Parlement européen

# Du «Safe Harbour» au «Privacy Shield»

## Avancées et insuffisances des nouvelles règles de transfert des données UE–États-Unis

ANALYSE APPROFONDIE

EPRS | Service de recherche du Parlement européen
Auteures: Shara Monteleone et Laura Puccio
**Service de recherche pour les députés**
Janvier 2017 — PE 595.892

FR
(or. EN)

L'arrêt Schrems de la Cour de justice de l'Union européenne (CJUE) d'octobre 2015 a invalidé la décision de la Commission européenne relative au «Safe Harbour» pour le transfert de données UE–États-Unis. La Commission européenne a négocié un nouvel arrangement, appelé «bouclier de protection des données» (Privacy Shield), et ce nouveau cadre de transfert des données UE–États-Unis a été adopté en juillet 2016. Cette publication a pour objectif de présenter le contexte de l'adoption du bouclier de protection des données ainsi que son contenu et les modifications introduites.

PE 595.892
ISBN 978-92-846-0368-8
doi:10.2861/119924
QA-06-16-293-FR-N

Manuscrit original en anglais achevé en janvier 2017.

Traduction achevée en mars 2017.

## Clause de non-responsabilité et droits d'auteur

Le contenu de ce document est de la seule responsabilité de l'auteur et les avis qui y sont exprimés ne reflètent pas nécessairement la position officielle du Parlement européen. Il est destiné aux Membres et au personnel du PE dans le cadre de leur travail parlementaire. Reproduction et traduction autorisées, sauf à des fins commerciales, moyennant mention de la source et information préalable et envoi d'une copie au Parlement européen.

© Union européenne, 2017.

Crédits photo: © vector_master/Fotolia.

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

## RÉSUMÉ

En 2015, dans l'arrêt Schrems, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision de la Commission européenne de l'année 2000 relative à la «pertinence» du régime du Safe Harbour UE–États-Unis permettant le transfert de données à des fins commerciales de l'Union européenne vers les États-Unis d'Amérique. L'une des principales notions qui sous-tend le raisonnement de la Cour est celle de «l'équivalence» entre le niveau de protection existant dans un pays tiers et le système européen de protection des données. La Cour a invalidé la décision relative à la pertinence du Safe Harbour, car celle-ci ne contenait aucune conclusion sur l'existence aux États-Unis de lois et de pratiques limitant les ingérences dans le droit à la vie privée et la protection des données (c'est-à-dire des ingérences de la part des autorités publiques pour des raisons liées à la sécurité), ni sur l'existence d'un recours juridictionnel efficace pour les citoyens. Par conséquent, d'après l'arrêt de la Cour, les lois qui établissent des exceptions (telles que l'adoption de mesures pour des raisons de sécurité) qui peuvent entraîner des conflits avec les droits fondamentaux doivent établir des règles claires et précises concernant la portée et l'application des mesures ainsi que des garanties minimales contre les risques d'abus, y compris l'accès illicite aux données et l'utilisation ultérieure de celles-ci. Cette affirmation a pour corollaire que les dérogations et les restrictions aux règles de protection des données ne doivent être autorisées que si elles sont strictement nécessaires. En outre, si le mécanisme d'autocertification des entreprises basées aux États-Unis peut faire partie d'un système adéquat de protection des données, il doit être accompagné de mécanismes efficaces d'application et de surveillance.

Par conséquent, le cadre du «Safe Harbour», qui était employé par un grand nombre d'entreprises, s'est avéré insuffisant pour assurer le niveau élevé de protection des citoyens européens exigé par le droit européen. Cette invalidation du «Safe Harbour» a créé une incertitude juridique et entraîné la nécessité d'un nouveau régime. Dans le même temps, plus de 4 000 entreprises américaines procédant à des transferts de données sont passées à d'autres outils existants, tels que les règles d'entreprise contraignantes ou les clauses contractuelles types, bien que ceux-ci soient plus contraignants et plus limités.

En conséquence, la Commission européenne et les États-Unis d'Amérique ont négocié en 2016 un nouveau cadre pour l'échange transatlantique des données à caractère personnel connu sous le nom de **bouclier de protection des données (Privacy Shield)**. Ce cadre devait répondre aux treize recommandations de la Commission formulées en 2013 ainsi qu'aux principales préoccupations soulevées par la Cour dans l'arrêt Schrems. Si ce cadre présente des améliorations significatives par rapport au Safe Harbour, certains problèmes doivent encore être réglés sous peine de voir l'incertitude juridique perdurer. C'est la raison pour laquelle le bouclier de protection des données pourrait ne pas résister à d'éventuelles futures plaintes.

## TABLE DES MATIÈRES

1. Introduction ..... 4
2. La politique européenne en matière de transfert de données et l'arrêt Schrems ..... 4
2.1. Niveau élevé de protection des données européennes et pays tiers ..... 4
2.2. Cour de justice de l'Union européenne: l'arrêt Schrems et ses conséquences ..... 6
2.2.1. Compétences des APD ..... 8
2.2.2. Niveau élevé de protection des données ..... 8
2.2.3. Dérogations afin de garantir l'application de la législation ..... 9
2.3. La transition à la suite de l'arrêt Schrems ..... 12
2.4. Réactions à la suite de l'arrêt Schrems ..... 15
3. Bouclier de protection des données: un long cheminement ..... 18
3.1. La première décision d'adéquation de la Commission et les nouveaux «principes de protection de la vie privée» ..... 18
3.2. Avis, analyses et réactions à la première version du bouclier de protection des données ..... 19
4. Révision du bouclier de protection des données ..... 23
4.1. Principes de protection de la vie privée et obligations des entreprises ..... 25
4.2. De nouvelles procédures de recours ..... 28
4.3. Les nouveaux engagements et procédures de surveillance des autorités américaines ..... 31
4.3.1. Le ministère américain du commerce ..... 31
4.3.2. Commission fédérale du commerce ..... 32
4.3.3. Services de renseignement et application de la loi aux États-Unis ..... 33
5. Vers un outil satisfaisant et durable? ..... 36
5.1. Réactions à la nouvelle version du bouclier de protection des données ..... 36
5.1.1. Défenseurs de la vie privée ..... 37
5.1.2. Groupe de travail «article 29» et Contrôleur européen de la protection des données ..... 38
5.2. Perspectives ..... 40
6. Principales références ..... 42

**Liste des principaux acronymes utilisés**

| | |
|---|---|
| **APD:** | autorités chargées de la protection des données (Union européenne) |
| **BPD:** | bouclier de protection des données |
| **CC:** | clauses contractuelles |
| **CCT:** | clauses contractuelles types |
| **CDF:** | charte des droits fondamentaux de l'Union européenne |
| **CE:** | Commission européenne |
| **CEDH:** | Cour européenne des Droits de l'homme |
| **CEPD:** | Contrôleur européen de la protection des données |
| **CJUE:** | Cour de justice de l'Union européenne |
| **DoC:** | Department of Commerce (ministère américain du commerce) |
| **DPD:** | directive sur la protection des données |
| **FISA:** | Foreign Intelligence Surveillance Act (loi sur la surveillance et le renseignement étranger) |
| **FOIA:** | Freedom of Information Act (loi sur la liberté de l'information) |
| **FTC:** | Federal Trade Commission (commission fédérale américaine du commerce) |
| **GT art. 29:** | groupe de travail «article 29» |
| **JDR:** | Judicial Redress Act (loi sur le recours juridictionnel) |
| **PCLOB:** | Privacy and Civil Liberties Office Board (conseil de surveillance de la vie privée et des libertés civiles) |
| **REC:** | règles d'entreprise contraignantes |
| **RGPD:** | règlement général sur la protection des données |
| **SH:** | Safe Harbour |

# 1. Introduction

Le 6 octobre 2015, dans l'arrêt Schrems contre Data Protection Commissioner, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision n° 2000/520/CE[1] de la Commission européenne relative à la pertinence de la protection assurée par les principes du «Safe Harbour» dans le cadre du transfert de données à caractère personnel de l'Union européenne aux États-Unis. Dans cet arrêt, la Cour a également établi que les pouvoirs d'enquête des autorités nationales chargées de la protection des données ne sont pas limités par l'existence d'une décision d'adéquation de la Commission. Par conséquent, le cadre du «Safe Harbour» s'est avéré insuffisant pour assurer la protection des citoyens européens considérant l'exigence imposée par le droit européen de respecter un niveau élevé de protection lorsque les données sont transférées à l'extérieur de l'espace économique européen (EEE). Dès lors, un nouveau cadre régulant les flux transatlantiques de données devenait impératif.

Un nouveau cadre remplaçant le Safe Harbour, le bouclier de protection des données, et l'adoption par la Commission de la décision d'adéquation y relative le 12 juillet 2016 font partie des évolutions récentes de la politique de l'Union européenne et des relations UE–États-Unis. Ces évolutions, ainsi que leurs conséquences pour les entreprises, pour les citoyens et pour les institutions de l'Union, sont examinées dans l'analyse qui suit.

# 2. La politique européenne en matière de transfert de données et l'arrêt Schrems

## 2.1. Niveau élevé de protection des données européennes et pays tiers

La directive européenne sur la protection des données (DPD) 95/46/CE[2] (et le règlement général sur la protection des données[3] qui la remplacera à partir de 2018) vise à encourager une circulation libre et cohérente des données à caractère personnel tout en protégeant les droits individuels des personnes concernées.

Un niveau élevé de protection est assuré dans la mesure où les transferts de données à l'extérieur de l'Union/EEE ne sont autorisés que si les pays tiers garantissent un niveau de protection **adéquat** (article 25 de la DPD). La Commission européenne peut considérer, par une décision dite «d'adéquation», qu'un pays tiers assure un niveau de protection adéquat. Ce caractère adéquat doit être apprécié «au regard de toutes les circonstances» relatives au transfert, y compris la législation nationale, les accords internationaux et «les règles de droit» en vigueur dans le pays tiers en question

---

[1] Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de protection de la vie privée du «Safe Harbour» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441].

[2] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

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

(article 25, paragraphe 2, DPD)[4]. Dès lors, la décision d'adéquation suppose d'évaluer l'existence dans le pays tiers d'un cadre juridique de protection des données offrant des garanties et des recours semblables à ceux de l'Union européenne.

**Encadré 1 — Procédure d'adoption d'une décision d'adéquation**

La Commission européenne évalue le niveau de protection des données dans le pays tiers au moyen d'une procédure d'examen (conformément à l'article 25, paragraphe 6, et à l'article 31, paragraphe 2, de la DPD). La proposition de la Commission est approuvée, conformément à la nouvelle procédure de comité, au sein du comité de l'article 31 composé de représentants des États membres[5]. La décision du comité est fondée sur un avis émis par les autorités nationales chargées de la protection des données et par le Contrôleur européen de la protection des données (CEPD). La Commission peut appliquer la mesure proposée si elle obtient une majorité qualifiée en faveur de sa proposition. Le collège des commissaires adopte formellement la décision d'adéquation. Le Parlement européen et le Conseil doivent être informés simultanément des mesures prises en comité (droit d'information) et peuvent demander à la Commission de maintenir, de modifier ou de retirer une décision d'adéquation à tout moment s'il est estimé que celle-ci dépasse les compétences d'exécution conférées à la Commission par la directive (droit de regard).

Sur cette base, la Commission a publié la **décision d'adéquation 2000/520/CE** (ci-après «décision d'adéquation du "Safe Harbour"») indiquant que le cadre du «Safe Harbour» arrêté par le ministère américain du commerce (DoC) était adéquat et permettait les transferts de données à caractère personnel de l'Union européenne vers les États-Unis. Cette décision autorisait en particulier les entreprises à transférer des données sans exiger aucune évaluation spécifique du système américain de protection des données, simplifiant ainsi leur application des exigences européennes en matière de protection des données[6].

**Encadré 2 — Ancien régime de protection dit «Safe Harbour»**

Les responsables du traitement des données aux États-Unis se conformant aux principes du «Safe Harbour»[7] étaient considérés comme offrant une protection adéquate et le transfert de données vers ces entreprises était donc autorisé au titre de l'article 25 de la directive sur la protection des données (DPD). Si le responsable du traitement des données confiait les activités de traitement à un sous-traitant, il devait s'assurer de l'existence de garanties en matière de protection des données dans les obligations contractuelles souscrites avec l'entreprise sous-traitante. En dernière analyse, aux termes des principes du «Safe Harbour», le responsable du traitement des données restait juridiquement responsable du traitement des données. Les

---

[4] Voir directive sur la protection des données, article 25, paragraphe 5: «La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4 [niveau inadéquat]», et article 25, paragraphe 6: «La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat [...] en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.»

[5] Voir article 5 du règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission, JO L 55 de 28.2.2011, p. 13.

[6] Consultez le site internet de la direction générale de la justice pour obtenir la liste complète des décisions d'adéquation de la Commission (en anglais).

[7] Issuance of SH principles and transmission to European Commission (Publication des principes de le Safe Harbour et transmission à la Commission européenne), Registre fédéral américain, 24 juillet 2000 et 19 septembre 2000.

principes du «Safe Harbour» n'étaient pas obligatoires: les entreprises y souscrivaient volontairement. Pour ce faire, elles procédaient à une autocertification, déclarant qu'elles se conformaient aux principes du «Safe Harbour». Les entreprises qui ne procédaient pas annuellement à une autocertification ne pouvaient plus apparaître dans la liste des participants et ne pouvaient plus bénéficier des avantages du «Safe Harbour». La validité des autocertifications était vérifiée par le ministère américain du commerce, qui tenait également à jour la liste des entreprises disposant de certifications valides[8].

Le contrôle du respect des règles revenait à la commission fédérale du commerce (FTC) et seules les entreprises relevant de la compétence de la FTC pouvaient participer au «Safe Harbour»[9]. En effet, les principes du «Safe Harbour» revenant à des promesses faites aux clients, le non-respect de ces promesses s'apparentait à une pratique déloyale et trompeuse au sens de la section 5 de la loi sur la Commission du libre-échange[10].

La Commission européenne a reconnu «l'inadéquation» de plus en plus évidente du «Safe Harbour» à partir de 2013. Dans un examen du cadre du «Safe Harbour» mené en 2013 par la Commission[11], les problèmes suivants concernant le contrôle et l'application des principes du «Safe Harbour» ont été détectés: a) une transparence parfois déficiente des pratiques en matière de respect de la vie privée des entreprises du «Safe Harbour», bien qu'il s'agisse d'un élément important permettant d'assurer la force exécutoire par l'intermédiaire de la section 5 de la loi sur la Commission du libre-échange; b) le manque de suivi et de vérification appropriés de la validité de la certification du Safe Harbour, ainsi que du respect effectif des principes; c) l'accès limité aux mécanismes de recours.

Le 6 octobre 2015, la Cour de justice de l'Union européenne (CJUE) a **invalidé** la décision d'adéquation du «Safe Harbour», rendant impérative la nécessité d'adopter un nouveau cadre pour le transfert de données entre l'Union et les États-Unis.

## 2.2. Cour de justice de l'Union européenne: l'arrêt Schrems et ses conséquences

À la lumière des révélations d'Edward Snowden[12] en 2013 concernant les programmes de surveillance de masse (le programme PRISM par exemple) de l'agence nationale de

---

8 Les services de télécommunication faisaient l'objet d'une exception au titre du Federal Trade Commission Act (loi sur la Commission du libre-échange) et ne pouvaient donc pas participer au cadre d'autocertification de le Safe Harbour. Les services de transport participant à le Safe Harbour étaient contrôlés par le ministère des transports.

9 La FTC n'est pas toujours l'autorité responsable. L'autorité légale primaire de la FTC découle de la section 5 de la loi sur la Commission du libre-échange qui interdit les pratiques commerciales déloyales ou trompeuses. La FTC dispose également de l'autorité pour faire respecter tout un éventail de lois spécifiques à certains secteurs (Truth in Lending Act, CAN-SPAM Act, Children's Online Privacy Protection Act, Equal Credit Opportunity Act, Fair Credit Reporting Act, Fair Debt Collection Practices Act et Telemarketing and Consumer Fraud and Abuse Prevention Act par exemple). D'autres lois garantissent le respect de la vie privée dans des secteurs tels que les services de santé et les télécommunications et dans certains secteurs financiers et des assurances qui ne relèvent pas des compétences de la FTC mais de celles d'autres ministères ou commissions. Concernant les affaires englobées dans le cadre de le Safe Harbour par la commission fédérale du commerce, voir également: C. J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge University Press, 2016, concernant les travaux de la FTC en matière de protection des données.

10 15 US Code §45

11 Communication de la Commission au Parlement européen et au Conseil Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique, COM(2013) 846 final du 27.11.2013; communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de le Safe Harbour du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM(2013) 847 final du 27.11.2013.

12 E. Macaskill et G. Dance, «NSA files: decoded», *The Guardian*, 1er novembre 2013.

sécurité américaine (NSA)[13] ainsi que la collaboration dissimulée de cette dernière avec des entreprises internet, un avocat autrichien spécialisé dans les libertés individuelles, Max Schrems, a déposé une plainte auprès de l'autorité irlandaise chargée de la protection des données (APD), mettant en doute la légalité du transfert de données vers les États-Unis d'Amérique à partir de l'hypothèse que toutes les données des abonnés européens de Facebook sont régulièrement transférées vers des serveurs situés aux États-Unis. En particulier, en invoquant les pouvoirs d'enquête de l'APD irlandaise[14], M. Schrems a argué que la législation et la pratique américaines n'offraient pas une protection adéquate **contre les risques de surveillance de masse** des citoyens européens (conformément à la DPD). Le commissaire irlandais chargé de la sécurité des données a rejeté cette plainte au motif que les transferts de données entre l'Union européenne et les États-Unis se basaient sur la décision d'adéquation contraignante de la Commission concernant le Safe Harbour.

Cette affaire a été portée devant la Haute Cour de justice irlandaise en vue d'un contrôle juridictionnel. La Haute Cour s'est à son tour tournée vers la CJUE pour une décision préjudicielle, mettant ainsi en question la légalité du cadre du «Safe Harbour» dans lequel le transfert avait lieu[15]. En d'autres termes, la Haute Cour de justice irlandaise a demandé si l'existence de la décision d'adéquation du «Safe Harbour» interdisait à une APD de procéder à une enquête à la suite d'une plainte.

Dans son arrêt Schrems contre Data Protection Commissioner[16], la CJUE, siégeant en grande chambre, a confirmé les conclusions de l'avocat général Bot[17] et est même allée au-delà des demandes de M. Schrems et de la Cour irlandaise en statuant d'office que:

1) les APD nationales sont compétentes pour examiner la plainte d'une personne [comme le prévoient la DPD et la charte des droits fondamentaux de l'Union européenne (CDF)]; cette compétence n'est pas limitée par l'existence d'une décision d'adéquation de la Commission;

---

[13] Sur cette question, le Parlement européen a adopté une série de résolutions dans lesquelles il a demandé de façon répétée la suspension de le Safe Harbour et a demandé instamment à la Commission d'agir immédiatement afin d'assurer une protection efficace des données dans le cadre des transferts vers les États-Unis; voir la résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union; résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures; et résolution du 29 octobre 2015 sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne.

