AIX-MARSEILLE UNIVERSITÉ

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE **R**ECHERCHE ET D'**É**TUDES EN **D**ROIT DE L'**I**NFORMATION ET DE LA **C**OMMUNICATION

Mémoire de recherche pour l'obtention du Master

« Droit des médias électroniques »

LE PRIVACY SHIELD : CADRE JURIDIQUE EFFICACE OU ACCORD POLITICO-ÉCONOMIQUE ?

Présenté par **M. Sylvain Longhais**

Réalisé sous la direction de **M. Jean Frayssinet**,

Professeur émérite à l'université d'Aix-Marseille

Année universitaire 2018-2019

AIX-MARSEILLE UNIVERSITÉ

FACULTÉ DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE **R**ECHERCHE ET D'**É**TUDES EN **D**ROIT DE L'**I**NFORMATION ET DE LA **C**OMMUNICATION

Mémoire de recherche pour l'obtention du Master

« Droit des médias électroniques »

LE PRIVACY SHIELD : CADRE JURIDIQUE EFFICACE OU ACCORD POLITICO-ÉCONOMIQUE ?

Présenté par **M. Sylvain Longhais**

Réalisé sous la direction de **M. Jean Frayssinet**,

Professeur émérite à l'université d'Aix-Marseille

Année universitaire 2018-2019

REMERCIEMENTS

Je tiens à remercier M. le Professeur Jean Frayssinet, d'avoir accepté d'orienter mes recherches et de diriger ce mémoire et de m'avoir généreusement prodigué ses précieux conseils.

Je tiens à remercier toute l'équipe de l'IREDIC pour sa bienveillance.

Je remercie toutes les personnes qui se reconnaîtront de leur soutien.

LISTE DES ABRÉVIATIONS

AEDH	Association européenne pour la défense des droits de l'homme
Art.	Article
BCR	Binding Corporate Rules
CalOPPA	California Online Privacy Protection Act
CalECPA	California Electronic Communication Privacy Act
CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography And Marketing
CCPA	Electronic Communication Privacy Act
CEPD	Comité Européen à la Protection des
CJCE	Cour de Justice des communautés européennes
CJUE	Cour de Justice de l'Union européenne
CLOUD Act	Claryfying Lawful Overseas Use of Data Act
CNIL	Commission Nationale de l'Informatique et des Libertés
Comm.	Commentaire
COPPA	Children's Online Privacy Protection Act
CSRE/FISAC	Cour de Surveillance du Renseignement Étranger/Foreign Intelligence Surveillance Act Court
DPA/APD	Data Protection Authority/Autorité de Protection des Données
DPC	Data Protection Commission
DoC	Department of Commerce
EPRS	European Parliament Research Service/Service de recherche du Parlement européen
Et seq.	Et sequentes paginate

FAI	Fournisseur d'Accès à Internet
FBI	Federal Bureau of Investigation
FCC	Federal Communication Commission
FTC	Federal Trade Commission
FTC Act	Federal Trade Commission Act
FISA	Foreign Intelligence Surveillance Act
G29	Groupe de l'article 29
GAFA	Google, Apple, Facebook, Amazon (désigne les grandes entreprises du numérique)
HIPAA	Health Insurance Portability and Accountability Act
Ibid.	Ibidem
ICO	Information Commissioner's Office
La REM	La revue européenne des médias et du numérique
NATU	Netflix, AirBnB, Tesla, Uber (autre désignation pour les grandes entreprises du numérique)
NSA	National Security Agency
OAEP	Office of Aviation Enforcement and Proceedings
QSP	Questions Souvent Posées
PCLOB	Privacy and Civil Liberties Oversight Board
PDG	Président-Directeur Général
PIB	Produit Intérieeur Brut
PII	Personal identifiable information
PME	Petites et Moyennes Entreprises
PNR	Passenger Name Record
PPD	Presidential Policy Directive
PRISM	Planning Tool for Resource Integration, Synchronization, and Management

RGPD	Règlement Général sur la Protection des Données
SCA (Act)	Stored Communication Act
TAFTA	Transatlantic Free Trade Agreement
TTIP	Transatlantic Trade and Investment Partnership
UE	Union Européenne
USA FREEDOM Act	Uniting and Strengthening America by Fulfilling Rights Ensuring Effective Discipline Over Monitoring Act
USA PATRIOT Act	Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USC	U.S Code

SOMMAIRE

INTRODUCTION

Réguler ce qui ne peut être appréhendé physiquement ou par l'esprit humain, semble être le défi majeur du XXIe siècle. Dans ce contexte de dématérialisation constante et de multiplication exponentielle du nombre d'informations de toutes natures, les données personnelles illustrent parfaitement les problématiques auxquelles le Droit doit répondre. En effet, ces données sont par nature nombreuses, volatiles, ubiquitaires ce qui rend leur régulation très complexe. Ainsi, il n'est pas question d'adopter un paradigme basé sur des frontières hermétiques et un contrôle total par le Droit. À l'ère du numérique, lorsque des données sont traitées, elles sont stockées, transférées, dupliquées, transférées à nouveau et ce en moins de temps qu'il ne nous en a fallu pour écrire cette phrase. Et on parle ici de données générées entre autres par quelques 4,3 milliards d'internautes sur Terre.[1] Le nombre de traitements et de transferts à l'échelle mondiale a notamment explosé, suite à l'apparition de nouvelles technologies comme le Big Data ou le Cloud Computing. Entre 2011 et 2013 avec la démocratisation de ces techniques informatiques, IBM estime que 90 % des données mondiales ont été créées.[2]

