablement selon qu'une conclusion d'inadéquation des protections américaines contre la surveillance s'applique uniquement aux SCC, ou s'applique plus largement à d'autres bases pour un transfert légal. L'impact d'une conclusion d'inadéquation concernant uniquement les SCC serait moins important qu'une conclusion d'inadéquation s'appliquant également au Privacy Shield et aux BCR. Si les tribunaux européens venaient à juger au fil du temps que les SCC, le Privacy Shield et les BCR n'étaient pas disponibles, il m'est difficile de voir comment créer une base légale pour de nombreux transferts de données actuellement existants. Il y a effectivement d'autres

[178] EU-U.S. PRIVACY SHIELD, Annex III.A., at 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL (indiquant que le médiateur traitera les « demandes relatives à la sécurité nationale d'accès à des données en provenance de l'UE vers les États-Unis conformément au Privacy Shield, aux Clauses contractuelles standard (SCC), aux Règles d'entreprise contraignantes (BCR), aux « dérogations » ou « éventuelles futures dérogations »).

dérogations qui autorisent les transferts de données, même lorsque le pays destinataire manque de mesures adéquates, notamment le consentement. Les autorités de protection des données de l'UE ont cependant pris clairement position contre l'utilisation généralisée du consentement dans une variété de paramètres, y compris pour les registres des ressources humaines,[179] et je ne connais aucune autre manière générale permettant de transférer légalement des données à caractère personnel.

[103] Si au fil du temps la CJUE établissait un manque d'adéquation pour l'ensemble des mécanismes de transfert vers les États-Unis, il semblerait alors y avoir peu de possibilités pour que des institutions autres que les tribunaux puissent effectivement être en désaccord avec cette conclusion ou les modifier après coup. En vertu du Traité de Lisbonne, les décisions de la CJUE ont force obligatoire sur les États membres.[180] Si la Commission, les États membres ou d'autres institutions devaient être en désaccord avec une conclusion de la CJUE sur une inadéquation aux États-Unis, la structure constitutionnelle de l'UE rendrait difficile sa mise en œuvre. En vertu de la Constitution des États-Unis, l'article V crée un processus d'amendement,[181] et le processus d'amendement a été parfois utilisé pour renverser les décisions de la Cour suprême des États-Unis.[182] Aucun processus similaire d'amendement n'existe actuellement au sein de l'UE. Conformément à mes entretiens avec des avocats de l'UE, ma compréhension est qu'une renégociation du Traité de Lisbonne pourrait être nécessaire pour contrer une conclusion d'inadéquation de la CJUE concernant les garanties américaines contre la surveillance.[183]

[104] **En bref, je ne fais aucune déclaration sur la question de savoir si la conclusion d'inadéquation concernant les SCC entraînerait une conclusion d'inadéquation pour le Privacy Shield ou les BCR. La discussion soutient ici la possibilité qu'une conclusion d'inadéquation pour les SCC pourrait avoir des répercussions sur d'autres bases légales concernant les transferts de données. Dans la suite de ce témoignage, je me réfère à la plus**

---

[179] La question des ressources humaines est discutée ci-dessus dans la partie 4(A) de mon résumé de témoignage, dans le cadre de la question du grand nombre d'entreprises différentes dont les transferts de données sont susceptibles d'être touchés par une décision dans cette affaire.

[180] *Voir en général* TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, Arts. 19, 251-281, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

[181] *Voir* U.S. CONST. Art. V Un amendement constitutionnel peut être adopté avec une super-majorité de soutien, généralement les deux tiers des deux chambres du Congrès des États-Unis, et la ratification par les trois quarts des États.

[182] Il existe au moins trois exemples où un amendement constitutionnel a renversé une décision de la Cour suprême des États-Unis : (1) le 11ème amendement, concernant des poursuites intentées par des citoyens d'un état contre un autre état, est survenu après l'affaire *Chisholm c. Géorgie*, 2 U.S. 419 (1793) ; (2) le 16ème amendement permettant un impôt sur le revenu, est survenu après l'affaire *Pollock c. Farmers' Loan & Trust*, 157 U.S. 429 (1895*) ;* et (3) le 24ème amendement, l'abolition de l'impôt de capitation, est survenu après l'affaire *Breedlove c. Suttles*, 302 U.S. 277 (1937).