[14] L'APD irlandaise était compétente dans la mesure où l'intermédiaire européen de Facebook était Facebook Ireland. Les documents relatifs aux différentes procédures administratives et judiciaires sont publiés par *Europe v Facebook*.

[15] La Haute Cour irlandaise, en demandant une décision préjudicielle de la CJUE, a posé les questions suivantes: «Eu égard aux articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne et sans préjudice des dispositions de l'article 25, paragraphe 6, de la directive [95/46/CE], [le commissaire] saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence les États-Unis d'Amérique) dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée est-il absolument lié par la constatation contraire de l'Union contenue dans la décision [2000/520/CE]? Dans le cas contraire, peut-il ou doit-il mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la [décision 2000/520/CE]?»

[16] Arrêt 362/14 *Maximilian Schrems* contre *Data Protection Commissioner*, du 6 octobre 2015.

[17] Consultez les conclusions de l'avocat général Bot présentées le 23 septembre 2015.

2) les conclusions de la Commission concernant le régime volontaire de Safe Harbour figurant dans la décision d'adéquation étaient insuffisantes pour garantir la protection des données des citoyens européens aux États-Unis d'Amérique;
3) les dérogations pour motif de sécurité devraient être strictement nécessaires et proportionnelles.

La Cour a donc, en tant que seule autorité habilitée à le faire, déclaré que la décision d'adéquation concernée de la Commission était invalide. Les principaux passages de l'arrêt sont analysés dans les sections suivantes.

2.2.1. *Compétences des APD*

Les autorités nationales de contrôle sont habilitées à examiner la légalité des transferts de données de l'Union européenne vers un pays tiers même s'il existe une décision de la Commission concernant le niveau de protection assuré dans ce pays. Comme Steve Peers l'a noté[18], la Cour a fondé ses conclusions sur les compétences et sur l'indépendance de ces autorités telles que consacrées dans la DPD, lue à la lumière de la charte des droits fondamentaux de l'Union, qui fait expressément état du rôle et de l'indépendance des APD[19]. Analysant cette question dans le cadre de l'architecture du système de protection des données au regard des transferts externes, la Cour a confirmé que, si les APD sont liées par la décision de la Commission et ne peuvent la déclarer invalide (seule la CJUE a cette compétence afin d'éviter une fragmentation du droit européen), elles peuvent néanmoins examiner une affaire lorsqu'une plainte a été déposée. De plus, si la plainte est fondée, les APD peuvent la porter devant les tribunaux nationaux, conformément au droit national, afin d'obtenir le renvoi de la question devant la CJUE[20].

2.2.2. *Niveau élevé de protection des données*

Comme indiqué ci-dessus, la Cour a statué que la décision d'adéquation de la Commission relative au «Safe Harbour» était invalide parce que la façon dont les ingérences dans les droits fondamentaux seraient limitées au strict nécessaire aux États-Unis ne ressortait pas de cette décision.

En cela, la CJUE a souligné la nécessité d'interpréter l'exigence de protection adéquate au titre de la DPD comme **substantiellement équivalente** à celle garantie dans l'Union européenne, conformément aux objectifs de la directive d'assurer un niveau élevé de protection couvrant les données à caractère personnel transférées à l'extérieur de l'Union (sans quoi ces exigences seraient aisément contournées)[21]. En outre, selon la Cour, cette exigence doit être lue à la lumière de la charte des droits fondamentaux de l'Union qui protège le droit au respect de la vie privée (article 7), le droit à la protection des données (article 8) et le droit à un recours judiciaire effectif (article 47), et qui, ainsi qu'il a été noté, confère aux APD nationales des compétences de contrôle. Cela suppose également une évaluation continue des règles et des pratiques des pays tiers en matière de garanties, conditions au transfert de données, c'est-à-dire une évaluation dynamique,

---

[18] S. Peers, *The party is over: EU data protection law after Schrems SH judgment*, EU law analysis Blog, 7 octobre 2015.

[19] Le nouveau règlement (RGPD) étend ces compétences et cette indépendance (article 51 et suivants).

[20] Voir également A. Azoulai et M. van der Sluis, «Institutionalizing personal data protection in times of global institutional distrust: Schrems», *Common Market Law Review* 53, p. 1343, 2016.

[21] Concernant la notion d'extraterritorialité (et la nécessité de déterminer les limites de l'application de la législation européenne de protection des données, voir C. Kuner, «Extraterritoriality and regulation of international data transfers in EU data protection law», *International Data Privacy Law* (2015), 5 (4).

caractérisée par des examens réguliers, de sorte que l'évolution des circonstances après l'adoption de la décision soit prise en compte[22].

**Encadré 3 — L'arrêt Schrems: dans le prolongement de la jurisprudence de la Cour de justice de l'Union européenne**

L'arrêt Schrems entre dans le cadre d'une jurisprudence cohérente et de plus en plus volumineuse de la CJUE, ce qui souligne l'importance accordée à un niveau élevé de protection des données à caractère personnel (affaires Google Spain et Digital Rights Ireland Ltd par exemple)[23]. Plus particulièrement, certaines questions traitées dans l'arrêt Digital Rights Ireland Ltd ont formé la base des arguments ultérieurement développés par la Cour dans l'arrêt Schrems[24]. Dans l'arrêt Digital Rights Ireland Ltd, la Cour a examiné la validité de la directive sur la conservation des données à la lumière des articles 7, 8 et 11 de la charte des droits fondamentaux et a statué que la conservation autorisée par cette directive représentait une ingérence particulièrement grave dans les droits consacrés dans ces articles (mais toutefois insuffisante pour toucher à leur essence même, car la directive n'autorisait pas l'acquisition du contenu des communications électroniques). Si l'objectif de la directive sur la conservation des données (la lutte contre la grande criminalité) est considéré comme légitime par la Cour, la conservation doit être strictement nécessaire pour représenter une limitation juridiquement justifiable du droit reconnu à l'article 7 de la charte[25].

Dans la même veine, la Cour a constaté dans l'arrêt Schrems que la décision d'adéquation ne concluait pas que les ingérences dans les droits fondamentaux (bien qu'elles aient des motifs légitimes) seraient limitées au strict nécessaire. En revanche, elle a autorisé les transferts, le stockage et l'utilisation ultérieurs des données sans fixer de critères objectifs permettant de déterminer les limites, les différenciations, les exceptions et les motifs spécifiques associés.[26]

### 2.2.3. *Dérogations afin de garantir l'application de la législation*

Les principes du «Safe Harbour»[27] n'étaient pas obligatoires. Comme la CJUE l'a confirmé, le système d'autocertification ne représente pas un problème en soi tant que des garanties adéquates et des mécanismes efficaces de contrôle et de sanction sont en place dans le pays tiers à l'égard de toute violation éventuelle des règles européennes relatives à la protection des données. De manière cruciale, le nombre de dérogations

---

[22] Voir S. Peers, qui a souligné que la décision de la Commission a été déclarée invalide en vertu de l'importance du droit à la protection des données dans l'Union européenne (qui sera affecté). Voir également S. Rodota, «Internet e-privacy, *c'e' un giudice in Europa che frena gli USA*», *La Repubblica*, 12 octobre 2015, qui a souligné que, «face à une politique repliée sur la seule économie, ce sont les juges qui cherchent à maintenir l'Europe des droits en vie».

[23] C-131/12 et affaires jointes C-293/12 et C-594/12; voir également l'arrêt récent dans les affaires jointes C-203/15 et C-698/15 (*Tele2 Sverige* et *Watson e. a.*).

[24] Dans ce sens, voir E. Ustaran et H. Lovells, «The Privacy Shield explained», partie 2, dans *Privacy & Data Protection Journal* 2016, vol. 16, n° 7, juillet/août 2016.

[25] La Cour a précisé les exigences s'appliquant à toute mesure pour que celle-ci soit considérée comme une ingérence légale dans le droit à la vie privée (exigences par ailleurs jugées absentes de la directive sur la conservation des données), par exemple: a) des règles claires et précises, c'est-à-dire des indications suffisantes pour garantir la protection effective des données à caractère personnel conservées contre les risques d'accès illicite ou d'abus; b) des limites à l'accès aux données: de manière cruciale, la directive sur la conservation des données n'établissait aucune limite ni à l'accès des autorités nationales aux données conservées, ni à l'utilisation de ces données; en d'autres termes, elle n'établissait aucune limite à l'*ampleur* de l'ingérence dans les droits fondamentaux.

[26] Arrêt *Schrems*, point 93.

[27] Voir, par exemple, S. Carrera et E. Guild, *Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment*, publications du CEPS, 12 novembre 2015.

envisagées dans le cadre des principes du «Safe Harbour»[28], telles que les dérogations afin d'assurer le respect de la législation ou pour motif de sécurité nationale[29], et la façon dont celles-ci étaient appliquées (c'est-à-dire en l'absence de limites appropriées), comptaient parmi les questions essentielles de l'arrêt Schrems. Si les dérogations pour ces motifs sont en principe légitimes, la décision d'adéquation de la Commission relative au «Safe Harbour» ne contenait aucun élément indiquant que l'application par les États-Unis de ces dérogations serait complétée, à l'égard des citoyens européens, par des garanties suffisantes contre les risques d'abus, d'accès illicite à ces données ou d'utilisation illicite de celles-ci. En d'autres termes, la décision d'adéquation n'a pas vérifié que les ingérences dans les droits fondamentaux seraient limitées au strict nécessaire[30].

**Encadré 4 — Les services répressifs et de renseignement américains et l'arrêt Schrems**

Dans l'arrêt Schrems, la Cour a estimé que la décision d'adéquation était dénuée de toute considération concernant les limitations du pouvoir des services de renseignement et des services répressifs dans l'accès aux données des entreprises, concernant les dispositifs de surveillance et concernant des mécanismes efficaces de recours en cas de plainte. Comme Montelero l'a noté[31], le principal défaut de la décision d'adéquation de la Commission était de ne reconnaître le caractère adéquat du «Safe Harbour» que sur la base de l'existence de l'accord (un «compromis»), sans prendre en compte l'ampleur des exceptions envisagées, ce qui signifie que ces dernières auraient prévalu sur les obligations des entreprises découlant du «Safe Harbour». La Cour a dès lors exigé de la Commission qu'elle procède à une évaluation de la mise en œuvre de ces dérogations en prenant en compte toutes les circonstances (article 25 de la DPD), en particulier la situation de l'état de droit aux États-Unis, et en raison de sa législation interne ou de ses engagements internationaux. Une attention particulière a donc aussi été portée, après l'arrêt Schrems, aux possibilités offertes aux services répressifs et de renseignement d'accéder aux données, ainsi qu'aux dispositifs de recours, dans la législation et les pratiques américaines.

---

[28] Voir A. Montelero, «I flussi di dati transfrontalieri e le scelte delle imprese tra SH e Privacy Shield», G.Resta - V. Zeno-Zencovich (éds), *La protezione transnazionale dei dati personali*. *Dai «SH Principles» al «Privacy Shield»*, Roma Tre Press, 2016, p. 240, livre numérique, qui souligne [traduction de l'auteur] que le motif sous-tendant l'invalidation de le Safe Harbour réside avant tout dans son anomalie», c'est-à-dire dans la nature exceptionnelle du compromis politico-économique qui a permis (nonobstant les conditions imposées par l'article 26 de la DPD européenne) la croissance des flux de données entre les entreprises européennes et américaines. Ceux-ci, toutefois, ne peuvent plus être limités aux frontières nationales. Dans certains cas, les entreprises et les gouvernements des pays tiers estiment qu'il est plus commode d'adopter les normes européennes que d'entrer dans des négociations complexes sur les transferts de données. Les pouvoirs économiques et politiques américains n'étaient pas dans ce cas, ce qui expliquerait le «compromis» que représente le Safe Harbour. Toutefois, en conséquence de l'arrêt Schrems, la mécanique politique des deux côtés de l'Atlantique s'est immédiatement mise en marche pour produire un nouvel accord (peut-être temporaire), en prévision également d'une réforme de la protection des données et du renseignement aux États-Unis à laquelle sont favorables autant les consommateurs que les entreprises.

[29] Le Safe Harbour précisait que «l'adhésion à ces principes peut être limitée par: a) les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis; ...».

[30] Voir les commentaires de D. Solove, «Sunken Safe Harbor: 5 Implications of Schrems and US-EU Data Transfer», *TechPrivacy*, 13 octobre 2015. Selon lui, tandis que les pays de l'Union européenne pratiquent également la surveillance à grande échelle («il y a donc ici une certaine hypocrisie»), l'attitude américaine de consentement face à ce pouvoir étendu de surveillance du gouvernement sans voies de recours judiciaires substantielles (c'est-à-dire le fait que la NSA peut pratiquer une surveillance massive et que personne ne peut contester cette surveillance) caractérise un pouvoir d'une arrogance inacceptable pour l'Union européenne.

[31] A. Montelero, *op. cit.*, note de bas de page 28.

L'une des conséquences de l'arrêt Schrems[32] dans le système juridique américain a précisément été la reprise du débat autour du **Judicial Redress Act (JRA)** (loi sur le recours juridictionnel) au Congrès[33]. Une attention particulière a été portée à l'adoption du JRA américain car celui-ci permet aux citoyens de pays ou d'organisations économiques régionales (y compris l'Union européenne), dont la liste est établie par le ministère de la justice, d'accéder à des mécanismes de recours en cas d'allégation d'utilisation abusive de données à caractère personnel traitées dans le cadre des accords de transfert de données UE–États-Unis. Plus précisément, il autorise «des actions civiles en vertu du Privacy Act de 1974 à l'encontre de certains organismes gouvernementaux des États-Unis en vue d'accéder à des données transférées vers les États-Unis depuis un pays étranger, de modifier ces données ou d'introduire un recours pour divulgation illicite de ces données afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière» (section 2). Les institutions de l'Union européenne ont notamment considéré l'adoption du **Judicial Redress Act** (finalement adopté en février 2016) comme une condition préalable à la conclusion de **l'accord-cadre**[34] (*umbrella agreement*) sur le transfert de données aux États-Unis à des fins d'application de la loi[35], qui fait en sorte «que le partage d'informations se base, pour la première fois, sur la protection des données[36]».

De plus, le US Freedom Act de 2015, qui a modifié des lois américaines antérieures, a interdit la collecte massive des métadonnées de télécommunication par les organismes de renseignement (comme la NSA) et introduit certaines exigences de transparence. Cette limitation de la collecte massive de métadonnées, combinée aux restrictions imposées au renseignement d'origine électromagnétique vis-à-vis des pays étrangers par la **directive politique présidentielle 28** (2014)[37], est, comme expliqué ci-dessous, particulièrement pertinente dans le cadre de l'évaluation par la Commission du nouveau cadre de transfert des données UE–États-Unis. Dans le même temps, différents observateurs et défenseurs du droit à la vie privée considèrent que ces mesures législatives ne suffisent ni à résoudre les problèmes de surveillance, ni à offrir des garanties adéquates.

Le Contrôleur européen de la protection des données (CEPD) a relevé que la CJUE interprète dans l'arrêt Schrems les articles 7, 8 et 47 de la charte des droits fondamentaux dans le cadre des transferts de données, articles qui s'appliquent tous aux domaines commerciaux et répressifs. De plus, dans son avis sur l'accord-cadre, le CEPD a considéré les conclusions de l'arrêt Schrems et, tout en saluant les garanties envisagées, a recommandé d'améliorer l'accord-cadre pour que celui-ci puisse être considéré comme conforme au droit primaire de l'Union. Ces améliorations devaient: a) préciser que toutes les garanties s'appliquaient à toutes les personnes

---

32 À l'époque de l'arrêt, seuls les citoyens américains avaient accès à un recours juridictionnel au titre du Privacy Act, même si les États-Unis avaient promis d'adopter une loi améliorant les droits de recours des citoyens européens en vue de protéger leur droit à la vie privée. Conformément à cette promesse, le Judicial Redress Act a été présenté à la Chambre des représentants et au Sénat, respectivement au mois de mars et au mois de juin 2015, avec l'objectif d'étendre les principaux avantages du Privacy Act aux citoyens des principaux alliés des États-Unis, leur accordant par là même des droits de recours au titre de cette loi. Voir également K. Archick et M. Weiss, *US-EU Data Privacy: From Safe Harbor to Privacy Shield*, CRS, mai 2016.

33 Judicial Redress Act de 2015.

34 Voir S. Monteleone, EU-US Umbrella Agreement on data protection, EPRS, 2016.

35 Conformément à l'article 218 du traité FUE, le Parlement européen a donné le 1er décembre 2016 son approbation à la conclusion de cet accord par le Conseil, qui a adopté sa décision d'autorisation le lendemain. Cet accord devrait entrer en vigueur au cours de l'année 2017, lorsque les autorités américaines auront parachevé leurs procédures internes.

36 CEPD, avis préliminaire du 12 février 2016 relatif à l'accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière.

37 Directive politique Obama nº 28/2014, Signals Intelligence activities (opérations de renseignement d'origine électromagnétique) (section 2).

(indépendamment de leur nationalité); b) garantir que les dispositions en matière de recours juridictionnel soient efficaces au sens de la charte des droits fondamentaux; c) préciser que les transferts massifs de données sensibles n'étaient pas autorisés[38].

La CJUE a en particulier souligné que toute réglementation autorisant **l'accès généralisé** des pouvoirs publics aux communications des personnes doit être considérée comme remettant en cause l'essence même du droit fondamental au respect de la vie privée. Dans le même sens, une réglementation qui ne prévoit aucune **voie de recours individuelle** (concernant par exemple le droit d'accès des personnes aux données les concernant et le droit à la rectification ou à la suppression de celles-ci) ne respecterait pas le droit à une protection juridictionnelle effective tel que consacré à l'article 47 de la charte des droits fondamentaux (point 95 de l'arrêt).

Sur ce point, **l'ULD, l'APD du Schleswig-Holstein**, en Allemagne, a été particulièrement critique dans son document exposant sa position sur l'arrêt[39]: «Si les citoyens de l'Union européenne ne bénéficient pas d'un droit effectif à accéder à leurs données à caractère personnel, à être entendus sur la question de la surveillance et de l'interception des communications et à bénéficier d'une protection juridictionnelle, l'article 47 de la charte des droits fondamentaux est violé […] Les États-Unis d'Amérique ne peuvent actuellement pas démontrer qu'ils disposent de moyens efficaces assurant une protection substantiellement équivalente au niveau de protection garanti dans l'Union européenne».