S'il existe en Europe une législation efficace en matière de droit des données personnelles pour encadrer les flux à l'intérieur de l'espace communautaire, il n'en est pas forcément de même pour les transferts qui sont effectués depuis le territoire de l'Union vers des pays tiers. La définition de transfert de données personnelles qui sera retenue dans les développements ultérieurs est celle issue de la conception européenne. C'est toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.[3] Ces transferts sont nécessaires mais peuvent être dangereux si les données personnelles sont traitées dans des États où la protection des données n'existe pas.

Pour cette raison, le règlement général sur la protection des données impose un certain nombre de règles pour que ces transferts aient lieu. Si certains pays sont autorisés par la Commission à échanger des données entre leur territoire et celui de l'UE conformément aux

[1] KEMP (S.), « Digital 2019: Global Internet Use Accelerates », wearesocial.com, publié le 30 janvier 2019, schémas disponible dans l'annexe 2.
[2] JACOBSON (R.), « 2.5 quintillion bytes of data created every day. How does CPG and Retail manage it? », www.ibm.com, publié le 24 avril 2013.
https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/
[3] Définition du transfert de données, www.cnil.fr.
https://www.cnil.fr/fr/definition/transfert-de-donnees

règles européennes,[4] tel n'est pas le cas pour les États-Unis d'Amérique. En effet, la Commission ne considère pas qu'ils offrent une protection globale suffisante des données personnelles dans leur pays. Par conséquent, il ne peut pas y avoir de décision autorisant tous les transferts de données vers les États-Unis.

Dès les prémices du droit des données personnelles de l'Union jusqu'à aujourd'hui, les États-Unis n'ont pas pu bénéficier de ce constat d'adéquation par la Commission. En effet, les philosophies juridiques de part et d'autre sont trop éloignées. Par exemple, en Europe, la donnée personnelle est toute information qui se rapporte à une personne physique identifiée ou identifiable et cette définition est globale, tandis qu'aux États-Unis, il existe une multitude de définitions, toutes taillées pour une situation bien précise.

Mais les échanges économiques de plus en plus importants, l'évolution des technologies du numérique ainsi que le nombre grandissant de données personnelles échangées ont amené les deux puissances à trouver un consensus. Dès les années 2000, un premier accord a été trouvé. Ce dernier permettait aux organisations américaines de transférer des données depuis l'Europe vers les États-Unis si elles acceptaient de se certifier au titre du Safe Harbor, un programme leur imposant le respect d'un certain nombre de principes relatifs à la protection des données personnelles, négocié de part et d'autre de l'Atlantique. Cet accord très critiqué a perduré jusqu'à son invalidation en 2015. L'absence d'accord signifiait le blocage des flux entre l'UE et les États-Unis ce qui n'était économiquement et politiquement pas envisageable. C'est pourquoi en 2016, le successeur du Safe Harbor, le Privacy Shield est entré en vigueur sur le même mode de fonctionnement. Il s'agira d'étudier en détail cet accord, et plus précisément son rôle dans le cadre des flux transfrontaliers de données entre les États-Unis et l'Union européenne.

Dans le cheminement de ce mémoire, il sera exclu du champ d'études les applications pratiques du Privacy Shield entre les acteurs concernés, afin de favoriser une approche plus transversale du sujet. En effet, le Privacy Shield cristallise un rapport de force très intense sur la question de la protection des données personnelles entre une multitude d'acteurs différents. Certes, il constitue un cadre juridique pour les transferts de données vers les États-Unis en prévoyant un certain nombre de principes que les organisations certifiées doivent respecter pour que de tels transferts soient légaux. D'ailleurs, beaucoup d'analyses issues de la doctrine se sont attelées à le décortiquer et à en faire la critique juridique. Mais, cet accord a été l'objet de vives

[4] Art. 45 du règlement général sur la protection des données, anciennement art. 25 de la directive 95/46/EC.

négociations et il a par conséquent une empreinte politique très marquée. En effet, il s'agit schématiquement de concilier la libre circulation des données à des fins économiques voulue par les Américains et la protection des données des citoyens européens. En ce sens, le Privacy Shield, c'est accepter de mettre le droit au service du politique afin de trouver des intérêts convergents. Reste que le volet d'obligations juridiques aussi critiquable soit-il, existe bel et bien, et que le bouclier de protection est le seul cadre juridique, commun et centralisé permettant les transferts de données personnelles depuis l'Union européenne vers les États-Unis.

Le Privacy Shield constitue-t-il alors un cadre juridique efficace de la protection des données personnelles en matière de transferts ou un simple outil politique et économique dans lequel chacun y négocie ses intérêts propres ?