[183] Une autre possibilité logique est qu'une décision de la CJCE pourrait indiquer l'existence actuellement d'une inadéquation, laquelle pourrait toutefois être corrigée si les États-Unis changeaient leurs pratiques. Une telle décision serait similaire à un ensemble d'instructions sur la manière dont les États-Unis devraient changer leurs pratiques de sécurité nationale, ce qui soulèverait des questions délicates dans les relations entre les États-Unis et l'Union européenne. À l'avenir, cela voudrait également dire que les tribunaux auraient besoin de mettre à jour leurs conclusions au sujet des pratiques générales de sécurité nationale d'une autre nation, ce qui implique souvent des informations classifiées. Ce genre d'évaluation des pratiques d'un État non membre impliquerait que les tribunaux s'attaqueraient à des questions difficiles historiquement gérées par des moyens diplomatiques.

large possibilité d'une « conclusion catégorique d'inadéquation » : une conclusion d'inadéquation qui s'appliquerait non seulement aux SCC, mais également au Privacy Shield et aux BCR. Si une conclusion d'inadéquation s'appliquait uniquement aux SCC, les effets de cette conclusion pourraient alors être limités, en particulier si l'opportunité se présente d'interpréter ou de mettre à jour le Privacy Shield et les BCR pour des cas spécifiques d'utilisation où les SCC se sont avérées les plus utiles à ce jour. Si une conclusion d'inadéquation catégorique devait cependant être établie, elle pourrait avoir des conséquences importantes sur l'ensemble des relations UE/États-Unis, affectant les relations étrangères, la sécurité nationale, les intérêts économiques et d'autres intérêts des États membres et de l'UE elle-même. Je m'intéresse ensuite à l'effet que pourrait avoir une conclusion aussi catégorique sur le bien-être économique des États membres de l'UE.

IV. Bien-être économique du pays

[105] Je suis d'avis qu'une conclusion catégorique stipulant que les États-Unis disposaient de mesures inadéquates en raison de son système de surveillance aurait des effets économiques importants. L'élaboration d'un dossier détaillé dans la présente procédure, à mon avis, est l'occasion d'exposer ces effets économiques, ainsi que mes nombreux commentaires sur la nature de l'adéquation des garanties systémiques contre la surveillance elles-mêmes.

[106] Je n'entreprends pas d'analyse statistique sur l'ampleur des effets économiques potentiels. Au lieu de cela, mes commentaires sont basés sur mon expérience générale dans ce domaine. En considérant les effets économiques, j'aborde brièvement certaines déclarations de l'UE sur l'importance de la relation économique transatlantique, avant d'examiner les considérations commerciales internationales.

A. Déclarations de l'Union européenne sur l'importance de la relation économique transatlantique

[107] La Commission de l'UE a souligné l'importance économique de la relation transatlantique et des flux transfrontaliers de données entre l'UE et les États-Unis. Les documents du Privacy Shield indiquent : « La relation économique transatlantique est déjà la plus importante du monde, représentant la moitié de la production économique mondiale et près de 1 000 milliards de dollars d'échange de biens et de services, . . . soutenant des millions d'emplois des deux côtés de l'Atlantique. »[184] Concernant les flux de données, la Décision finale de la Commission concernant l'adéquation du Privacy Shield précise que « l'augmentation exponentielle des flux de données » entre l'UE et les États-Unis est d'une importance cruciale pour l'économie transatlantique. »[185]

---

[184] EU-U.S. PRIVACY SHIELD, Annex I.1., at 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

[185] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, para. 7, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL.

[108] Les autorités de protection des données de l'UE ont indiqué leur accord. Dans son examen des documents préliminaires du Privacy Shield, le Contrôleur européen de la protection des données a indiqué que l'alliance UE-États-Unis est « le plus grand partenariat commercial au monde, » et que le but de cet examen était de « renforcer les relations transatlantiques » afin qu'elles puissent être « stables sur le long terme. »[186] Le Groupe de travail Article 29, tout en exprimant des réserves quant à certains aspects du Privacy Shield, a convenu que « les transferts de données qui ont lieu entre l'UE et les États-Unis sur une base quotidienne » constituent « une partie essentielle de l'économie des deux côtés de l'Atlantique. »[187]

[109] Les États membres de l'UE, à la lumière des enjeux, ont également exprimé leur « appui solide » au Privacy Shield, afin de créer la base légale pour les flux de données.[188] Les branches politiques d'Irlande, ainsi que des partenaires majeurs comme la France, l'Allemagne et le Royaume-Uni, ont participé au processus du Comité de l'article 31 afin d'examiner le Privacy Shield. Les registres du Comité montrent que 24 États membres, représentant 96 pour cent de la population de l'UE, ont voté en faveur du Privacy Shield,[189] avec 4 abstentions et aucun vote contre. L'Irlande, représentée par son Ministère de la Justice et de l'Égalité[190], a soutenu le Privacy Shield. En somme, les institutions de l'UE et les États membres ont clairement indiqué l'importance de maintenir les flux transfrontaliers de données et de favoriser la relation transatlantique.