## 2.3. La transition à la suite de l'arrêt Schrems

Les marchés de l'Union européenne et des États-Unis d'Amérique sont extrêmement interconnectés, grâce à des échanges commerciaux annuels d'une valeur supérieure à 1 000 milliards de dollars et des stocks d'investissement dans chaque économie proches de 4 000 milliards de dollars[40]. En 2012, les exportations américaines livrées en ligne dans l'Union européenne se sont élevées à 140 milliards de dollars[41]. Les flux de données croisées peuvent concerner différents aspects de la vie économique ou différents secteurs: les flux de données les plus importants concernent des données concernant les ressources humaines mais ils peuvent également concerner des transactions et des informations concernant les clients ainsi que des données liées à l'innovation et à la recherche et développement, etc.[42] Plus de 4 000 entreprises étaient tributaires de cette

---

38 CEPD, avis préliminaire.

39 Document exposant la position de l'ULD concernant l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015, C-362/14. De plus, l'ULD a relevé que, s'il s'agit là de la situation aux États-Unis d'Amérique et étant donnés les principes européens de protection des données, même d'autres moyens tels que le consentement de la personne concernée ne pouvaient être aisément invoqués comme base juridique car un consentement véritable et librement exprimé nécessite la communication d'informations exhaustives, y compris concernant les risques associés aux larges dérogations accordées aux autorités américaines. En dernière analyse, cela exigerait de l'individu qu'il renonce à l'exercice de ses droits fondamentaux. D'autres agences nationales ont publié leur position sur l'arrêt Schrems. C'est le cas du *garante* italien qui souligne que l'arrêt exige des États membres et des organes de l'Union qu'ils garantissent un respect réel et concret de la charte des droits fondamentaux.

40 O. Maisse et G. Sabbati, *US: Economic indicators and trade with the EU*, EPRS, juillet 2016.

41 *Ibid*.

42 Ces flux peuvent couvrir des transactions d'entreprise à entreprise en ligne (EEL), dans lesquelles les flux de données peuvent provenir de filiales et d'investissements étrangers de part et d'autre de l'Atlantique, ou des transactions commerciales entre entreprises (échange de données de recherche et développement, conseil financier, etc.). Les transferts de données peuvent survenir dans des

décision d'adéquation pour leurs transferts transatlantiques de données. Les petites et moyennes entreprises sont également tributaires du «Safe Harbour» pour les transferts de données croisées[43].

En **invalidant** la décision d'adéquation de la Commission, la CJUE a précisé que les transferts de données vers les États-Unis d'Amérique sur la base des principes du «Safe Harbour» n'étaient plus conformes au droit de l'Union. En conséquence, les entreprises auparavant tributaires du «Safe Harbour» pour leurs transferts transatlantiques de données faisaient face à différents problèmes[44]. Certaines orientations ont été fournies par le groupe de travail «article 29» (GT art. 29), le groupe des APD de l'Union européenne, qui a publié une déclaration concernant l'application de l'arrêt et l'utilisation des autres outils disponibles. La Commission a fait de même dans sa communication de novembre 2015[45].

- Le **premier problème** concernait l'incidence sur les transferts de données effectués au titre du «Safe Harbour» avant l'arrêt de la CJUE. Le GT art. 29[46] a affirmé que les transferts ayant toujours lieu au titre de la décision d'adéquation du «Safe Harbour» après l'arrêt de la CJUE étaient illicites.
- Le **deuxième problème** concernait les instruments toujours à disposition des entreprises pour le transfert des données (voir encadré ci-dessous). Le GT art. 29 a ici considéré que les instruments de transfert existants sont toujours applicables, tels que les règles d'entreprise contraignantes ou les clauses contractuelles types institués par la Commission au titre de la DPD. Le recours au consentement sans ambiguïté de la personne concernée aurait pu constituer une alternative. En effet, en vertu de l'article 26 de la directive sur la protection des données (DPD)[47], lorsqu'il a été constaté qu'un pays tiers n'assure pas un niveau de protection adéquat (ou en l'absence d'une décision d'adéquation), les transferts peuvent toujours avoir lieu sur d'autres bases, c'est-à-dire le consentement de la personne concernée[48], ou si le responsable du traitement des données offre des garanties appropriées, y compris au

---

transactions entre une entreprise et un client, comme dans le cas du commerce électronique. Les transactions à l'échelle mondiale impliquent la transmission de grandes quantités de données sensibles et à caractère personnel. L'incertitude créée par l'invalidation du cadre de le Safe Harbour porte préjudice aux entreprises américaines et européennes des deux côtés de l'Atlantique. Pour différents exemples de transferts transatlantiques de données potentiels, voir: J. P. Meltzer, *Examining the EU SH decision and impacts for transatlantic data flows*, Brookings Institution, novembre 2015. Certaines données concernant le commerce numérique transatlantique sont également disponibles dans une étude publiée par le département thématique du Parlement européen, voir: P. Chase, S. David-Wilp, T. Ridout, *Transatlantic Digital Economy and Data Protection*: *State-of-Play and Future Implications for the EU's External Policies*, direction générale des politiques externes de l'Union, Parlement européen.

43 *Ibid.*

44 Safe Harbour Data Privacy Briefing: Your Questions Answered by Giovanni Buttarelli, Sidley Austin, 20 octobre 2015.

45 Déclaration du groupe de travail «article 29».

46 Le groupe de travail «Article 29» est un organe consultatif indépendant sur la protection des données et la vie privée, institué au titre de l'article 29 de la directive 95/46/CE sur la protection des données.

47 Voir le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (GT 114) du GT art. 29, adopté le 25 novembre 2005, qui considère que les dérogations de l'article 26 doivent être strictement interprétées.

48 D'autres critères pertinents dans un contexte commercial existent qui incluent les transferts nécessaires: à l'exécution d'un contrat en réponse à la demande de la personne concernée; à la constatation, à l'exercice ou à la défense de droits en justice.

moyen de clauses contractuelles. Ces dernières doivent compenser de façon satisfaisante l'absence d'un niveau général de protection adéquate.

- Le **troisième problème** concernait la mise en place d'une période de transition permettant aux entreprises de s'adapter. Le GT art. 29 a accordé un délai de trois mois en précisant que des mesures coercitives coordonnées seraient prises avant la fin du mois de janvier 2016 si aucune solution appropriée n'était trouvée avec les autorités américaines.

**Encadré 5 — Règles d'entreprise contraignantes et clauses contractuelles types**

En l'absence d'un cadre juridique jugé apte à fournir les garanties d'une protection adéquate des données, les entreprises d'un pays tiers désirant utiliser les données en provenance de l'Union européenne peuvent utiliser les instruments alternatifs tels que les règles d'entreprise contraignantes (un code intergroupe de pratiques publié par des entreprises multinationales) ou les clauses contractuelles types (instituées par la Commission au titre de la DPD). Le GT art. 29 a envisagé l'utilisation de ces instruments pour permettre la circulation des données à la suite de l'arrêt Schrems.

*Règles d'entreprise contraignantes*

Les entreprises peuvent décider de se soumettre volontairement aux règles d'entreprise contraignantes mais, comme leur nom l'indique, ces règles, une fois adoptées, sont contraignantes vis-à-vis de l'entreprise qui les a adoptées. La nature contraignante de ces règles doit être claire et suffisante pour garantir le respect des règles à l'extérieur de l'Union européenne/de l'Espace économique européen. Cela signifie qu'une entité juridique au sein de la société doit être responsable en droit européen du respect des règles d'entreprise et peut faire l'objet de mesures coercitives en cas de non-respect[49]. Une telle responsabilité est normalement confiée au siège européen qui doit prendre toutes les mesures nécessaires pour garantir que toutes les composantes étrangères de la société conforment leurs activités de traitement des données aux règles d'entreprise contraignantes. Si le siège du groupe de sociétés ne se trouve pas dans l'Union/EEE, le siège doit déléguer ses responsabilités à une composante de la société basée dans l'Union. Lorsque le groupe peut démontrer pourquoi il ne lui est pas possible de désigner une entité unique dans l'Union/EEE, il peut proposer d'autres mécanismes de responsabilité convenant mieux à son organisation[50].

*Clauses contractuelles et clauses contractuelles types*

Des clauses contractuelles appropriées peuvent également être employées pour garantir une protection adéquate (voir article 26, paragraphe 2, de la DPD). Ces clauses contractuelles doivent exister dans la relation entre le responsable du traitement et la personne concernée, entre le responsable du traitement dans l'UE/EEE et le responsable du traitement à l'extérieur de l'UE/EEE et entre le responsable du traitement et le sous-traitant (si le responsable du traitement confie le traitement à un sous-traitant dans un pays tiers qui ne bénéficie pas d'une protection adéquate des données dans le pays tiers). Ces clauses contractuelles doivent être évaluées par l'APD de l'État membre responsable de l'autorisation du transfert. L'État membre doit signaler à la Commission et aux autres États membres l'autorisation accordée. La Commission ou un autre

[49] En d'autres termes, cela permet aux personnes concernées de déposer une plainte auprès de l'autorité chargée de la protection des données compétente et d'avoir accès à des mécanismes de recours en cas de non-respect des règles d'entreprise contraignantes de la part de la société.

[50] Il serait possible de créer un mécanisme de responsabilité conjointe des importateurs et des exportateurs de données tel que disposé dans les clauses contractuelles types européennes 2001/497/CE (ensemble I) ou de définir un régime alternatif de responsabilité basé sur des obligations de diligence raisonnable tel que prescrit dans les clauses contractuelles types européennes 2004/915/CE (ensemble II). Enfin, il existe une possibilité spécifique aux transferts effectués par les responsables du traitement vers les sous-traitants et qui consiste en l'application du mécanisme de responsabilité des clauses contractuelles types 2002/16/CE.

État membre peut objecter à cette autorisation pour des motifs justifiés relatifs à la protection du respect de la vie privée et d'autres droits fondamentaux.

La Commission peut décider, conformément à la procédure de comité mentionnée à l'article 31, paragraphe 2, de la DPD, que certaines clauses contractuelles types fournissent des garanties appropriées. L'utilisation de ces clauses contractuelles types simplifie la procédure d'autorisation car les États membres doivent se conformer à la décision de la Commission. Les clauses contractuelles types, en tant que modèle établi par la Commission européenne[51], établissent des obligations pour les exportateurs et les importateurs de données concernant par exemple les mesures de sécurité, l'information des personnes concernant le transfert de données sensibles, la notification par l'exportateur des données des demandes d'accès provenant des services répressifs de pays tiers et le droit à l'accès aux données à caractère personnel, à leur rectification ou à leur suppression. Ces clauses doivent également mentionner que les citoyens de l'Union ont la possibilité d'invoquer leurs droits devant une APD ou un tribunal de l'État de l'exportateur des données. Étant donné le caractère contraignant de la décision de la Commission, l'incorporation des clauses contractuelles types dans un contrat signifie que les autorités nationales sont, en principe, tenues d'accepter ces clauses: elles ne peuvent refuser le transfert de données vers un pays tiers. Néanmoins, à la lumière de l'arrêt Schrems, il apparaît que les APD conservent la compétence d'examiner ces clauses conformément au droit européen et qu'elles peuvent, en cas de doute, porter une affaire devant un tribunal national (qui peut à son tour saisir la CJUE d'une décision préjudicielle, comme dans le cas de l'arrêt Schrems). Lorsqu'ils sont soumis à un contrat contenant des clauses contractuelles types, les exportateurs de données et les importateurs dans un pays tiers sont placés sous la surveillance des APD européennes.

## 2.4. Réactions à la suite de l'arrêt Schrems

L'arrêt de la CJUE a déclenché un débat animé dans l'Union et ailleurs[52]. Nous examinons dans cette section les principales réactions pertinentes et de sources faisant autorité.

Dans sa première déclaration après l'arrêt, le **groupe de travail «article 29»** (GT art. 29) n'a pas seulement précisé que l'expression «substantiellement équivalent» dans la formulation de la CJUE contenait «l'essence des principes fondamentaux de la protection des données», il a également demandé aux États membres et aux institutions européennes de trouver urgemment avec les autorités américaines une solution permettant de mettre fin à la situation d'incertitude, solution contenant des obligations en matière de mécanismes de surveillance, de transparence, de proportionnalité et des mécanismes de recours[53].

Dans le prolongement de la position du GT art. 29, certaines **autorités nationales chargées de la protection des données** (APD) ont non seulement interdit les transferts

---

[51] «Responsable du traitement (dans l'Union) à responsable du traitement (hors Union/EEE)»: décision de la Commission 2001/497/CE relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, JO L 184, 4 juillet 2001, et décision de la Commission 2004/915/CE du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JO L 385 du 29 décembre 2004; «Responsable du traitement (dans l'Union) à responsable du traitement (hors Union/EEE)» décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (et abrogeant la décision 2002/16/CE).

[52] Voici quelques exemples extraits de la presse européenne et américaine. Consultez également la déclaration de la ministre américaine du commerce Penny Pritzker concernant la décision rendue le 6 octobre 2015 par la Cour européenne de justice sur le cadre de le Safe Harbour.

[53] Déclaration du groupe de travail «article 29» du 16 octobre 2016.

dans leur pays sur la base du régime actuel de Safe Harbour mais ont également réaffirmé leur compétence à procéder à des contrôles de la légalité des transferts de données de la part des exportateurs de données[54]. Un document commun d'orientation des **16 APD allemandes** a suivi dans lequel il était précisé que : 1) les transferts se basant uniquement sur le Safe Harbour étaient interdits considérant que le Safe Harbour avait été invalidé; 2) les APD allemandes, prenant apparemment le contre-pied des autres APD, avaient temporairement suspendu les nouvelles approbations de règles d'entreprise contraignantes et des accords d'exportation de données et remis en question la validité des transferts de données basés sur les clauses types européennes[55].

Un certain nombre **d'ONG européennes et américaines** (comme EPIC et Privacy International) ont rédigé en commun une «lettre concernant le Safe Harbour après l'arrêt Schrems», adressée à la fois à la commissaire Jourová et à la ministre américaine du commerce Pritzker, dans laquelle elles affirmaient qu'un «cadre révisé du Safe Harbour semblable à l'ancien sera presque certainement invalidé par la CJUE», estimant que l'arrêt Schrems a exigé des «modifications nécessaires dans les législations internes et les accords internationaux des négociateurs[56]». Elles ont en particulier observé que la CJUE avait mis l'accent sur le fait que les pays tiers devaient garantir une protection effective et que les limitations à la protection des données n'étaient admissibles que lorsqu'elles étaient strictement nécessaires. Elles évoquaient également l'arrêt de la collecte massive du contenu des communications électroniques.

Certaines **entreprises technologiques américaines** ont considéré l'invalidation du «Safe Harbour» comme un avertissement pour les entreprises, qui peuvent s'attendre, région par région, à un effet de dominos en matière de réglementation, et ont prié instamment les entreprises d'adopter une attitude volontariste dans l'application de la nouvelle réglementation[57].

Le **Parlement européen** a depuis longtemps adopté une position considérant comme inadéquat le niveau de protection des droits fondamentaux dans le régime du «Safe Harbour» et, outre les différentes enquêtes menées, il a, de façon répétée,

---

[54] Parmi les premières à réagir à l'arrêt Schrems, **l'APD du Schleswig-Holstein, en Allemagne**, a publié un document exposant sa position le 14 octobre 2015. Comme d'autres APD, le ***garante*** italien a statué que les transferts actuels basés sur la précédente autorisation étaient interdits tandis que les entreprises étaient autorisées à utiliser d'autres instruments (comme les clauses contractuelles types, les règles d'entreprise contraignantes et les autorisations spécifiques du *garante*). L'APD espagnole (**AEPD**) a exigé des entreprises opérant en Espagne de s'assurer que des mécanismes alternatifs étaient mis en place pour les données transférées vers les États-Unis, les avertissant de possibles mesures coercitives au cas où elles ne mettraient pas en place ces mécanismes et ne les lui notifieraient pas. La CNIL française a adopté une position similaire.

[55] Les APD allemandes ont réaffirmé leur compétence à interdire les transferts sur la base des clauses types européennes et ont en effet exercé cette compétence en invalidant un transfert spécifique de données.

[56] Consultez la lettre commune, p. 8: «l'Union européenne devrait mettre fin à la surveillance massive des individus par les États membres»; «l'Union européenne devrait suspendre l'accord Swift et l'accord PNR et déposer un catalogue numérique des droits tel que recommandé par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen (rapport sur la surveillance électronique de masse des citoyens de l'union européenne)»;«les États-Unis devraient adopter, sur la base du Consumer Privacy Bill of Rights, un cadre juridique global de protection des données contenant des compétences appropriées de régulation et d'exécution»; «les États-Unis devraient mettre en place un organisme indépendant de protection des données»; «les États-Unis devraient ratifier la convention 108 du Conseil de l'Europe».

[57] Ron Hovsepian, «Living In A Post-Safe Harbor World», *CloudTweaks*, 30 novembre 2016.

demandé la suspension des principes du «Safe Harbour», en particulier dans sa résolution de 2014 relative aux programmes de surveillance électronique de masse conduits aux États-Unis et dans certains pays de l'Union européenne[58]. À la suite de l'arrêt de la CJUE, cet arrêt et ses conséquences ont été débattues au Parlement européen[59]. Le 29 octobre 2015, une résolution sur le suivi de la résolution de 2014 a été adoptée[60] dans laquelle le Parlement a également souligné l'importance de l'autre arrêt de la CJUE[61] invalidant la directive sur la conservation des données. Le caractère novateur de l'arrêt Schrems est également illustré par la référence que fait la CJUE aux principes exprimés par la Cour européenne des Droits de l'homme (**CEDH**) dans sa jurisprudence sur la question des limites aux «programmes généraux de surveillance»[62]. Les références croisées entre les deux cours en matière de protection des données (et leur concomitance) sont particulièrement significatives[63].

Dans sa résolution de suivi de 2015, le Parlement européen a également estimé que les réformes de la législation sur la surveillance menées aux États-Unis étaient significatives pour l'élaboration et l'application du nouveau cadre, en particulier l'adoption du Judicial Redress Act[64]. Au sujet du contrôle démocratique, le Parlement européen a indiqué que: «tout en respectant pleinement que les parlements nationaux soient maîtres du contrôle des services de renseignements nationaux, appelle l'ensemble des parlements nationaux

---

58 Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens.

59 Le président de la commission LIBE, Claude Moraes (S&D, Royaume-Uni), a prié instamment la Commission de prendre l'initiative d'un nouveau cadre de transfert des données, déclarant: «Il s'agit de commerce, il s'agit d'affaires, il s'agit des libertés des citoyens, mais il s'agit aussi d'une question au jour le jour».

60 Résolution du Parlement européen du 29 octobre 2015 sur le suivi de la résolution du Parlement européen du 12 mars 2014 sur la surveillance électronique de masse des citoyens de l'Union européenne.

61 Voir note de bas de page 23.

62 Concernant les références mutuelles dans les jurisprudences de la CEDH et de la CJUE, voir F. Bohem, «Assessing the New Instruments in EU-US Data Protection Law», *EDPL* 2/2016, qui souligne également l'interconnexion croissante entre les contextes de préservation de l'ordre public et de pure surveillance aux États-Unis et dans l'Union européenne (avec un échange de données entre les organismes des différents secteurs) qui semble se retrouver dans le manque de distinction que fait chacune des cours lorsqu'elle fait référence aux arguments de l'autre. Consultez également le rapport (résumé en français) de l'agence des droits fondamentaux intitulé «Surveillance par les services de renseignements: protection des droits fondamentaux et voies de recours dans l'Union européenne», 2015. Il est donc attendu de la CJUE qu'elle applique également dans l'avenir ce même raisonnement de la CEDH lorsqu'elle évalue la validité, au vu de la charte des droits fondamentaux, d'autres mesures législatives de l'Union et des États membres dans ce même domaine.

63 Voir P. de Hert et P. C. Bocos, «the Case of *Roman Zakharov* v. *Russia*: The Strasbourg follow-up to the Luxembourg Court's *Schrems* judgment», *Strasbourg Observers*, 2016.

64 Dans sa résolution de suivi de 2015, le Parlement européen «salue en particulier le fait que le Judicial Redress Act de 2015 ait été adopté avec succès par la Chambre des représentants le 20 octobre 2015, ce qui témoigne des efforts considérables et constructifs consentis par les États-Unis afin de répondre aux préoccupations de l'Union; estime qu'il est crucial de garantir, dans toutes les circonstances identiques, les mêmes droits en matière de recours juridique effectif aux citoyens ou personnes physiques de l'Union [...]; [...] insiste sur le fait qu'une condition préalable à la signature et à la conclusion de l'accord-cadre est l'adoption du Judicial Redress Act au Congrès américain»; «rappelle que tout accord international conclu par l'Union prime sur le droit dérivé de l'Union et souligne par conséquent qu'il faut s'assurer que l'accord-cadre ne limite pas les droits des personnes concernées et les garanties qui s'appliquent au transfert de données en vertu du droit de l'Union».

qui ne l'ont pas encore fait à évaluer de manière approfondie et à mettre en place une surveillance appropriée des activités de renseignement et à s'assurer que ces comités/organes de surveillance [puissent] assurer un contrôle efficace et indépendant des services de renseignement tout comme des échanges d'informations avec d'autres services de renseignement étrangers»[65].

# 3. Bouclier de protection des données: un long cheminement

## 3.1. La première décision d'adéquation de la Commission et les nouveaux «principes de protection de la vie privée»

La nouvelle décision d'adéquation concernant le bouclier de protection des données a été adoptée par la Commission européenne le 12 juillet 2016 pour mettre le nouveau cadre en conformité avec les indications de la CJUE (arrêt Schrems et autres arrêts). Les différentes étapes de la procédure ayant mené à l'adoption du nouveau cadre méritent l'attention.

La Commission et le ministère américain du commerce ont examiné le cadre du «Safe Harbour» pendant au moins les deux dernières années et, après l'arrêt Schrems, les négociations sur ce chapitre se sont intensifiées afin d'obtenir un nouvel accord. L'échange, entre les deux rives de l'Atlantique, d'informations concernant le fonctionnement du système américain de protection des données et les engagements vis-à-vis de garanties plus fortes ont occupé une part substantielle des négociations afin que la Commission puisse procéder à une évaluation correcte du système américain en vue de l'adoption d'une nouvelle décision d'adéquation[66].

À cette fin, la commissaire pour la justice, les consommateurs et l'égalité des genres, **Vera Jourová**, a annoncé lors de la réunion du 2 février 2016 de la commission pour les libertés civiles, la justice et les affaires intérieures (LIBE) du Parlement européen qu'**un nouvel accord politique**, le **bouclier de protection des données**, avait été trouvé avec les États-Unis d'Amérique (bien qu'aucun texte n'ait été alors mis à disposition). À cette occasion, la commissaire Jourová a souligné que «les États-Unis [avaient] donné l'assurance par écrit que la capacité des autorités répressives et de sécurité nationale à accéder aux données à caractère personnel serait sujette à des limitations, des garanties et des mécanismes de surveillance bien définis et [...] ne pratiqueront pas de surveillance de masse et sans discrimination», suggérant que la réforme en cours des mécanismes de recours et de la protection des données faisait l'objet de toutes les attentions aux États-Unis[67].

En outre, le 2 février 2016, le **groupe de travail européen «article 29»** a publié sa première déclaration concernant l'annonce du bouclier de protection des données dans

---

[65] *Ibid*. paragraphe 20.

[66] Ainsi qu'une récente étude commandée par la commission LIBE le précise, les systèmes américain et européen de protection des données restent caractérisés par de colossales différences au niveau constitutionnel, au niveau procédural et au niveau des voies de recours. C'est pourquoi les transferts de données futurs semblent fortement conditionnés par la réforme en cours de la législation américaine, en particulier concernant les activités répressives et de surveillance. Voir l'étude «A comparison between US and EU data protection legislation for law enforcement purposes» de Franziska Boehm, commandée par le département thématique C du Parlement européen pour la commission LIBE.

[67] Annonce du nouvel accord par la commissaire Jourová.

laquelle il a présenté **quatre garanties essentielles** dans les activités de renseignement, garanties sur lesquelles il aurait basé son évaluation (une fois les documents concernant le bouclier de protection des données rendus publics) et qui sont tirées de la jurisprudence européenne en matière de droits fondamentaux:

(1) le traitement doit reposer sur des bases claires, précises et compréhensibles: quiconque doit être capable de comprendre ce qui sera fait de ses données et où elles seront transférées;
(2) la nécessité et la proportionnalité au regard de la finalité poursuivie (sécurité nationale) doivent être démontrées;
(3) un mécanisme indépendant, efficace et impartial de surveillance doit exister (un juge ou tout autre organe indépendant);
(4) des voies de recours efficaces doivent être offertes à quiconque.

Si le GT art. 29 a reconnu les efforts consentis par les États-Unis en 2014 et en 2015 pour améliorer la protection des données des citoyens non américains, il a confirmé dans cette déclaration ses préoccupations concernant le cadre juridique américain actuel relativement aux quatre garanties essentielles, notamment celles portant sur le champ d'application et les mécanismes de recours. Le GT art. 29 a également rappelé que, étant donné l'invalidation du «Safe Harbour», les APD de l'Union européenne traitaient les affaires et les réclamations afférentes au cas par cas[68].

Le 29 février 2016, la Commission a publié un ensemble de documents constituant la **première version du cadre du nouveau bouclier de protection des données UE–États-Unis**, ensemble qui inclut :

- une **communication** de la Commission européenne au Parlement européen et au Conseil intitulée «Flux de données transatlantiques: rétablir la confiance grâce des garanties solides»;
- le **projet de décision d'adéquation** de la Commission européenne;
- les **principes de protection de la vie privée** publiés par le ministère américain du commerce (DoC);
- **plusieurs lettres** contenant des «engagements» de la part des autorités américaines, à la fois du point de vue commercial et du point de vue des services répressifs et de renseignement; parmi celles-ci, des lettres du secrétaire d'État John Kerry, du ministre du commerce et du président de la commission fédérale du commerce (FTC) (annexes)[69].

## 3.2. Avis, analyses et réactions à la première version du bouclier de protection des données

Comme il a pu être constaté durant l'audition organisée par la commission LIBE[70] du Parlement européen et dans les médias[71], les réactions à la publication du (projet de)

---

[68] Déclaration du groupe de travail «article 29» sur les conséquences de l'arrêt Schrems. Voir également la conférence de presse de la présidente Isabelle Falque-Pierrotin du 3 février 2016.

[69] Voir le communiqué de presse de la Commission européenne du 29 février 2016.

[70] Parlement européen, audition du 3 mars 2016, *Le nouveau bouclier de protection des données UE-États-Unis pour les transferts commerciaux de données à caractère personnel européennes vers les États-Unis*.

[71] Exemple: Glyn Moody, «Privacy Shield proposed to replace US-EU Safe Harbor, faces skepticism», *Ars technica*, 29 février 2016.

bouclier de protection des données étaient prudentes (sinon critiques),[72] pointant en particulier le fait qu'il permet toujours aux services de renseignement américains de collecter massivement et sans discrimination des données et de les utiliser au moins dans six cas spécifiques[73], et que de nouvelles affaires peuvent être portées devant les tribunaux.

Dans le cadre de la procédure d'adoption de la décision d'adéquation de la Commission (article 25 DPD), le GT art. 29, le groupe des APD européennes, a fourni un avis concernant le projet de nouveau cadre avant son adoption. De plus, la DPD dispose que les représentants des États membres siégeant au **comité de l'article 31** doivent approuver la décision[74]. **L'évaluation**, fort attendue, du GT art. 29 concernant ce nouvel accord a été publiée le 13 avril 2016[75]. Dans cet avis, le GT art. 29 a salué les efforts consentis de part et d'autre de l'Atlantique pour obtenir un nouveau cadre pour le transfert des données et a reconnu les améliorations qu'il apportait par rapport à son prédécesseur (le Safe Harbour). Il a toutefois exprimé ses préoccupations concernant certains aspects qu'il avait demandé à la Commission d'aborder et de clarifier. De plus, cet avis contenait des recommandations d'amélioration du projet de décision d'adéquation. En particulier, cet avis évaluait de façon critique à la fois les aspects commerciaux (partie i) et l'accès des pouvoirs publics américains aux données transférées dans le cadre du bouclier de protection des données (partie II). Le **manque de clarté** de certaines parties de la décision d'adéquation de la Commission, **la proposition de mise en place d'un médiateur américain dont l'indépendance peut être mise en doute**, la persistance des **possibilités de collecte massive des données** et la **complexité des mécanismes de recours** faisaient l'objet de ses principales **critiques**.

Concernant les aspects commerciaux, le GT art. 29 a demandé davantage de clarté ainsi que des améliorations concernant les principes de conservation des données et de limitation de la finalité, les décisions individuelles automatisées et les transferts ultérieurs.

Dans la seconde partie, qui concerne l'accès des pouvoirs publics américains aux données transférées dans le cadre du bouclier[76], les critiques principales portent sur le manque d'éléments concrets concernant la proportionnalité de la collecte de données, considérant que «le traitement sur-mesure des données peut néanmoins être considéré comme massif». Les préoccupations à cet égard demeurent, malgré les limitations

---

[72] Voir par exemple G. Vermeulen, 2016. «The Paper Shield: On the Degree of Protection of the EU-US Privacy Shield Against Unnecessary or Disproportionate Data Collection by the US Intelligence and Law Enforcement Services», in D. Svantesson et D. Kloza (éds), *Transatlantic Data Privacy Relationships as a Challenge for Democracy*, Intersentia, 2016.

[73] Comme l'indique la directive politique Obama n° 28/2014, opérations de renseignement d'origine électromagnétique, qui est rappelée dans la décision d'adéquation du bouclier de protection des données.

[74] Voir la procédure et les documents de comité.

[75] GT art. 29, avis 01/2016 sur le projet de décision d'adéquation du bouclier de protection des données, 13 avril 2016.

[76] Cette partie de l'avis est complétée par un autre document dans lequel les autorités en charge de la protection des données ont confirmé les **quatre garanties essentielles** à l'égard des mesures justifiées pour des motifs de sécurité et qui constituent une ingérence dans les droits fondamentaux (traitement des données conforme à la loi et sur la base de règles précises et compréhensibles; démonstration de la nécessité et de la proportionnalité au regard de la finalité poursuivie; existence d'un mécanisme indépendant de surveillance; voies de recours efficaces offertes aux individus).Ces garanties doivent être respectées dans tout transfert de données vers un pays tiers.

introduites dans la réglementation après 2013[77]. De plus, concernant les recours juridictionnels, le GT art. 29 relève que le système américain pose une limite importante dans la mesure où il exige de l'individu qu'il démontre sa qualité pour agir, ce qui signifie que le demandeur doit subir un préjudice direct. Cette conception est différente de la conception européenne dans laquelle quiconque peut s'adresser à un tribunal s'il a une raison légitime de soupçonner une ingérence dans ses droits fondamentaux[78]. De plus, l'exigence américaine semble contrecarrée par l'absence de notification aux individus qui ont fait l'objet de mesures de surveillance, même après que celles-ci ont pris fin.

Bien que cet avis ne soit pas contraignant, la Commission a été invitée à mettre en œuvre les améliorations prescrites. Il convient de noter que les autorités européennes joueront un rôle dans l'application du bouclier dans la mesure où elles seront compétentes pour entendre/examiner les plaintes concernant l'accord.

Le Contrôleur européen de la protection des données (**CEPD**), s'exprimant sur l'avis du GT art. 29[79], a précisé que, si le bouclier de protection des données pouvait être considéré comme une avancée par rapport au «Safe Harbour», l'aune à laquelle il devait être mesuré demeure la DPD et c'est pourquoi le texte du projet de bouclier devait être vigoureusement amélioré. De plus, le CEPD a souligné que, si les règles d'entreprise contraignantes ou les clauses contractuelles types fonctionnaient correctement pour les transferts de données des grandes entreprises, de nombreuses petites et moyennes entreprises avaient besoin d'une nouvelle solution qui devait également être considérée du point de vue du règlement général sur la protection des données (**RGPD**), de sorte qu'il ne soit pas exigé des entreprises qu'elles modifient à nouveau leurs pratiques en matière de respect de la vie privée une fois le nouveau règlement en vigueur. Le CEPD a appelé, en d'autres termes, à **regarder vers l'avenir**. Outre sa participation aux travaux du GT art. 29, le CEPD a également publié une évaluation et des recommandations. Dans son **avis** du 30 mai 2016, le CEPD a appelé de ses vœux de fortes améliorations afin d'obtenir un cadre solide et durable (une solution à long terme). En particulier, tout en saluant les efforts consentis par les deux parties afin de trouver une solution dans les transferts de données (cruciaux «alors que les flux de données sont devenus mondiaux, instantanés et imprévisibles») et la plus grande transparence du côté américain concernant les pratiques du renseignement visant la collecte de données de citoyens non américains, le CEPD a souligné que le nouveau cadre devait refléter pleinement les valeurs communes fondées sur les droits démocratiques et individuels[80].

---

[77] Le GT art. 29 n'a pu, dans son avis, procéder à une évaluation définitive de la légalité du traitement ciblé mais néanmoins massif des données, en particulier parce qu'il attendait que la CJUE exprime sa position. Les limitations à l'égard, à tout le moins, de la *conservation* générale et sans discrimination des données ont dans les faits été récemment réaffirmées par la CJUE dans les affaires jointes C-203/15 et C-698/15 — *Watson & autres* ainsi que dans l'arrêt *Tele2Sverige*; voir également l'affaire en cours concernant le PNR UE-Canada).

[78] Comme la CEDH l'a statué dans l'arrêt *Zakharov* et tel qu'affirmé dans l'avis du GT art. 29.

[79] Voir présentation de Giovanni Buttarelli du rapport annuel 2015 du CEPD (résumé en français) à la commission LIBE du Parlement européen.

[80] Avis du CEPD, avril 2016. Ainsi, le projet de bouclier pouvait constituer un pas dans la bonne direction, mais il ne comprenait pas, tel qu'il était alors formulé, l'ensemble des garanties nécessaires à la sauvegarde des droits de la personne tels que consacrés par le traité et la charte des droits fondamentaux. Voir également X. Tracol, «EU-US PS: the saga continues», *Computer Law & Security Review* 32 (2016), 775-777, qui estime que la Commission européenne a de nouveau échoué à procéder à un examen général de l'ordre juridique américain et ne s'est basée que sur des lettres provenant de différentes autorités.

Après quelques retards, les représentants des **États membres de l'Union** (comité de l'article 31) ont voté (avec quatre abstentions) l'adoption du paquet du bouclier de protection des données le 8 juillet 2016[81].

Le **Parlement européen**, qui n'a pas de droit de vote dans les décisions d'exécution de la Commission, a exprimé ses préoccupations au sujet du nouveau cadre en adoptant une **résolution** (non contraignante) le 26 mai 2016[82] dans laquelle il a invité la Commission à mettre en œuvre pleinement les recommandations formulées par le groupe de travail «article 29» afin de renforcer le bouclier de protection des données. Parmi les éléments pertinents de la résolution, le Parlement a, d'une part, souligné l'importance de la protection des données, considérant qu'elle signifiait «la protection des personnes auxquelles appartiennent les informations faisant l'objet d'un traitement et que cette protection est l'un des droits fondamentaux» reconnus dans la charte des droits fondamentaux, et a, d'autre part, insisté sur l'importance de la sécurité juridique liée aux transferts de données pour la confiance des consommateurs, pour le développement des relations commerciales transatlantiques[83] et pour la coopération dans le domaine répressif. De plus, le Parlement européen a souligné que «le bouclier de protection des données s'inscrit dans un dialogue plus large entre l'Union européenne et les pays tiers [...] en ce qui concerne la confidentialité des données [...] et les objectifs d'intérêt commun», insistant sur la nécessité de définir une démarche générale en matière de transfert des données vers les pays tiers[84].

Dans sa déclaration devant le Parlement européen, la **commissaire Jourová** a reconnu que le bouclier de protection des données n'était peut-être pas parfait, mais a estimé que la Commission était satisfaite d'avoir obtenu tout ce qu'il était possible d'obtenir[85].

---

[81] Voir le vote formel du comité de l'article 31. En cas de vote défavorable du comité de l'article 31, la Commission aurait pu faire appel ou soumettre une version révisée de sa décision d'adéquation. Les commissaires Jourová et Ansip, annonçant cette adoption dans une déclaration conjointe le même jour, ont déclaré : «Pour la première fois, les États-Unis ont donné par écrit à l'Union européenne l'assurance que l'accès des pouvoirs publics aux données à des fins répressives et de sécurité nationale serait subordonné à des limitations, des conditions et des mécanismes de surveillance bien définis et ont exclu toute surveillance de masse non ciblée des données des citoyens européens. [...] le bouclier protège les droits fondamentaux et prévoit plusieurs mécanismes de recours accessibles et abordables».

[82] Parlement européen, résolution sur les flux de données transatlantiques, 26 mai 2016. Tandis qu'elle souligne l'importance de la relation transatlantique, la résolution a insisté sur le fait que «le dispositif du bouclier de protection des données doit être conforme au droit primaire et au droit dérivé de l'Union européenne ainsi qu'aux arrêts concernés de la **Cour de justice de l'Union européenne** et de la **Cour européenne des droits de l'homme**». Sept amendements proposés par différents groupes politiques ont été rejetés durant le débat concernant cette résolution du Parlement européen. De nombreux députés se sont demandés si le bouclier résisterait devant les tribunaux et les députés de gauche, menés par Jan Philipp Albrecht (Verts, Allemagne), ont proposé l'inclusion, au minimum, d'une clause de limitation dans le temps donnant un délai de quatre ans au bout duquel une révision de l'accord serait nécessaire, en raison de la nouvelle administration américaine et de la mise en œuvre du RGDP.