B. Accords commerciaux, y compris l'Accord général sur le commerce des services

---

[186] European Data Protection Supervisor, *Opinion 4/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision*, (May 30, 2016), at 2, 12, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.

[187] Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (WP 238), (Apr. 13 2016) at 12, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[188] European Commission, Statement by Vice-President Ansip and Commissioner Jourová on the occasion of the adoption by Member States of the EU-U.S. Privacy Shield Privacy Shield, Statement 16/2443 (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm.

[189] *Voir* Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Formal vote on Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of protection provided by the EU-U.S. Privacy Shield , V046420/01, CMTD(2016)0868 (July 8, 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx1H1ssUUcBMQ0wtPEeDmiVQXV3U4/r7rgJvJWdYwELHg (montrant que 95 % des États membres représentés dans le Comité de l'article 31 ont voté en faveur du Privacy Shield).

[190] *Voir* Summary record of the 71st meeting of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee), S046419/01 CMTD(2016)0868 (July, 8 2016), http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&ZMd/3IPPHtzAeedC2zZGx41KHuMFW2Bq3YHOFmINgVoXV3U4/r7rgJvJWdYwELHg (montrant que le Ministère de la Justice et de l'Égalité d'Irlande a participé au vote sur le Privacy Shield) ; Jedidiah Bracy, *EU Member States approve Privacy Shield*, IAPP.ORG (July 8, 2016), https://iapp.org/news/a/eu-member-states-approve-privacy-shield/ (identifiant que seules l'Autriche, la Croatie, la Slovénie et la Bulgarie s'étaient abstenues de voter sur le Privacy Shield).

[110] Il existe des dispositions importantes dans les traités commerciaux internationaux soutenant la protection de la vie privée.[191] À mon avis, une conclusion d'inadéquation catégorique des garanties américaines contre la surveillance, et le blocage des transferts de données vers les États-Unis, créerait une forte possibilité de violation de traité.

[111] Comme cela est largement compris, l'approche générale de l'Organisation mondiale du commerce et de l'Accord général sur les tarifs douaniers et le commerce est d'appuyer le libre-échange et de supprimer les mesures protectionnistes. Pour cette raison, une règle juridique empêchant des données de quitter une juridiction peut poser une difficulté dans le libre-échange : quelle est la base légale du traitement des transferts vers un autre pays comme les États-Unis différemment du partage de données au sein d'un même pays ?

[112] Concernant la vie privée, la réponse habituelle est que l'Accord général sur le commerce des services (General Agreement on Trade in Services, GATS) dispose d'une exception spécifique en matière de vie privée. Pour offrir aux nations de plus larges possibilités d'adopter des lois de protection des données, l'article IV du GATS stipule que :

> Rien dans le présent Accord ne sera interprété comme empêchant l'adoption ou l'application par tout Membre de mesures . . . (c) nécessaires pour assurer le respect des lois et règlements qui ne sont pas incompatibles avec les dispositions du présent Accord, y compris celles relatives à : . . . (ii) la protection de la vie privée des personnes concernant le traitement et la diffusion de données à caractère personnel et la protection de la confidentialité des dossiers et des comptes individuels.

Ce langage fournit une protection juridique importante contre l'allégation qu'un système de protection des données viole le GATS ou le système de libre-échange en général.

[113] L'exception de protection des données est toutefois limitée. L'article XIV indique également que l'exception est soumise « à la condition que ces mesures ne soient pas appliquées de manière à constituer soit *un moyen de discrimination arbitraire ou injustifiable entre des pays où des conditions similaires existent*, soit une restriction déguisée au commerce des services. » (soulignement ajouté).

[114] Il existe une question factuelle quant à savoir ce qui constitue « une discrimination injustifiable entre des pays où des conditions similaires existent. » Cependant, à mon avis, ce langage du GATS fournit une autre raison de considérer dans quelle mesure les garanties américaines peuvent être comparées à celles de l'UE et à d'autres pays, comme les pays du BRIC. Comme nous l'avons vu dans le chapitre 6, la conclusion de l'équipe d'Oxford affirmant que les États-Unis constituaient une « référence » pour de telles garanties soulève une difficulté au regard du GATS lorsque des États membres de l'UE présentent des garanties moins complètes. En outre, l'inquiétude au sujet de la « discrimination injustifiable » ne semble pas

[191] PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 188-96 (1998).

s'appliquer si des transferts ont été autorisés vers les pays du BRIC ou vers d'autres pays mais pas aux États-Unis.[192]

[115] Une conclusion d'inadéquation catégorique sur les garanties américaines contre la surveillance soulève donc le risque d'effets économiques importants en raison de l'élimination des transferts légaux, lesquels sont, selon les institutions de l'UE, d'une importance vitale, et aussi en raison des sanctions pouvant résulter d'une violation de traité en vertu du GATS.