[83] La résolution a rappelé en particulier (considérant E) que la mise en œuvre rapide du nouvel accord était particulièrement importante pour les PME qui représentent 60 % des entreprises qui avaient recours à l'ancien Safe Harbour, c'est-à-dire des entreprises qui ont pu profiter de procédures de mise en conformité rationalisées et réduites.

[84] La Chine par exemple, tel que débattu par le Parlement européen.

[85] Ces débats se sont déroulés les 25 et 26 mai 2016 au Parlement européen. Le commissaire européen pour le marché unique numérique, Andrus Ansip, a déclaré avoir confiance dans le fait que le nouvel accord offrirait aux citoyens européens différents mécanismes de règlement des litiges avec les

Le projet de bouclier de protection des données a toutefois fait l'objet de critiques. Les **défenseurs des Droits de l'homme** et d'autres observateurs ont estimé que les engagements américains étaient insuffisants et trop vagues[86] pour garantir le respect des droits des citoyens européens et que le bouclier aurait le même destin que le Safe Harbour[87]. Dans le même temps, certaines publications ont critiqué l'arrêt de la CJUE[88].

## 4. Révision du bouclier de protection des données

Les préoccupations exprimées dans l'Union européenne ont entraîné des modifications au projet de décision d'adéquation. La nouvelle décision modifiée, qui établit le nouveau cadre UE–États-Unis et assure une protection adéquate des données des citoyens européens, a été **adoptée définitivement** le **12 juillet 2016** par la Commission, réunie en collège, de sorte que le nouveau bouclier de protection des données soit «en action

---

entreprises. Concernant la nécessité de trouver (à quelque degré que ce soit) un accord transatlantique pour protéger les citoyens des deux côtés de l'Atlantique de la surveillance de la part des services de renseignement américains et européens (considérant que les citoyens américains seraient également exposés à la surveillance des États européens), voir D. Cole et F. Fabbrini, «Bridging the transatlantic divide?: The United States, the European Union, and the protection of privacy across borders», *International Journal of Constitutional Law* (2016) 14 (1).

86 Voir notamment: Anna Fielder, «From an unSafe Harbour to a Privacy Shield full of holes», *Privacy International*, 12 avril 2016; Allison Deighton, «The EU-US Privacy Shield — is it strong enough?» *PDPRO Privacy & Data Protection*, 2016, 16 (4), 8-10. Le cabinet TLT Solicitors a relevé qu'au moins deux menaces principales pourraient peser sur ces engagements: tout d'abord, la directive politique présidentielle (qui est actuellement contraignante pour les services de renseignement américains et restreint actuellement l'étendue des activités de surveillance) pourrait bien être remplacée par la prochaine administration américaine; ensuite, en cas de doute concernant la nature contraignante de ces engagements, le nouvel accord sur le transfert transatlantique de données pourrait bien être attaqué de la même façon que le Safe Harbour. Concernant la nature des engagements américains, la Commission, au cours d'un débat tenu en janvier avec la commission LIBE du Parlement sur le projet de proposition de résolution concernant le bouclier de protection des données, a relevé que, indépendamment du changement d'administration aux États-Unis, les engagements existants de façon permanente sont contraignants pour les États-Unis d'Amérique (et non pour une administration plutôt que d'une autre).

87 Ars Technica a rapporté que nombreux sont ceux qui craignent que la NSA ne continue à disposer de larges pouvoirs dans certains cas, indépendamment des préoccupations exprimées par les défenseurs du respect de la vie privée. L'activiste du respect de la vie privée, Max Schrems, a estimé que, de par «l'existence d'une loi américaine autorisant explicitement la surveillance de masse [,] [...] les États-Unis confirment publiquement qu'ils violent les droits fondamentaux de l'Union européenne dans au moins six cas.»

88 David Bender, «Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective», *International Data Privacy law*, 2016, Vol 6, No 2; Lothar Determann, «Adequacy of data protection in the USA: myths and facts», *International Data Privacy Law*, 2016, Vol 6, No 3, qui estime que: «si la révision de le Safe Harbour a pour véritable objectif d'atteindre de meilleurs niveaux de protection des données, l'Union européenne devrait alors envisager de rendre ce programme bidirectionnel dans sa portée et également d'appliquer et de faire respecter en Europe les lois américaines de protection des données qui sont plus efficaces, plus spécifiques et plus modernes.» Concernant l'importance d'un accord transatlantique, voir également J. Brill «Strengthening International Ties Can Support Increased Convergence of Privacy Regimes», *European Data Protection Law Review*, Vol 2 (2016), No 2.

avant l'été 2016 [...] afin de mettre fin à l'incertitude juridique actuelle»[89]. La décision d'adéquation a été notifiée aux États membres le même jour et est donc entrée en vigueur immédiatement. Du côté américain, le cadre du bouclier de protection des données a été publié au **Federal Register**, l'équivalent du Journal officiel de l'Union européenne, bien que quelques semaines supplémentaires aient été accordées aux entreprises pour passer au nouveau régime. Le nouveau régime est désormais entièrement opérationnel.

Parmi les modifications promises, et conformément aux articles 25 et 26 de la directive sur la protection des données tels qu'interprétés par la CJUE dans l'arrêt Schrems, il a été prévu que le caractère adéquat du niveau de protection des données devait être évalué régulièrement et en considération de la situation dans son ensemble et des pratiques de droit. Le nouvel accord prévoit donc également un **examen conjoint annuel** du bouclier de protection des données.

À partir du 1er août 2016, les entreprises basées aux États-Unis (qui, comme il a été noté précédemment, utilisaient des régimes plus complexes de transfert des données, comme les règles d'entreprise contraignantes, durant la période de transition) ont pu adhérer au bouclier de protection des données. En d'autres termes, elles ont commencé à **autocertifier** leur conformité avec le nouveau cadre auprès du DoC. Le DoC doit vérifier que leurs pratiques en matière de respect de la vie privée sont conformes aux normes élevées de protection des données requises par le bouclier. Elles sont, en pratique, encouragées à s'engager publiquement à se conformer aux exigences du bouclier en s'inscrivant sur un **site internet**[90] ad hoc qui explique:

> *«Le programme du bouclier de protection des données, qui est administré par l'administration du commerce international (ITA) au sein du ministère américain du commerce, permet aux entreprise basées aux États-Unis d'adhérer au cadre du bouclier de protection des données afin de bénéficier de l'évaluation [par la Commission européenne] du caractère adéquat de la protection offerte[.] [...] Si l'adhésion au cadre du bouclier de protection des données est volontaire, une fois qu'une entreprise éligible s'est engagée publiquement à se conformer aux exigences du cadre, cet engagement prend force exécutoire en droit des États-Unis. Toutes les entreprises intéressées par l'adhésion au cadre du bouclier de protection des données sont invitées à examiner ses exigences dans leur intégralité.»*

En parallèle, la Commission a publié un **guide du bouclier de protection des données UE–États-Unis**[91] à l'égard duquel le groupe de travail «article 29» s'est engagé à formuler

---

[89] Tel que l'a demandé la commissaire Jourová lors de la réunion de la commission LIBE tenue le 11 juillet 2016, au cours de laquelle elle a présenté un état des lieux concernant le bouclier de protection des données.

[90] Privacy Shield Framework.

[91] Le guide souligne tout d'abord l'importance pour la relation transatlantique des transferts de données vers les États-Unis (en particulier dans l'économie mondialisée et numérique d'aujourd'hui) et la nécessité du bouclier de protection des données pour s'assurer que les données transférées vers les États-Unis continuent de bénéficier d'un niveau élevé de protection. Il convient de noter qu'il précise que cette protection s'applique que la personne concernée par les données soit citoyenne de l'Union européenne ou non (tel que l'avait demandé le GT art. 29 afin que soient reconnus les droits de toutes les personnes indépendamment de leur nationalité, conformément à la charte des droits fondamentaux). La question de savoir si les recours juridictionnels au titre du JRA sont également disponibles pour les résidents de l'Union européenne ou seulement pour ses citoyens reste toutefois en suspens. Le guide explique également que le bouclier de protection des données est l'un des instruments disponibles (hormis les clauses contractuelles et les règles d'entreprise contraignantes) et que si les entreprises adhèrent au cadre du bouclier, leur politique en matière de protection de la vie

des commentaires dans les prochains mois. Ce guide, qui s'adresse principalement aux personnes, est un document bref et informatif visant à clarifier certains des enjeux. Il contient des informations concernant les obligations des entreprises ayant adhéré au bouclier de protection des données, concernant les droits des personnes et concernant les mécanismes de recours. Il explique également comment introduire une plainte auprès d'une entreprise (par plusieurs moyens) ou auprès d'une autorité publique américaine (par exemple par l'intermédiaire du médiateur nouvellement institué).

## 4.1. Principes de protection de la vie privée et obligations des entreprises

Si les principes paraissent semblables à ceux du «Safe Harbour» au premier abord, le nouveau bouclier de protection des données les a développés pour y inclure un certain nombre de modifications des obligations qu'ils imposent aux entreprises.

Le premier principe, le principe «**notification**», spécifiait, dans le cadre du «Safe Harbour», que les organisations devaient notifier aux personnes les finalités des informations les concernant collectées et utilisées; a façon dont les personnes pouvaient les contacter en cas de question ou de plainte; le type de tiers auxquels elles divulguaient les informations et les choix et moyens qu'elles proposaient pour limiter l'utilisation et la divulgation des données. Si ce principe est conservé dans le bouclier de protection des données, il inclut désormais l'obligation faite aux entreprises de rendre publiques leurs pratiques en matière de respect de la vie privée (en indiquant qu'elles se conforment aux principes du bouclier)[92] et de fournir des liens renvoyant à celles-ci et à des informations supplémentaires disponibles auprès du DoC. De plus, ce principe inclut désormais la désignation d'un organisme indépendant de règlement des litiges afin de traiter les plaintes. À l'origine, le principe de notification ne s'appliquait pas au transfert à un tiers agissant en tant que mandataire sur instruction de l'entreprise. Cette dernière situation n'était couverte que par le principe concernant le transfert ultérieur. Cette exception a été modifiée dans le nouveau bouclier de protection des données de sorte que les entreprises doivent désormais fournir aux personnes concernées des informations concernant le droit d'accès, les choix disponibles et les transferts ultérieurs.

Le deuxième principe du «Safe Harbour», celui du **choix**, exigeait des organisations qu'elles donnent aux personnes la possibilité de choisir (refus) si leurs informations à caractère personnel pouvaient être **divulguées à un tiers** (responsable du traitement) ou utilisées à des **fins différentes** (même incompatibles) des fins initiales de la collecte de données. Concernant les informations sensibles, un choix affirmatif ou explicite (*opt in*) devait être donné pour que les informations puissent être divulguées à un tiers ou utilisées à une fin différente. Le bouclier de protection des données autorise actuellement le refus lorsqu'une finalité modifiée est **sensiblement différente mais reste compatible avec la finalité initiale** (tel que recommandé par le GT art. 29). Le bouclier de protection des données spécifie expressément que **le principe du choix ne peut être**

---

privée doit être conforme aux «principes de protection de la vie privée» dans lesquels les obligations des entreprises au titre du bouclier sont spécifiées. Une liste des entreprises ayant adhéré au bouclier (ainsi que de celles qui l'ont quitté) est disponible sur le site internet du DoC. Le DoC doit veiller à ce que «les entreprises respectent leurs engagements» (les entreprises ne peuvent conserver des données que si elles «s'engagent» auprès du DoC à continuer à appliquer les principes de respect de la vie privée). Si les entreprises ne réexaminent pas annuellement leur appartenance au bouclier, elles ne peuvent plus ni recevoir, ni utiliser des données provenant des États-Unis au titre du cadre du bouclier de protection des données (mais elles peuvent continuer à le faire sur la base d'autres instruments).

[92] Voir également le principe complémentaire de vérification, annexes II, III et 7 du bouclier de protection des données.

**utilisé pour annuler l'interdiction de traitement incompatible**. Ceci le distingue fondamentalement du «Safe Harbour». Le bouclier reste toutefois vague concernant le délai dont disposent les personnes concernées pour se prévaloir de leur droit de refus. Le bouclier donne sans ambiguïté le droit aux personnes concernées de s'opposer à tout moment à une utilisation uniquement à des fins de marketing direct[93] tout en gardant le silence sur les autres cas de refus[94].

Le troisième principe concernant les **transferts ultérieurs** (transferts à des tiers) traite de la divulgation des données à un tiers. Dans le Safe Harbour, les organisations devaient appliquer les principes de notification et de choix. Les obligations de ces principes étaient levées, dans le Safe Harbour, pour les organisations qui désiraient transférer des données à un tiers agissant en tant que mandataire dans trois cas: 1) l'organisation s'était assurée que le tiers avait adhéré au principe de protection de la vie privée du «Safe Harbour»; 2) le tiers était soumis à la DPD ou à une autre décision d'adéquation; ou 3) l'organisation ayant adhéré au «Safe Harbour» avait conclu par écrit un accord avec le tiers exigeant de sa part qu'il assure pour le moins le même niveau de protection de la vie privée que celui requis par le Safe Harbour. Dans le bouclier de protection, le principe de notification est toujours applicable, même à l'égard du transfert ultérieur, tandis que la dérogation pour transfert ultérieur à des tiers agissant en tant que mandataires (sous-traitants) reste applicable au principe de choix, ce qui signifie que les personnes ne jouiront pas d'un droit de refus dans ce cas[95]. Néanmoins, l'organisation a l'obligation de passer un contrat avec le mandataire. Comme l'a demandé le GT art. 29, la décision finale d'adéquation concernant le bouclier de protection des données a été modifiée pour souligner que le transfert ultérieur doit impliquer un niveau équivalent de protection, comme le garantissent les principes du bouclier[96]. Cette exigence signifie, entre autres choses, que le tiers ne doit traiter les données qu'à des fins qui ne sont pas incompatibles avec la finalité initiale de la collecte des données et à laquelle la personne concernée a donné son consentement. Cette exigence s'applique à **tous les transferts à des tiers indépendamment de leur lieu d'implantation**[97] Pour se conformer à cette exigence, l'organisation doit: passer avec le tiers un contrat stipulant que, si le tiers ne peut plus se conformer aux principes du bouclier de protection des données, il doit en informer l'organisation d'origine et cesser de traiter les données transférée; toute autre mesure nécessaire pour remédier au problème doit être prise. De plus, si des problèmes

---

[93] Voir annexe II de la décision d'exécution relative aux principes du cadre du bouclier de protection des données UE–États-Unis émanant du ministère américain du commerce, p. 20 et 42.

[94] À cet égard, le **GT art. 29** a regretté l'absence d'un droit général d'opposition lorsque la personne a des motifs légitimes et impérieux du fait de sa situation particulière.

[95] Voir annexe II de la décision d'exécution relative aux principes du cadre du bouclier de protection des données UE–États-Unis émanant du ministère américain du commerce, p. 20.

[96] Voir l'avis du GT art. 29 d'avril 2016, p. 20, la décision d'adéquation de la commission p. 8 et annexe II.II.3.

[97] Le GT art. 29, dans son avis d'avril 2016 (p. 22), a salué le principe de «responsabilité en cas de transfert ultérieur» qui permet les transferts à des mandataires (sous-traitants) sur la base d'un contrat et uniquement pour une finalité limitée et spécifique, mais il a également demandé que cette finalité limitée soit compatible avec la finalité initiale. Le nouveau texte du bouclier inclut désormais une exigence de «cohérence avec le consentement fourni par la personne». De plus, ce texte demandait des obligations supplémentaires et une clarification concernant le transfert à un sous-traitant ultérieur (mandataire) considérant que le responsable d'origine du traitement dans l'Union européenne ne devrait pas se voir retirer ses capacités de contrôle et devait être informé d'autres transferts ultérieurs: le contrat entre le responsable du traitement dans l'Union européenne et le premier mandataire détermine si le transfert ultérieur est autorisé (p. 23).

de conformité devaient apparaître dans le contexte d'une sous-traitance du traitement des données, l'organisation d'origine agissant en tant que responsable du traitement sera tenue pour responsable à moins qu'elle ne puisse prouver qu'elle n'est pas responsable du préjudice.

L'**accès** aux informations à caractère personnel détenues par une organisation devait être donné aux personnes concernées aux termes des principes du «Safe Harbour». Les personnes concernées pouvaient demander la correction, la modification ou la suppression de ces informations lorsqu'elles étaient incorrectes. Toutefois, l'accès pouvait être refusé lorsque les contraintes ou les coûts de la fourniture de cet accès étaient disproportionnés par rapport aux risques encourus par la personne vis-à-vis de sa vie privée ou lorsque les droits de personnes autres que la personne concernée pouvaient être violés. **Le bouclier de protection des données transforme ce principe en un droit plein et entier des personnes concernées**. Les personnes concernées peuvent obtenir, sans justification et pour un coût qui n'est pas excessif, confirmation que leurs données à caractère personnel sont traitées par une organisation et elles doivent recevoir les données demandées dans un délai raisonnable. Le bouclier de protection des données régule plus précisément **les exceptions** à l'accès aux données en spécifiant les conditions suivantes: 1) la situation est caractérisée par une circonstance exceptionnelle; 2) la limitation de l'accès est nécessaire et dûment justifiée; 3) il revient à l'organisation de prouver que ces exigences sont remplies[98]. Concernant la question des **décisions automatisées** basées sur le **traitement automatisé**[99], la décision d'exécution adoptée concernant le bouclier de protection des données, à la différence du premier projet, contient une référence spécifique à la législation américaine concernant la protection des personnes dans les domaines où le traitement automatisé est utilisé (prêts, hypothèques)[100]. Elle suggère de plus la nécessité de débattre du profilage, sujet abordé dans le RGPD; cette question sera abordée lors du premier examen annuel.

Le bouclier de protection des données **renforce les exigences de sécurité**. Dans le Safe Harbour, ce principe n'exigeait des organisations que de prendre des précautions raisonnables pour protéger les informations à caractère personnel de la perte, de l'utilisation abusive, de la consultation illicite, de la divulgation, de la modification et de la destruction. Le bouclier de protection des données exige la mise en œuvre de mesures de sécurité raisonnables et appropriées. Ces mesures doivent être évaluées en considérant les risques résultant du traitement et la nature des données. De plus, le

---

[98] Il convient de noter que le GT art. 29 a demandé qu'il soit précisé que la limitation contenue dans le principe complémentaire 8 (l'accès ne doit être fourni que dans la mesure où une organisation stocke les données) devait être interprétée de façon restrictive en rendant équivalents le «stockage» et le «traitement» en toutes circonstances. Il n'a pas été donne suite à cette suggestion.

[99] Les instruments automatisés comme les ordinateurs peuvent utiliser des algorithmes ou d'autres systèmes à base de règles pour prendre automatiquement des décisions concernant les personnes et à la place de celles-ci sur la base des informations à caractère personnel stockées. La directive européenne sur la protection des données (article 15) donne aux personnes le droit de ne pas être soumises à des décisions prises sur la base d'un traitement automatisé.

[100] Voir décision d'adéquation p. 7 Toutefois, voir aussi l'avis du GT art. 29 qui a critiqué le nombre d'exceptions disposées par les principes complémentaires, accès (annexe II, III, 8.e. (i), confirmées dans le bouclier adopté, et sa déclaration la plus récente regrette l'absence dans le bouclier de règles spécifiques concernant les décisions automatisées. Concernant les questions d'exécution en matière de protection des données en général, voir D. Wright & P. De Hert (éds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer, 2016.

bouclier exige qu'un contrat soit passé avec les sous-traitants éventuels, qui garantisse le même niveau de protection.

Dans le cadre du «Safe Harbour», le sixième principe, **intégrité des données**, exigeait que les données collectées soient pertinentes au vu de leurs finalités et que l'entreprise garantisse que les données soient fiables, exactes, exhaustives, et actuelles. Ce principe a été modifié dans le bouclier de protection des données pour inclure également le **principe de limitation de la finalité**. Ce principe spécifie que les organisations ne peuvent pas traiter des données à des fins incompatibles avec celles pour lesquelles ces données ont été collectées auprès de la personne concernée et auxquelles cette dernière a donné son consentement. Il est désormais spécifié que les données ne peuvent être conservées qu'aussi longtemps qu'elles servent la finalité pour laquelle elles ont été collectées et pour laquelle le traitement a été autorisé. Dans les limites définies par le bouclier, les données ne peuvent être conservées plus longuement que pendant la durée et dans la mesure nécessaires à l'une des finalités suivantes: archivage d'intérêt public, journalisme[101], littérature et arts, recherche scientifique et historique et analyse statistique. Les entreprises ne semblent donc pas être soumises à l'obligation de fixer une limite spécifique dans le temps à la conservation des données dans leur politique en matière de protection de la vie privée. En revanche, les entreprises sont obligées de mentionner la finalité pour laquelle les données sont collectées.

Le dernier principe du «Safe Harbour» concernait les **obligations d'exécution**. Il a été complété dans le bouclier de protection des données. L'analyse de ces obligations d'exécution fait l'objet de la section suivante.

## 4.2. De nouvelles procédures de recours

Le Safe Harbour a introduit des **obligations d'exécution** permettant de s'assurer que les organisations se conforment à ses principes. Les organisations devaient mettre à disposition des mécanismes de recours indépendants simples et peu coûteux afin d'examiner les plaintes des personnes et devaient verser des indemnités le cas échéant. Les entreprises devaient également s'assurer de la mise en place de procédures de vérification de l'application des principes du «Safe Harbour» et veiller à remédier à tout problème provenant d'un défaut d'application de ces principes. Ces sanctions devaient être suffisamment dissuasives pour garantir le respect des principes. Enfin, les procédures de recours se trouvaient dans la section 5 du Federal Trade Commission Act. Néanmoins, la coopération avec les autorités chargées de la protection des données (APD) était facultative.

Le bouclier de protection des données développe les voies de recours. En particulier, il rend la coopération avec les APD obligatoire pour les organisations participant au bouclier qui traitent des **données concernant les ressources humaines**. Pour les autres organisations, la coopération avec les APD reste facultative; elles peuvent choisir une APD pour régler indépendamment les litiges au lieu d'utiliser un autre mécanisme de règlement. De plus, le bouclier introduit **des mécanismes de recours en cas de non-respect** d'une décision provenant d'un organisme de règlement des litiges ou d'autoréglementation. Dans ce cas, l'organisme de règlement des litiges ou d'autoréglementation doit notifier les cas de non-respect des décisions au DoC ou à la FTC (ou à toute autre autorité américaine compétente pour examiner les pratiques

[101] Le GT art. 29 auraient préféré que le bouclier limite davantage les exceptions journalistiques en matière de traitement et de conservation des données, conformément à l'opinion de la CJUE (arrêt *Google Spain* par exemple).

déloyales ou de nature à induire en erreur), ou à un tribunal compétent. En dernier ressort, les parties peuvent porter l'affaire devant un **panel d'arbitrage du bouclier de protection des données** (*Privacy Shield panel*)[102].

La Commission envisage différentes étapes possibles dans le recours.

(1) Les personnes concernées peuvent déposer une plainte directement à l'entreprise autocertifiée. L'entreprise doit avoir mis en place un mécanisme efficace de recours et doit indiquer aux personnes où elles peuvent déposer leurs plaintes. Ce point de contact peut être à l'intérieur ou à l'extérieur de l'entreprise. Les plaintes peuvent également être communiquées par les personnes concernées par l'intermédiaire du DoC ou de l'APD. L'entreprise doit répondre à la plainte dans les 45 jours.

(2) Les plaintes peuvent être portées devant l'organisme indépendant de règlement des litiges désigné par l'organisation pour traiter les plaintes individuelles et ce gratuitement. Cet organisme de règlement des litiges doit fournir une décision qui peut inclure des sanctions et des actions correctrices et mettre fin au non-respect. L'organisme indépendant de règlement des litiges doit fournir des informations concernant le bouclier de protection des données et les procédures. Il doit également produire des statistiques annuelles concernant les services qu'il a fournis. Au cas où l'entreprise n'exécute pas la décision d'un organisme de règlement des litiges, la personne concernée peut porter plainte devant la FTC ou tout autre autorité américaine compétente pour examiner les pratiques déloyales et de nature à induire en erreur aux États-Unis.

(3) La personne concernée peut introduire un recours auprès d'une APD si l'entreprise est obligée ou accepte de coopérer. L'obligation de coopérer avec l'APD ne s'impose que si l'entreprise ayant adhéré au bouclier traite des données concernant les ressources humaines provenant de l'Union européenne; d'autres entreprises peuvent accepter de coopérer volontairement. L'APD exprime son opinion par l'intermédiaire d'un panel informel composée d'APD européennes. Les deux parties ont la possibilité de commenter l'affaire avant que le panel ne formule son avis. Les entreprises tenues de coopérer avec les APD sont dans l'obligation de répondre aux demandes faites par le panel d'APD et doivent se conformer à l'avis formulé par celui-ci, y compris à toute mesure corrective ou compensatoire. L'avis du panel doit être émis dans les 60 jours suivant la réception de la plainte et l'organisation doit se conformer à l'avis dans les 25 jours suivant l'émission.

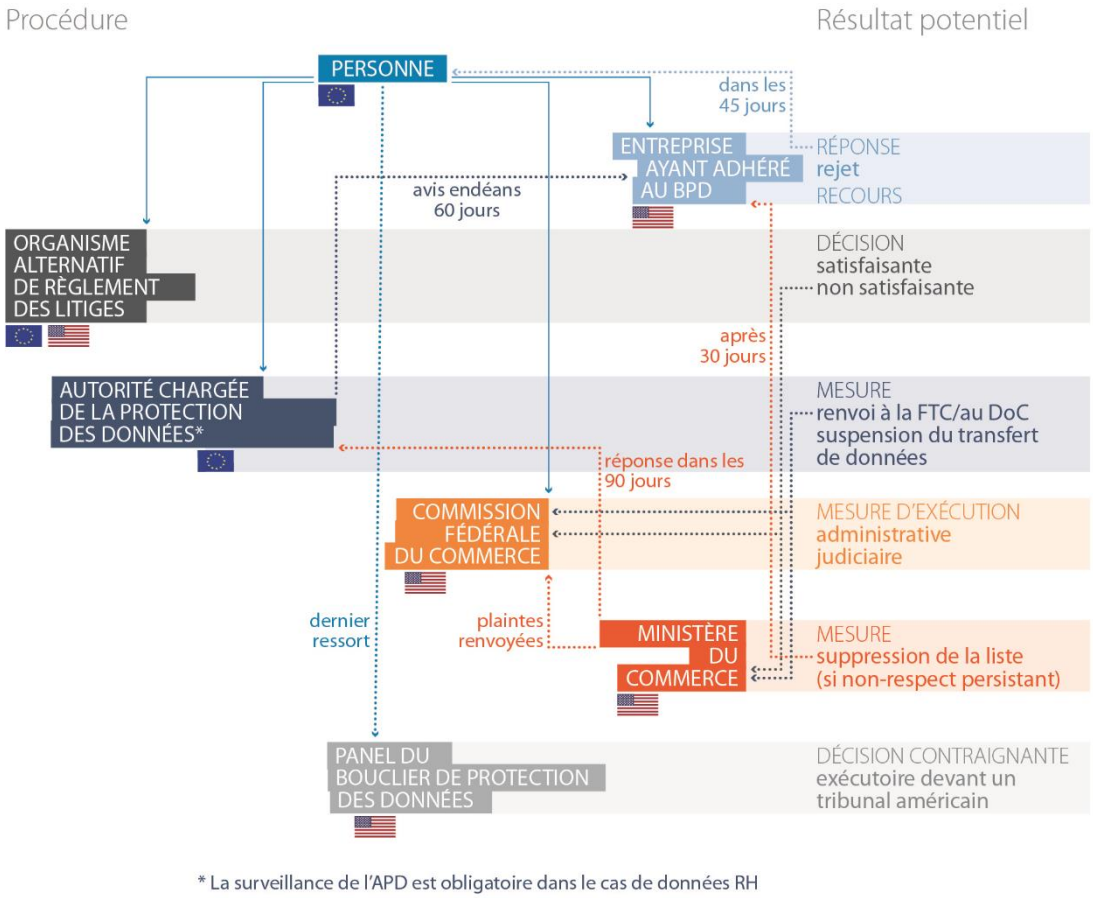
(4) En cas de non-respect injustifié de l'avis du panel d'APD, cette dernière peut notifier le renvoi de la plainte à la juridiction de la FTC ou conclure à une infraction à l'exigence de coopération. Dans le premier cas, ceci peut déclencher une mesure coercitive fondée sur la section 5 du Federal Trade Commission Act (comme indiqué dans la section 4.3.2 de cette étude). Dans le second cas, le DoC peut considérer le refus de coopérer comme un non-respect persistant qui entraîne la suppression de l'entreprise de la liste du bouclier de protection des données (après préavis de 30 jours). Les APD peuvent faire suivre les plaintes au DoC par l'intermédiaire d'un point de contact. À la réception d'une plainte, si l'APD considère que le transfert à une entreprise s'est fait en violation du droit européen de la protection des données,

[102] Le GT art. 29 a salué les différents niveaux de mécanismes de recours dont dispose le bouclier de protection des données mais il a critiqué la complexité et le manque de clarté de la structure générale qui, selon lui, affaibliraient la capacité des personnes concernées à exercer efficacement leurs droits (avis, p. 26).

elle peut, si nécessaire, suspendre le transfert de données.

(5) Les autorités américaines ayant pouvoirs d'enquête et d'exécution, telles que la FTC, sont compétentes s'agissant des entreprises qui ont adhéré au bouclier de protection des données. La priorité sera donnée aux renvois pour non-respect provenant des organismes indépendants de règlement des litiges ou d'autoréglementation, des APD et du DoC. Les personnes pourront toujours présenter directement les plaintes pour non-respect au titre de la section 5 du Federal Trade Commission Act.

**Figure 1 — Mécanismes de recours à disposition des personnes**




*Source*: EPRS, 2017.me

(6) En **dernier ressort**, le bouclier instaure un **panel d'arbitrage du bouclier de protection des données** (*Privacy Shield arbitration panel*) si aucun des mécanismes de recours susmentionnés n'a permis de donner satisfaction à la plainte d'une personne. Seules les personnes peuvent intenter une action devant ce panel et son intervention est déclenchée par l'envoi d'une notification formelle à l'entreprise par la personne concernée (indiquant les mesures déjà prises). Le panel d'arbitrage du bouclier sera composé de un à trois arbitres choisis par le DoC et la FTC parmi un corps de vingt arbitres. Le panel a l'autorité d'ordonner une réparation non monétaire (accès, correction, suppression des données par exemple). Si aucune indemnité monétaire ne peut être ordonnée par le panel (alors qu'un tribunal peut ordonner une telle indemnité), les personnes concernées peuvent demander **l'exécution de la sentence arbitrale devant les tribunaux américains** au titre du Federal Arbitration Act. Les **coûts de l'arbitrage** sont financés par un fonds spécifique (alimenté par des contributions des entreprises qui ont adhéré au bouclier de protection des données); si la personne demande l'assistance d'un avocat, les frais

d'avocat ne sont pas couverts par le fonds.

(7) Les plaintes peuvent être introduites directement au titre des lois américaines établissant des voies de recours au titre de la responsabilité délictuelle et dans les cas de dol, de pratiques déloyales ou frauduleuses[103] ou de rupture de contrat.

## 4.3. Les nouveaux engagements et procédures de surveillance des autorités américaines

4.3.1. *Le ministère américain du commerce*

Le ministère américain du commerce (Department of Commerce, DoC) a réitéré ses précédents engagements et en a pris de nouveaux afin de renforcer la capacité à faire respecter les procédures. Dans le cadre du «Safe Harbour», le DoC devait déjà établir la liste de l'ensemble des organisations autocertifiées. Le DoC a désormais réaffirmé son engagement à tenir cette liste à jour en supprimant les entreprises qui ne respectent plus les règles du «Safe Harbour» ou qui ne renouvellent pas leur autocertification. Le DoC s'est engagé à notifier aux entreprises leur suppression de la liste et à vérifier si les entreprises qui ont été supprimées ou qui ont décidé de se retirer de la liste effacent les données reçues durant leur participation au «Safe Harbour» ou si elles ont l'intention de conserver ces données et, dans ce dernier cas, dans quelles circonstances (si elles continueront à respecter les principes du «Safe Harbour» et s'il existe un point de contact pour ces données). La liste doit également indiquer quelles données sont concernées et, en particulier, si les entreprises autocertifiées ont reçu des données concernant les ressources humaines, car celles-ci imposent des obligations supplémentaires aux entreprises. Le DoC doit également vérifier les exigences d'autocertification, c'est-à-dire vérifier que toutes les entreprises autocertifiées ont choisi un organisme indépendant de règlement des litiges et vérifier la publication de la politique des entreprises en matière de protection de la vie privée.

Le DoC s'attaquera désormais à la question des entreprises qui se prévalent indûment de leur participation par:

(1) l'examen des entreprises supprimées de la liste et la vérification qu'elles ne prétendent plus participer au bouclier de protection des données;
(2) l'examen des entreprises qui doivent être supprimées de la liste parce qu'elles n'ont pas renouvelé leur autocertification, s'en sont retirées ou en ont été supprimées pour non-respect persistant;
(3) toute autre mesure permettant de détecter les affirmations inexactes;
(4) l'examen diligent de toute question ou plainte reçue concernant des affirmations inexactes et par l'adoption de mesures correctives, y compris des poursuites.

Le DoC examinera la conformité d'une entreprise participante si elle reçoit une plainte, si une entreprise ne répond pas à ses demandes concernant l'application du bouclier et s'il existe un doute raisonnable concernant le respect des principes de la part de l'entreprise[104]. Enfin, le DoC créera des points de contact spécifiques afin d'améliorer la

---

[103] Voir également C. Hoofnagle «US Regulatory Values and Privacy Consequences», *European Data Protection Law Review*, vol. 2 (2016), n° 2, p. 169, qui estime que la loi américaine devrait davantage mettre l'accent sur les pratiques déloyales que sur celles de nature à induire en erreur, ce qui lui permettrait de se rapprocher de la perspective européenne en matière de protection des données.

[104] Le GT art. 29 a salué dans son avis d'avril 2016 les compétences d'enquête du DoC ainsi que sa capacité à procéder de droit à des vérifications, en particulier par l'envoi de questionnaires. Toutefois, il s'est interrogé sur les pouvoirs exacts des autorités de contrôle américaines en matière d'inspections sur site, dans les entreprises autocertifiées, concernant d'éventuelles violations du bouclier de protection

coopération avec les APD et de recevoir les plaintes des personnes concernées concernant l'application du bouclier par une entreprise participante qui lui ont été renvoyées par les APD.

### 4.3.2. *Commission fédérale du commerce*

L'action de la commission fédérale du commerce (Federal Trade Commission, FTC) ne semble pas avoir changé fondamentalement. Toutefois, la FTC doit désormais donner la priorité aux plaintes pour non-respect renvoyées par a) les organismes indépendants de règlement des litiges; b) les APD européennes; c) le DoC. Comme mentionné ci-dessus, les personnes concernées peuvent toujours déposer une plainte directement auprès de la FTC.

**Encadré 6 — La commission fédérale du commerce et les procédures de la section 5**

L'autorité légale primaire de la FTC découle de la section 5 du Federal Trade Commission Act[105] qui interdit les pratiques commerciales déloyales ou trompeuses. La section 5 du Federal Trade Commission Act a un large champ d'application (pour le moins aussi large que la compétence de la FTC, ce qui signifie qu'elle ne s'applique pas aux domaines exclus de la compétence de la FTC)[106]. La FTC a compétence pour connaître à la fois des affaires de fausses déclarations (c'est-à-dire les cas dans lesquels les entreprises font des déclarations et des promesses frauduleuses à leurs clients) et des affaires dans lesquelles les entreprises omettent un fait matériel (ce dernier peut également renvoyer à des données, par exemple dans les cas où l'entreprise ne notifie pas au consommateur qu'elle collecte des informations à caractère personnel le concernant). Les actions de la FTC au titre de la section 5 peuvent être intentées contre toute entreprise sous sa juridiction. La section 5 s'applique aux actions intentées aux États-Unis ou ayant des effets aux États-Unis. À la lumière de ces éléments, la section 5 peut être employée pour examiner les plaintes de citoyens de l'Union européenne lésés par les agissements d'une entreprise américaine (ainsi, dans l'affaire Best Price Brand[107] relative au «Safe Harbour», une action a été intentée contre une entreprise américaine active sur le marché britannique). Toutefois, la commissaire de la FTC Julie Brill a estimé que l'invalidité du cadre du «Safe Harbour» réduisait la capacité de la FTC à faire respecter la réglementation dans les affaires entre des parties de part et d'autre de l'Atlantique. Ceci est exact dans la mesure où le cadre du «Safe Harbour» obligeait les entreprises participantes à publier des déclarations de protection des données sans ambiguïté, transparentes et contraignantes. Le non-respect de cette déclaration pouvait déclencher une action de la FTC. Les déclarations de protection des données de la sphère privée devant être publiques et transparentes, elles facilitaient l'action de la FTC en provoquant des plaintes pour fausses déclarations. Des actions au titre de la section 5 ont parfois été intentées pour des violations commises à l'étranger[108]. Le bouclier de protection des données rétablit cette exigence de transparence et de publicité des politiques des entreprises en matière de protection de la vie privé, facilitant ainsi les plaintes portées devant la FTC.

La FTC peut employer principalement deux méthodes pour porter une plainte devant les tribunaux[109]. La première consiste à intenter une action devant les tribunaux fédéraux. Cette

des données et sur la façon dont l'exequatur d'une décision d'une autorité de l'Union européenne pouvait être obtenue sur le territoire des États-Unis.