V. Sécurité nationale

[116] Pour le bien-être économique, les institutions européennes ont fortement appuyé la relation UE/États-Unis dans les domaines de la sécurité nationale, de l'application et de l'échange d'informations à des fins de renseignement. La Commission de l'UE a déclaré que : « L'Union européenne et les États-Unis sont des partenaires stratégiques, et ce partenariat est essentiel pour la promotion de nos valeurs communes, pour notre sécurité et pour notre leadership dans le commerce mondial. »[193] Les flux de données « sont un élément important et nécessaire » de cette alliance, non seulement pour des raisons économiques, mais également comme « un élément essentiel de coopération UE-États-Unis dans le champ de l'application de la loi. »[194] Les flux de données sont également essentiels pour « la coopération entre les États membres et les États-Unis dans le domaine de la sécurité nationale. »[195]

[117] La « Directive de partage des informations » publiée cette année par l'UE est une indication récente et claire de l'importance de la relation UE/États-Unis dans la lutte contre la criminalité internationale et le terrorisme.[196] Cette Directive régit l'échange d'informations avec des pays non-membres de l'UE pour la lutte contre le terrorisme et à des fins d'application de la loi. La Directive déclare que la « libre circulation » des données vers des pays tiers tels que les États-Unis « devrait être facilitée » pour « la prévention de menaces sur la sûreté publique. »[197] À la suite de cette Directive, l'UE et les États-Unis ont signé l'Umbrella Agreement (abordé plus haut) régissant le partage des données avec les États-Unis à ces fins. Le Ministre néerlandais qui a signé l'Umbrella Agreement au nom de l'UE a déclaré que l'Accord « symbolise les valeurs

---

[192] Une autre réflexion concerne l'effet possible des dispositions de « nation la plus favorisée » (most favored nation, NPF) en vertu de traités commerciaux internationaux. Le problème se posera lorsque des États membres seront tenus de fournir les mêmes opportunités commerciales à un partenaire NPF (comme les États-Unis), mais en fournissant aux États-Unis moins d'accès aux marchés de l'UE que des pays présentant moins de garanties contre la surveillance.

[193] European Commission, *Communication from the Commission to the European Parliament and the Council*, COM (2013) 846, at 2 (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[194] *Id.*

[195] *Id.*

[196] *Voir* Directive (EU) 2016/680 du 27 avril 2016 sur la protection des personnes physiques à l'égard du traitement de données à caractère personnel par des autorités compétentes aux fins de la prévention, de la recherche, de la détection ou de la poursuite des infractions pénales ou de l'exécution des peines, sur la libre circulation de ces données, et abrogeant la Décision-cadre du Conseil 2008/977/JHA, http://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.

[197] *Id.* at Recital (4).

partagées par les États-Unis et l'UE »,[198] et l'Accord lui-même décrit les flux de données comme « essentiels pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris en matière de terrorisme. »[199]

[118] Un soutien similaire pour le partage entre l'EU et les États-Unis et la sécurité nationale découle d'obligations des États membres en matière de sécurité nationale, par exemple en vertu de l'Organisation du Traité de l'Atlantique Nord (OTAN). En vertu de l'article 3 du Traité de l'Atlantique Nord, les membres « maintiennent et développent leur capacité individuelle et collective de résistance à une attaque armée » par le biais d'« un développement personnel et d'une aide mutuelle continue et efficace. »[200] La cybersécurité et la cyberdéfense illustrent l'importance de l'échange d'information : « Nous continuerons à intégrer la cyberdéfense dans les opérations de l'OTAN et dans la planification opérationnelle et d'urgence, tout en améliorant le partage des informations et la conscience de la situation entre Alliés. »[201] Des relations similaires de sécurité nationale pour l'échange d'informations existent entre des agences de renseignement, y compris, mais sans s'y limiter, les pays de l'alliance Five Eyes.[202]

[119] Le partage d'informations pour des raisons de sécurité nationale et de sûreté publique est important dans la lutte contre les attaques terroristes comme celles qui ont frappé Bruxelles, Paris et d'autres lieux dans un passé récent. Le rapport de notre Groupe d'étude a traité en détail pourquoi le partage d'informations sur des personnes est particulièrement important dans la lutte contre les menaces terroristes.[203] Aujourd'hui, les citoyens ordinaires aussi bien que les terroristes utilisent en grande partie les mêmes appareils, logiciels et réseaux informatiques, et la surveillance des personnes suspectées de terrorisme a souvent lieu sur les réseaux utilisés par des citoyens ordinaires. En revanche, pendant la guerre froide, les principales menaces provenaient de pays tels que l'Union soviétique, avec une probabilité beaucoup plus faible de surveillance des communications de citoyens ordinaires. Cette convergence des systèmes de communication utilisés par des terroristes présumés et d'autres personnes est un facteur important, à mon avis, de ce qui est « nécessaire dans une société démocratique » pour faire face aux menaces terroristes actuelles.