105 Federal Trade Commission Act.

106 Voir note de bas de page 9.

107 *Best Priced Brands, LLC, et al*

108 Voir par exemple l'affaire *GMR Transcription Services* dans laquelle le sous-traitant à l'étranger d'une entreprise américaine avait, lors du traitement des données, enfreint les règles relatives au respect de la vie privée; la FTC a intenté une action contre l'entreprise américaine car celle-ci n'avait pas été en mesure de vérifier de façon appropriée les agissements du sous-traitant.

109 Pour plus d'informations concernant ces méthodes, consultez le site internet de la FTC (dernière consultation le 9 novembre 2016).

méthode a par exemple été utilisée dans l'affaire Best Priced Brand susmentionnée. Cette méthode est souvent utilisée dans les affaires de fraude dans lesquelles la FTC désire obtenir une décision de justice gelant les actifs d'une entreprise qui pourraient sinon disparaître avant la fin de l'enquête. L'autre méthode est interne et comporte des procédures d'enquête et administratives (voir par exemple l'affaire Google, Inc., In the Matter of)[110]. Si le défendeur ne se conforme pas à la décision, la FTC peut exiger des astreintes. Ce fut le cas dans certaines des affaires relatives au «Safe Harbour» introduites par la FTC[111].

### 4.3.3. *Services de renseignement et application de la loi aux États-Unis*

Aux termes du bouclier de protection des données, «l'adhésion aux principes peut être limitée par les exigences relatives à la sécurité nationale, l'intérêt public et le respect de la législation [...]» (annexe II, I.5). Les pouvoirs publics américains sont donc, dans certaines circonstances, autorisés à accéder aux données à caractère personnel (européennes) et à les utiliser. Concernant l'étendue et le caractère justifiable de ces dérogations dans une société démocratique (l'un des principaux enjeux dans l'arrêt Schrems), cette évaluation concerne le cadre juridique américain donnant accès aux données aux services de renseignements et à d'autres autorités américaines mentionnées dans les annexes du bouclier de protection des données[112]. La commissaire Jourová a fourni l'assurance que la Commission avait répondue aux opinions exprimées dans la résolution du Parlement européen et du groupe de travail «article 29» pour renforcer les garanties offertes par le bouclier de protection des données. Concernant la question de la collecte massive de données, la Commissaire a confirmé avoir reçu des autorités américaines des assurances supplémentaires que la collecte massive de renseignements d'origine électromagnétique (c'est-à-dire de signaux de communication)[113] de la part de la communauté américaine du renseignement sera exceptionnelle et «aussi ciblée que possible» lorsque d'autres mesures sont techniquement impossibles (tel que mentionné dans les annexes III-A, VI and VII of the PS).[114] Ces assurances ont permis à la Commission de conclure que le traitement des

---

[110] Voir par exemple l'arrêt relatif à le Safe Harbour portée devant la FTC dans l'affaire Google concernant le retrait du réseau social Buzz.

[111] Voir par exemple l'affaire Facebook et *l'affaire* Myspace.

[112] À savoir: le Foreign Intelligence Surveillance Act (FISA), l'Executive Order (décret) 12333, le USA Freedom Act, et la directive politique présidentielle n° 28 de 2014 (PPD-28) (bien que cette dernière ne constitue pas une des bases juridiques de la collecte).

[113] Le GT art. 29 a fait observer dans son avis le manque de définition des renseignements d'origine électromagnétique dans tous les textes applicables.

[114] En particulier, le **USA Freedom Act** de 2015 (conforme au quatrième amendement de la constitution américaine) a introduit des règles de minimisation de l'accès des pouvoirs publics aux données sur la base du **FISA** qui, dans sa **section 702** par exemple, qui est soumise aux exigences de la PPD-28 (annexe VI), permet aux services de renseignement américain de mener des programmes de surveillance (comme PRISM) et de chercher à se procurer des informations dans les communications électroniques de citoyens non américains se trouvant à l'étranger qui sont supposés être des «cibles légitimes identifiées individuellement». La **PPD-28 de 2014** impose des limitations aux opérations de renseignement d'origine électromagnétique des services de renseignement. Ces renseignements ne peuvent être collectés que lorsqu'une finalité de renseignement vis-à-vis de l'étranger existe dans la mesure du possible et doivent être «orientés sur des cibles ou des sujets spécifiques du renseignement étranger moyennant l'utilisation de discriminants» (termes ou identifiants spécifiques, comme des adresses électroniques). La PPD-28 spécifie également que la collecte doit se fonder sur une loi, être conforme à la constitution américaine et respecter la dignité de toutes les personnes. Elle précise également que les services de renseignement peuvent collecter en masse des renseignements dans certaines circonstances, lorsque l'utilisation de discriminants n'est pas possible «pour des raisons techniques ou opérationnelles» afin de détecter de nouvelles menaces, mais qu'elle doit être aussi limitée que possible (c'est-à-dire, être concentrée sur un territoire) et employer des outils de filtrage

données restait dans les limites de nécessité et de proportionnalité demandées par la CJUE.

Concernant les mécanismes de surveillance[115] et **de recours** dans le contexte de l'accès aux données par les services répressifs et de renseignement, la Commission a salué le nouveau rôle du médiateur (annexe III, a) qui a l'obligation de répondre aux plaintes des personnes en confirmant le respect des règles ou en remédiant au non-respect. La Commission a confirmé avoir reçu l'assurance que le médiateur serait indépendant des services de renseignement (voir toutefois la déclaration du groupe de travail «article 29» dans la section 5.1.2).

**Encadré 7 — Voies de recours pour consultation et utilisation abusives des données par les pouvoirs publics américains**

En ce qui concerne les voies de recours pour consultation et utilisation abusives des données par les pouvoirs publics américains à des fins de sécurité nationale, les voies suivantes sont les voies principales ouvertes aux personnes[116] qui sont mentionnées dans la décision d'exécution de la Commission concernant le bouclier de protection des données:

(1) Aux termes du Foreign Intelligence Surveillance Act (FISA), les citoyens non américains peuvent demander réparation pour une surveillance électronique illégale[117]. Néanmoins, la portée des recours du FISA reste limitée et les conditions qu'il impose actuellement aux réclamations se sont avérées difficiles à remplir. Le FISA est complété par le Freedom of Information Act (FOIA) qui permet aux personnes de demander la consultation des archives des organismes fédéraux. Les possibilités sont toutefois limitées, par exemple par les exceptions s'appliquant aux informations classifiées de sécurité nationale ou celles concernant des enquêtes menées par les services répressifs.[118]

(2) D'autres bases juridiques spécifiques sont fournies par le Computer Fraud and Abuse Act, l'Electronic Communications Privacy Act et le Right to Financial Privacy Act. Ces voies de

réduisant au minimum la collecte de données non pertinentes. L'utilisation des données ainsi collectées serait limitée à **six cas spécifiques** à finalité de sécurité nationale (y compris la lutte contre le terrorisme) qui, néanmoins, selon le GT art. 29, sont trop larges pour éliminer la possibilité d'une collecte sans discrimination: «[aux termes de la PPD-28], les possibilités de collecte restent vagues et potentiellement de grande ampleur» (avis du groupe de travail «Article 29», p. 38). Selon le bureau du directeur du renseignement national (Office of the Director of National Intelligence, ODNI) (annexe VI du bouclier), les renseignements d'origine électromagnétique collectés par les autorités américaines ne représenteraient qu'une fraction des communications passant par internet et la collecte en vrac ne signifierait pas la collecte en masse ou sans discrimination de données. Ceci est un aspect du débat (et, fréquemment, un sujet de divergence) entre l'Union européenne et les États-Unis d'Amérique car le droit européen considère la collecte de données (et non pas seulement l'accès aux données) comme un traitement de données soumis aux règles de la protection des données (y compris le consentement et d'autres bases juridiques).

[115] Par exemple, les activités de renseignement fondées sur le FISA sont soumises à un examen et, dans certains cas, à une autorisation préalable de la part de la cour du FISA (FISC), dont les décisions peuvent être attaquées devant la cour d'appel appropriée et, en fin d'analyse, devant la Cour suprême des États-Unis. Son contrôle semble toutefois être limité à la condition que la finalité de l'acquisition des données soit d'obtenir des informations de renseignement étranger et il ne garantit pas un contrôle juridictionnel efficace du ciblage de citoyens non américains (GT art. 29, avis, p. 43).

[116] La nécessité de préciser que des mécanismes et des droits de recours sont garantis aux personnes dont les données sont transférées de l'Union européenne aux États-Unis (c'est-à-dire les résidents et non pas seulement les citoyens de l'Union) fait l'objet d'une insistance particulière de la part du GT art. 29 dans son avis d'avril 2016 (p. 14). Voir également le guide de la Commission à l'intention des citoyens.

[117] 50 US Code § 1810 — responsabilité civile.

[118] La personne dans cette situation ne peut recevoir qu'une réponse dans laquelle l'organisme confirme ou dément l'existence d'archives.

recours ne concernent que des données, des cibles et des types d'accès aux données spécifiques. Il existe une voie administrative plus générale de demande de contrôle juridictionnel lorsqu'une personne subit «un dommage du fait d'une décision d'une agence ou est affectée ou lésée par la décision d'une agence»[119]. La décision d'exécution ne fait toutefois pas mention du niveau de preuve requis pour intenter une action dans le cadre de ce recours administratif plus général.

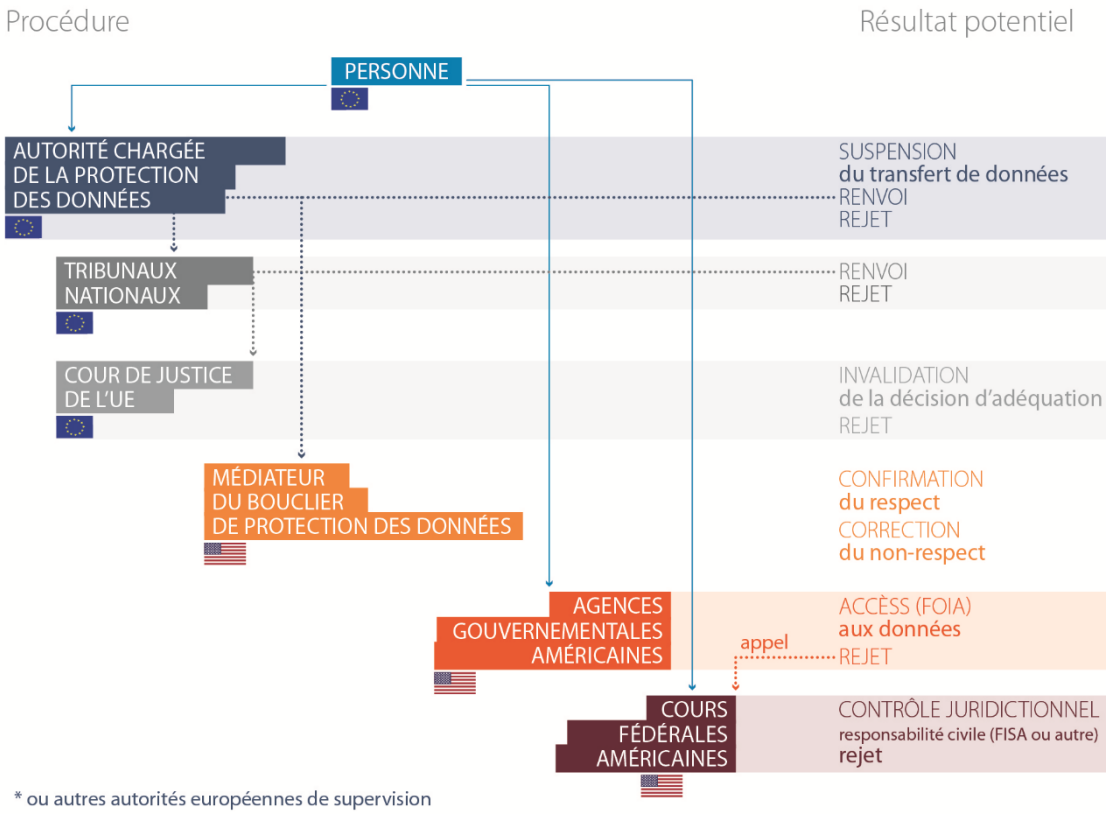
(3) Le bouclier de protection des données crée un nouveau mécanisme de **médiateur du bouclier de protection des données** qui doit garantir que les plaintes des personnes sont dûment examinées et traitées. Le médiateur est assisté de structures (préexistantes) indépendantes d'enquête comme les inspecteurs généraux[120] et le conseil de surveillance de la vie privée et des libertés civiles (PCLOB). Ce dernier a été institué en tant qu'organisme bipartite indépendant au sein du pouvoir exécutif dont le rôle principal est de veiller à ce que l'action de l'exécutif américain en matière de lutte contre le terrorisme respecte la vie privée et les libertés civiles[121]. Des obligations légales de transparence publique s'imposent à lui.

[119] Droit de révision dans l'Administrative Procedure Act, 5 US Code § 702.

[120] Les inspecteurs généraux (IG) sont chargés de contrôler les activités de chaque entité du secteur du renseignement. Ils mènent des inspections et des enquêtes concernant les activités des entités du secteur de renseignement.

[121] Recommandations du 9/11 Commission Act, Pub. L. 110-53, devenues loi en août 2007 (42 USC §2000ee et suiv.). Un récent examen du dispositif de contrôle s'est intéressé aux programmes de surveillance menés en vertu de la section 701 du FISA. Il convient de noter que le PCLOB a accès à l'ensemble des archives, rapports, documents et autres pièces pertinents des organismes fédéraux, y compris les informations classifiées, conformément à la loi (annexe VI, p. 96).

**Figure 2 — Voies de recours pour consultation et utilisation abusives par les pouvoirs publics américains**




# 5. Vers un outil satisfaisant et durable?

## 5.1. Réactions à la nouvelle version du bouclier de protection des données

Différentes réactions ont été enregistrées dans la foulée de l'adoption du nouveau régime. La plupart des représentants des milieux économiques en Europe et aux États-Unis ont salué le nouvel accord[122]. Néanmoins, l'arrivée à sa conclusion de la procédure formelle d'adoption ne semble pas signaler la fin du débat pour de nombreux observateurs et décideurs. L'accord ne semble pas non plus complètement faire taire les critiques exprimées dans la foulée de la publication du nouveau bouclier de protection des données[123]. En particulier, la **viabilité à long terme** du bouclier en tant qu'instrument permettant de protéger le droit à la vie privée de manière efficace et conformément aux

---

[122] Voir la déclaration de Digital Europe exprimant l'opinion du secteur européen des technologies numériques; voir également N. Drozdiak, «The EU Agree on Final Adjustments to Data Privacy Shield», *Wall Street Journal*, 24 juin 2016.

[123] Jan Philipp Albrecht (Verts/ALE, Allemagne, également rapporteur pour le RGPD) a par exemple affirmé: «La Commission vient de signer un chèque en blanc pour le transfert des données personnelles des citoyens de l'Union européenne vers les États-Unis [...] La Commission ne devrait donc pas se contenter du discours se voulant rassurant des autorités américaines mais exiger de meilleures garanties pour la protection des données des consommateurs européens.» Albrecht a en particulier critiqué le fait que la collecte massive des données personnelles à caractère personnel par les services de renseignement américains reste possible malgré les limitations (six possibilités d'accès) et a observé que la PPD-28 n'était pas équivalente à une loi américaine et qu'elle pouvait être unilatéralement retirée par n'importe quel président des États-Unis à l'avenir. Jan Philipp Albrecht a également estimé que la décision d'adéquation devait être renégociée lorsque le nouveau règlement général de protection des données entrera en vigueur au début de l'année 2018.

normes européennes doit encore être confirmée. Certains décideurs européens et certaines associations de consommateurs au sein de l'Union européenne sont sceptiques.

Les critiques ont en outre mis en avant un certain nombre d'insuffisances.

### 5.1.1. *Défenseurs de la vie privée*

Concernant les **aspects commerciaux**, il est considéré que le bouclier de protection des données autorise le traitement des données à des fins très larges et générales, contrairement au principe de limitation de la finalité consacré dans le droit de l'Union. Dans les faits, le texte du bouclier exige de toute entreprise qu'elle informe les personnes «des fins auxquelles elle collecte et utilise des informations à caractère personnel les concernant»; toutefois, la précision avec laquelle ces fins doivent être présentées reste incertaine car le bouclier n'exige pas des entreprises de spécifier l'utilisation concrète à laquelle les informations sont destinées. De plus, des observateurs ont relevé que le bouclier de protection des données serait basé sur un système de «refus» (notification et choix) exigeant des utilisateurs de s'opposer activement au traitement de leurs données par une entreprise (s'ils ont conscience d'un tel traitement), **ce qui va à l'encontre du système européen de «consentement»** qui exige des entreprises d'obtenir le consentement préalable de l'utilisateur. Concernant les mécanismes de recours à l'égard d'une entreprise, il a été souligné que **le système reste très complexe** et, nonobstant les efforts en matière de coûts, pourrait demeurer inaccessible aux citoyens de l'Union (les citoyens devraient par exemple contacter l'entreprise en premier lieu puis s'adresser, après les avoir identifiés, aux différents organismes privés d'arbitrage ou aux différentes autorités nationales, la FTC et le DoC, puis, après ceux-là seulement, au «panel d'arbitrage du bouclier de protection des données» pour obtenir une sentence arbitrale contraignante). Dans le cas où l'entreprise n'exécuterait pas la sentence du nouveau «panel du bouclier de protection des données», il reviendrait à un tribunal de faire respecter celle-ci[124].

Concernant les insuffisances dans le domaine de la «**surveillance**», le principal problème semble résider dans la référence explicite à la «collecte en vrac» des données par les autorités américaines (annexe VI), bien que son emploi soit limité à six cas à des fins de sécurité nationale (largement définies). Concernant les voies de recours dans ce domaine, le rôle du médiateur est considéré comme insatisfaisant pour deux raisons. Tout d'abord, il est considéré que le médiateur ne pourra pas traiter de façon appropriée les plaintes concernant la surveillance des données par les autorités américaines car il ne sera pas capable de confirmer si une personne a fait l'objet de mesures de surveillance ou non. Cette question restera soumise au FOIA uniquement, dans la limite d'exceptions spécifiques toutefois. Le médiateur et les services indépendants d'enquête collaborant avec lui limiteront donc leur enquête à la question de savoir si les services de renseignement ont violé la loi par leurs actions. La seconde objection soulevée par les observateurs concerne le fait que le médiateur ne serait pas un tribunal indépendant mais un sous-secrétaire du département d'État américain. Bien que cette situation puisse donner au médiateur plus facilement accès à certaines informations lui permettant d'évaluer les activités faisant l'objet d'une plainte, et bien que le bouclier de protection des données mentionne à de nombreuses reprises l'indépendance du médiateur, les observateurs n'ont pas constaté la présence des garanties requises. C'est pourquoi le

[124] Voir la déclaration de Max Schrems, *Bouclier de protection des données — Petit-déjeuner avec la presse en compagnie du député européen Jan Albrecht*, 12 juillet 2016.

médiateur ne garantirait pas le droit à un recours efficace et à un procès équitable exigé par l'article 47 de la charte des droits fondamentaux[125].