---

[198] *Voir* European Council, Press Release 305/16, Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign "Umbrella agreement," (June 2, 2016), http://www.consilium.europa.eu/en/press/press-releases/2016/06/02-umbrella-agreement/ (remarques du Ministre néerlandais Ard van der Steur qui a signé l'Umbrella Agreement au nom de l'UE).

[199] *Voir* Umbrella Agreement, *supra* note 70, at Recital 1, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

[200] The North Atlantic Treaty, Washington, D.C., April 4, 1949, U.N.T.S. 243, http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[201] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, Art. 73, September 5, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[202] Une source publique d'informations concernant les activités de partage de renseignement de ces cinq pays est DAVID ANDERSON, A QUESTION OF TRUST: A REPORT OF THE INVESTIGATORY POWERS REVIEW PRESENTED TO THE PRIME MINISTER PURSUANT TO SECTION 7 OF THE DATA RETENTION AND INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT (June 2015) (UK), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

[203] REVIEW GROUP REPORT, *supra* note 10, at 180-187.

[120] En somme, cette discussion montre qu'une conclusion d'inadéquation catégorique créerait des risques importants pour la sécurité nationale et la sûreté publique, irait à l'encontre des politiques claires des institutions de l'UE, et poserait également des problèmes concernant les obligations d'État membre en vertu de traités. Dans une période marquée par des attaques terroristes bien visibles au sein de l'UE, la perturbation de l'échange d'informations soulève également le risque de ne pas pouvoir empêcher de futurs attentats.

PARTIE 5 :
Discussion finale

[121] Ce résumé de témoignage explique que la combinaison de garanties systémiques et de recours individuels aux États-Unis est, à mon avis, clairement efficace et adéquate pour la protection des données à caractère personnel des personnes non américaines. Par ailleurs, la Cour de justice de l'Union européenne (CJUE) a annoncé une norme juridique d'« équivalence essentielle » pour les transferts de données à caractère personnel vers des pays tiers comme les États-Unis. D'après mon examen complet de la législation et de la pratique aux États-Unis, et mes années d'expérience en droit sur la protection des données dans l'UE, ma conclusion est que, dans l'ensemble, les États-Unis offrent de meilleures garanties sur le renseignement concernant les données à caractère personnel que l'UE. Pour être plus précis, les garanties américaines sont au moins « essentiellement équivalentes » à celle de l'Union européenne. Par conséquent, je ne vois pas de fondement en droit ou de fait pour conclure que les États-Unis manquent de protections adéquates, en raison de ses activités de renseignement, pour le transfert de données à caractère personnel vers les États-Unis depuis l'UE.

[122] Ce résumé de témoignage porte sur l'ampleur potentielle d'une décision dans la présente procédure, et fournit des observations pertinentes permettant d'évaluer l'adéquation des protections sur les transferts de données vers les États-Unis. J'examine des questions dans la présente procédure au titre de l'article 8 de la Convention européenne des Droits de l'homme (et de dispositions connexes d'autres instruments juridiques de l'UE). L'article 8 dispose que « [t]oute personne a droit au respect de sa vie privée et familiale. » Il stipule également : « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. » Je réponds également à des considérations similaires en vertu de l'article 7 (droit à la vie privée et familiale), de l'article 8 (droit à la protection des données) et de l'article 47 (droit à un recours effectif) de la Charte.

[123] Au sens de l'article 8 de la Convention, selon mon avis basé sur vingt ans d'expérience en matière de vie privée et des lois et pratiques de surveillance aux États-Unis et à l'international, l'association des garanties systémiques et des recours individuels aux États-Unis entraîne des actions nécessaires qui sont prises « en conformité avec la loi ». À la lumière de ces garanties et des recours mis à la disposition des citoyens de l'UE aux États-Unis, je crois et j'affirme respectueusement que la poursuite des transferts de données à caractère personnel en vertu de clauses contractuelles types est nécessaire dans une société démocratique en vue de

protéger les intérêts vitaux de l’UE, notamment la sécurité nationale, la sûreté publique et le bien-être économique.