Des critiques semblables ont été formulées par le **Bureau européen des unions de consommateurs** (BEUC) qui s'est déclaré déçu que le bouclier de protection des données sous-tende le transfert des données sans protéger suffisamment les citoyens de l'Union européenne. Si un cadre est jugé nécessaire («car la manipulation des données personnelles à des fins commerciales n'est soumise à aucune réglementation aux États-Unis»), le bouclier de protection des données, considéré comme le produit de pressions politiques et commerciales du gouvernement des États-Unis et du secteur technologique américain, n'offre pas un niveau satisfaisant de protection[126].

5.1.2. *Groupe de travail «article 29» et Contrôleur européen de la protection des données*

Le **groupe de travail «article 29» a publié sa déclaration** concernant la décision d'adéquation du bouclier de protection des données modifié deux semaines après la publication de cette dernière[127]. Dans celle-ci, le groupe des APD européennes a salué les améliorations présentes dans la version finale mais exprimé un certain nombre de préoccupations qui subsistent au sujet des aspects commerciaux et de l'accès des pouvoirs publics américains aux données. Sur le premier point, cette déclaration mentionne l'insuffisance des règles spécifiques concernant les décisions automatisées ainsi que le droit de s'opposer au traitement et le manque de clarté concernant l'application du nouveau cadre aux responsables du traitement des données. Concernant les dérogations à des fins de sécurité et l'accès des pouvoirs publics américains aux données, le groupe de travail «article 29» est préoccupé par le manque de garanties plus strictes sur **l'indépendance et les pouvoirs du médiateur** dans le nouveau bouclier. Concernant la collecte en vrac de données (l'un des problèmes les plus épineux dans l'ensemble du débat sur le bouclier), le bureau du directeur du renseignement national américain (ODNI) s'est engagé à ne pas conduire de collecte massive et sans discrimination de données. Néanmoins, les APD de l'Union ont exprimé leur

---

[125] *Ibid*. Max Schrems considère que le nouveau bouclier de protection des données pose toujours question concernant la surveillance généralisée et, en particulier, l'accès des services de renseignement à certaines données, par exemple pour des raisons de menace terroriste, même si celui-ci est limité. Selon lui, la définition reste trop vague et il est également inquiet des difficultés que rencontreront les Européens pour faire appel considérant que les mécanismes de recours sont particulièrement complexes et pourraient imposer aux plaignants d'attendre «des années».

[126] BEUC, communiqué de presse, 12 juillet 2016, «La protection de la vie privée des citoyens européens mise à mal par le Privacy Shield», rapportant les déclarations de la directrice du BEUC, Monique Goyens, selon lesquelles, en ne se souciant pas de défendre sa réglementation de protection des données de manière adéquate, la Commission a permis aux motivations commerciales de l'emporter sur le droit des citoyens à la vie privée («D'ordinaire, les consommateurs ignorent ou ne contrôlent pas où les entreprises envoient leurs données personnelles.»). Si ce communiqué reconnaît quelques améliorations, il estime que «les mécanismes de recours pour les consommateurs et, de manière générale, la valeur et structure du mécanisme, restent plus confus et compliqués que jamais». Par ailleurs, un recours devant la Cour n'est pas à exclure. Et de conclure: «Un problème fondamental subsiste en effet, à savoir que le côté américain du bouclier est fait d'argile et non de fer».

[127] Voir la déclaration du GT art. 29 concernant la décision de la Commission européenne sur le bouclier de protection des données UE–États-Unis. De plus, le GT art. 29 a fait remarquer le manque de clarté concernant l'utilisation des «interceptions sur câble» (*cable interceptions*) par le renseignement américain pour les données en transit vers les États-Unis, interceptions dont la légalité n'a, jusqu'ici, pas été établie dans la jurisprudence. Par ailleurs, la notion de renseignement d'origine électromagnétique n'est définie dans aucun texte applicable.

préoccupation face au fait qu'aucune **assurance concrète** que ce type de surveillance serait évité ne figurait dans le bouclier de protection des données.

Le **premier examen conjoint annuel** (prévu pour l'été 2017) constituera, de l'avis du GT art. 29, une étape cruciale de l'évaluation de l'efficacité et de la solidité du bouclier de protection des données. L'objectif de cet examen devrait être, selon le GT art. 29, de vérifier si les problèmes persistants ont été résolus et si les garanties fournies par le bouclier sont efficaces. Il convient de noter que les résultats du premier examen conjoint devraient également avoir des effets sur les autres instruments de transfert comme les règles d'entreprise conjointes et les clauses contractuelles types en confirmant leur force juridique[128]. De plus, le GT s'est engagé à aider activement les **personnes concernées** à gérer leurs plaintes et à fournir des suggestions aux responsables du traitement des données leur permettant de respecter leurs obligations au titre du bouclier de protection des données. Enfin, le GT art. 29 semblait (par le soutien apporté à l'assertion de la commissaire Jourová) enclin à donner une chance au nouveau bouclier, en adoptant toutefois une **position prudente** plutôt qu'en lui donnant une véritable approbation (tout au moins dans l'attente de l'examen annuel prévu).

Les paroles du **CEPD**, Giovanni Buttarelli, permettent de mieux comprendre l'importance donnée par les observateurs à l'existence de mécanismes de contrôle et de systèmes efficaces et rapides de recours: «Il y a eu croissance exponentielle des volumes de données à caractère personnel collectées, stockées et transférées, informations qui, à un degré de plus en plus élevé, ne sont pas fournies par la personne elle-même mais plutôt observées, déduites ou calculées par quelqu'un d'autre. Pour que les Droits de l'homme aient un sens quelconque, il est donc essentiel que quelqu'un soit responsable de la façon dont ces données sont employées»[129]. De plus, concernant la «longévité prévisible» du bouclier de protection des données, il a estimé que «nous avons besoin d'un modèle robuste de fonctionnement des accords bilatéraux de partage des données [...]. L'exercice pratiqué actuellement entre l'Union européenne et les États-Unis pourrait maintenant devoir être répété avec d'autres partenaires commerciaux». Giovanni Buttarelli a, en définitive, l'espoir qu'avec l'entrée en vigueur complète du **RGDP** (2018), «nous pourrons aboutir à une norme commune, une espèce d'étalon-or numérique, qui accompagnera la mondialisation et tous les défis qu'elle pose aux individus et à la société ainsi que tous les avantages qu'elle leur offre»[130].

---

[128] Les détails de l'organisation pratique de l'examen conjoint et des compétences des APD durant cet examen font l'objet d'attentes spécifiques: dans cette même déclaration, le GT art. 29 demande que les membres du comité d'examen puissent accéder à toutes les informations nécessaires pour l'examen, c'est-à-dire qu'il leur soit permis de vérifier la nécessité et la proportionnalité de la collecte et de la consultation des données par les pouvoirs publics.

[129] Giovanni Buttarelli, «The EU GDPR as a clarion call for a new global digital gold standard», éditorial en collaboration spéciale, *International Data Privacy Law*, Oxford Journals Law, 2016, vol. 6, n° 2, p. 77-78. Il a également souligné que «les individus font l'objet d'inférences granulaires tirées des statistiques au moyen de systèmes sophistiqués d'analyse fondés sur des algorithmes dont ils ne sont, dans le meilleur des cas, que partiellement conscients. Ils sont menacés par un traitement des données inéquitable ou discriminatoire qui conforte les stéréotypes et l'exclusion sociale. La responsabilisation devrait favoriser un traitement des données durable en garantissant que la charge de l'évaluation de la légalité et de l'équité de traitements complexes repose principalement sur les responsables du traitement et sur les régulateurs, et non sur l'individu».

[130] *Ibid*.

## 5.2. Perspectives

Si le bouclier de protection des données peut être considéré comme achevé du point de vue formel, l'histoire ne s'arrête pas là.

- Tout d'abord, **l'examen annuel** conjoint, comme mentionné, devrait avoir lieu d'ici l'été 2017.
- Bien que le nouveau texte du bouclier de protection des données contienne déjà, afin de l'adapter au RGDP, des aspects qui n'étaient pas abordés par la directive sur la protection des données (comme les transferts ultérieurs de données), une évaluation du bouclier devrait avoir lieu lorsque le **RGDP** entrera pleinement en vigueur, en **mai 2018**, afin de procéder aux améliorations nécessaires[131].
- Le **Parlement européen** devrait adopter une **nouvelle résolution** concernant le bouclier de protection des données dans un proche avenir[132].
- Concernant l'**attitude des entreprises** (qui peuvent décider de s'en tenir aux autres instruments): du point de vue pratique, certains universitaires[133] suggèrent que, dans un avenir proche, les entreprises pourraient également adopter une attitude volontariste en réduisant au minimum les données et en les rendant anonymes (réduisant ainsi les cas de traitement de données soumis à la réglementation européenne de protection des données). Les entreprises semblent aussi avoir été assez prudentes dans leur adhésion au bouclier de protection des données: à la fin du mois d'octobre 2016, environ 1 500 entreprises s'étaient soumises à une certification (500 d'entre elles bénéficiant de la certification du DoC au 18 octobre 2016)[134]. Ce nombre est beaucoup moins élevé que les 4 000 entreprises qui avaient adhéré au «Safe Harbour». Il peut y avoir plusieurs explications à cela: 1) le temps nécessaire pour comprendre les règles et s'y adapter avant de demander une certification; 2) les entreprises sont prudentes et peuvent craindre de nouveaux recours contre le bouclier de protection des données, alors que ce dernier semble plus coûteux à appliquer que le Safe Harbour.
- Les négociations du PTCI concernant les flux de données ont été temporairement suspendues pendant que l'Union européenne et les États-Unis d'Amérique négociaient une solution sur les questions de protection des données, y compris le bouclier de protection des données. En raison de l'adoption de la décision d'adéquation de la Commission concernant le bouclier de protection des données et son approbation par les États membres le 8 juillet 2016, les négociations sur le commerce électronique et les flux de données peuvent reprendre. Les dispositions autorisant les transferts de données sont partie intégrante de certains chapitres des

---

[131] Comme souligné par G. Buttarelli, *op. cit.*, la CJUE «applique ces règles [RGDP] strictement en les interprétant à la lumière de la charte des droits fondamentaux de l'Union européenne et en favorisant les droits et les intérêts de l'individu plutôt que les objectifs des entreprises ou les objectifs commerciaux, quelque raisonnables et légitimes que soient ceux-ci».

[132] Un projet de proposition de (nouvelle) résolution concernant le caractère adéquat de la protection offerte par le bouclier de protection des données UE–États-Unis (exprimant certaines préoccupations persistantes) a été discuté en commission LIBE lors de sa première réunion de l'année 2017.

[133] Voir A. Montelero, *op. cit.*

[134] US Department of Commerce marks posting of 500th company on Privacy Shield Framework list, International Trade Administration (ITA), 18 octobre 2016.

accords commerciaux, en particulier dans les services financiers et numériques[135]. Ces dispositions contiennent des exceptions particulières offrant des garanties adéquates de protection de la vie privée[136]. L'Union européenne introduit également des règles de protection de la vie privée dans les exceptions générales d'autres accords[137].

- De plus, le bouclier de protection des données pourrait, si ce n'est directement, être pris en considération dans les questions de transfert de données vers **d'autres pays tiers**[138].
- Par ailleurs, l'arrêt Schrems et ses conséquences devraient être pris en compte dans d'autres arrêts de la CJUE, comme récemment dans le cas de l'accord UE-Canada sur les dossiers passagers (PNR)[139].
- Un autre problème est apparu récemment qui nécessitera des discussions supplémentaires, à savoir les conséquences du «**Brexit»**[140] sur le bouclier de protection des données et sur les flux triangulaires de données entre les États-Unis d'Amérique, le Royaume-Uni et l'Union européenne. L'incertitude créée par le «Brexit» pourrait persister pendant deux ans (voire plus) à partir de la notification au titre de l'article 50 du traité UE de la décision du Royaume-Uni de quitter l'Union. Le bouclier de protection des données s'appliquera au Royaume-Uni aussi longtemps qu'il appartiendra formellement à l'Union européenne. Si le Royaume-Uni quittait l'Union européenne, les transferts transfrontaliers de données seraient semblables à ceux vers d'autres pays tiers[141]. Dans le cas où l'Union et le Royaume-Uni décideraient d'appliquer le droit de l'EEE dans leurs relations, le bouclier devrait être appliqué au Royaume-Uni, tout comme le RGPD.
- Enfin, le caractère adéquat du bouclier de protection des données pourrait être attaqué devant les tribunaux nationaux et européens par des personnes, par les APD

---

[135] Sur cette question, voir également l'étude de K. Irion et al, Trade and privacy: complicated bedfellows? *How to achieve data protection-proof free trade agreements*, commandée par le BEUC et al., juillet 2016, Amsterdam, Institut de droit de l'information (IViR).

[136] Sur cette question, voir l'avis de la commission LIBE du Parlement européen d'avril 2015 recommandant que l'accord envisage une exception horizontale sans ambiguïté pour la législation européenne de protection des données.

[137] Ainsi, la protection des données est mentionnée dans plusieurs chapitres de l'AECG; voir par exemple son article 13.15 concernant les services financiers et son article 28.3 concernant les exceptions générales.

[138] Sur ce point, la Commission a publié récemment une communication sur l'échange et la protection des données à caractère personnel à l'ère de la mondialisation exposant sa stratégie pour les nouvelles décisions d'adéquation en matière de transfert de données vers des pays tiers (comme le Japon et la Corée) et mentionnant d'autres mécanismes de transfert de données.

[139] Voir les conclusions de l'avocat général de la CJUE (Mengozzi) sur le projet **d'accord PNR UE–Canada**. Le Parlement européen avait demandé à la CJUE une vérification préliminaire de l'accord en novembre 2014, avant un vote définitif en plénière. L'avocat général a semblé confirmer les préoccupations du Parlement européen concernant sa conformité à la charte européenne. Voir aussi les conclusions du CEPD lors de l'audition du 5 avril 2016.

[140] Le terme Brexit renvoie à la sortie du Royaume-Uni de l'Union européenne, résultat d'un récent référendum.

[141] Dans le premier cas, un niveau adéquat de protection des données doit être garanti pour que les entreprises puissent transférer des données entre l'Union européenne et le Royaume-Uni. Il existe toutefois plusieurs raisons de croire que le Royaume-Uni conservera la réglementation européenne de protection des données (voir la déclaration du commissaire britannique à l'information), de sorte que l'adoption d'une décision d'adéquation permettant les flux de données entre l'Union et le Royaume-Uni serait une formalité. Voir également Christopher Kuner, «The global data protection implications of Brexit», *International Data Privacy Law*, 2016, vol. 6, n° 3.

européennes[142] ou par des associations de défense de la vie privée. En effet, un recours a récemment été déposé par Digital Rights Ireland (DRI) auprès du tribunal de l'Union européenne, la juridiction inférieure de la CJUE[143].

## 6. Principales références

Bender D., «Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective», *International Data Privacy Law*, 2016, vol. 6, nº 2

Boehm F., *A comparison between US and EU data protection legislation for law enforcement purposes*, direction générale des politiques internes, Parlement européen, septembre 2015.

Brill J., «Strengthening International Ties Can Support Increased Convergence of Privacy Regimes», *European Data Protection Law Review*, vol. 2 (2016).

Determann L., «Adequacy of data protection in the USA: myths and facts», *International Data Privacy Law*, 2016, vol. 6, nº 3.

Fielder A., «From an unSafe Harbour to a Privacy Shield full of holes», *Privacy International*, avril 2016;

Hoofnagle C., «US Regulatory Values and Privacy Consequences», *European Data Protection Law Review*, vol. 2 (2016), nº 2.

Irion K. et al, Trade and privacy: complicated bedfellows? *How to achieve data protection-proof free trade agreements*, commandé par le BEUC et al., juillet 2016, Amsterdam, Institut de droit de l'information (IViR).

Kuner C., «Extraterritoriality and regulation of international data transfers in EU data protection law», *International Data Privacy Law* (2015), 5 (4).

Resta G. — V. Zeno-Zencovich (*éds*), La protezione transnazionale dei dati personali. *Dai «SH Principles» al «Privacy Shield»*, Roma Tre Press, 2016.

[142] L'APD de Hambourg, par exemple, semble vouloir demander à la CJUE de contrôler la validité de la nouvelle décision de la Commission.

[143] Comme Reuters l'a rapporté, le recours contre la décision d'adéquation concernant le bouclier de protection des données (T-670/16) a été déposé par DRI contre la Commission européenne le 16 septembre 2016. Dans sa requête, DRI estime que le bouclier de protection des données est «une erreur manifeste d'évaluation de la part de la Commission», arguant que: les principes de protection de la vie privée et les engagements officiels contenus dans les annexes du bouclier ne sauraient constituer des «engagements internationaux» au sens de la directive 95/46/CE; que le FISA autoriserait les pouvoirs publics américains à accéder secrètement de façon généralisée aux communications électroniques; qu'en définitive, la décision attaquée échouera à garantir de façon adéquate le respect intégral des droits des citoyens de l'Union européenne lorsque leurs données sont transférées aux États-Unis d'Amérique.

L'arrêt Schrems de la CJUE d'octobre 2015 n'a pas seulement déclaré invalide la décision de la Commission européenne concernant le régime de transfert de données du «Safe Harbour» UE–États-Unis, il a également statué sur nombre d'exigences cruciales constituant les fondations de la protection des données de l'Union européenne. Celles-ci doivent être prises en considération dans l'évaluation du bouclier de protection des données, le nouveau cadre de transfert des données entre l'Union européenne et les États-Unis d'Amérique.

Moins d'un an après l'arrêt de la CJUE, la Commission a adopté une nouvelle décision d'adéquation dans laquelle elle estime que le régime du bouclier de protection des données offre une protection adéquate aux citoyens de l'Union. Les principales améliorations apportées par le bouclier de protection des données (par rapport à son prédécesseur) ainsi que les réactions critiques à ce nouveau régime sont examinées dans cette étude, tout en considérant néanmoins qu'il devrait être procédé, d'ici l'été 2017, à un examen annuel qui tiendra également compte de l'entrée en vigueur en 2018 du règlement général de protection des données de l'Union européenne.

QA-06-16-293-FR-N

Publication du
**Service de recherche pour les députés**

*Direction générale des services de recherche parlementaire, Parlement européen*

PE 595.892
ISBN 978-92-846-0368-8
doi:10.2861/119924

Le contenu de ce document est de la seule responsabilité de l'auteur et les avis qui y sont exprimés ne reflètent pas nécessairement la position officielle du Parlement européen. Il est destiné aux Membres et au personnel du PE dans le cadre de leur travail parlementaire.