Force est de constater que sur le fond et la forme, le Privacy Shield a toutes les caractéristiques d'un cadre juridique. Cependant, du fait du contexte, et de l'état des législations européennes et américaines, et de ces nombreuses imperfections il doit être considéré comme un cadre juridique imposé par nécessité (Partie I). Mais cette qualification ne doit pas pour autant occulter le rapport de force omniprésent à la base de ce cadre qui dissimule de fait une approche politico-économique (Partie 2), où les intérêts de chaque partie sont représentés.

PARTIE I : Le Privacy Shield, un cadre juridique imposé par nécessité.

Il est certain que le contexte entourant le Privacy Shield fait de lui un accord imposé par nécessité. En effet, c'est l'invalidation brutale du Safe Harbor qui a précipité l'adoption du Privacy Shield. Il convient dès lors de revenir sur l'avant Privacy Shield et notamment l'arrêt Schrems afin de comprendre le contenu du nouvel accord. Ainsi, en très peu de temps, après le Safe Harbor, il y a le Privacy Shield, en passant par l'arrêt Schrems (Chapitre 1).

Dans l'arrêt Schrems, la CJUE a méthodiquement déconstruit le Safe Harbor afin de démontrer pourquoi il n'était pas conforme avec la législation européenne. Il a donc fallu pour les négociateurs européens et américains reconstruire un accord respectant les prérequis fixés par la CJUE. Cependant, le Privacy Shield est un accord encore fragile (Chapitre 2).

CHAPITRE I : Après le Safe harbor, le Privacy Shield… en passant par l'arrêt Schrems

Il est impératif de contextualiser ce nouveau cadre juridique. Ainsi, il faut noter que l'arrêt Schrems est l'arrêt de mort du Safe Harbor (Section 1). À la suite de cette décision, il a fallu appliquer un pansement juridique visant une meilleure conformité (section 2) sous le nom de Privacy Shield.

Section 1 : L'arrêt Schrems ; Arrêt de mort de l'accord Safe Harbor

Il est important de scinder l'avant de l'après « Arrêt Schrems ». En effet le Safe Harbor, prédécesseur du Privacy Shield souffrait d'un contexte délicat (I) laissant planer le doute sur son adéquation avec la législation européenne. Après son invalidation par la CJUE, s'est imposé le besoin de reconstruire un accord très rapidement (II).

I) Le contexte délicat du Safe harbor

Le contexte délicat entourant le Safe Harbor résulte de l'adoption d'un accord nécessaire, mais laxiste, (A) mais également d'affaires importantes sous-jacentes à l'arrêt Schrems (B) questionnant son utilité. Sous un ciel déjà menaçant, l'arrêt Schrems qui signe l'invalidation du Safe Harbor, est un véritable coup de tonnerre (C).

A) Un accord nécessaire, mais laxiste

Le « Safe Harbour » ou « Sphère de sécurité », c'est la rencontre d'une proposition américaine d'un accord résultant d'une négociation avec les opérateurs américains et la Commission européenne[5] et d'une décision de la part de la Commission décidant de l'adéquation des principes édictés par cet accord à la règlementation européenne en vigueur relative à la protection des données personnelles.[6] C'est donc le reflet d'un compromis politique. La négociation de cet accord a débuté à la fin des années 90 quand la directive 95/46/CE relative à la protection des données personnelles, qui instituait pour la première fois au niveau communautaire, des règles contraignantes en la matière, a été adoptée.

[5] FRAYSSINET (J), « Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les États-Unis : l'accord dit "sphère de sécurité" (ou safe harbour) », *Communication Commerce électronique* n°3, Mars 2001, chron.7 p. 3.

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

Cette dernière contenait notamment des règles relatives au transfert des données personnelles vers des pays tiers dont le principe était que de tels transferts n'étaient possibles, qu'à la condition que le pays tiers assure un niveau de protection adéquat, et de poursuivre en donnant un large éventail d'indices et de critères permettant de reconnaître un tel niveau de protection.[7] Cependant, elle comportait également un certain nombre de dérogations. Ces dérogations par définition permettaient à des responsables de traitements de procéder à des transferts interdits par l'article 25 de la directive par exemple : « lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées. »[8] A contrario, cela signifiait que hors du champ dérogatoire de l'article 26 de la directive, les transferts ne pouvaient pas avoir lieu. Mais les flux de données étaient de plus en plus importants, notamment entre les États-Unis et l'Union européenne du fait du développement numérique combiné à une relation économique privilégiée. Il fallait donc trouver une solution avant la date d'entrée en application de la directive de 1995, pour autoriser et faciliter ces transferts, en sachant qu'au regard de l'article 25 de la directive, les États-Unis n'assuraient pas un degré de protection suffisant. Les transferts non couverts par une dérogation étaient donc illégaux. C'est de ce constat que sont nées les premières négociations en vue d'un accord permettant de trouver une solution pérenne qui ne discréditerait pas pour autant la règlementation européenne. En parallèle, en 1995, la commission fédérale du commerce (Federal Trade Commission ou FTC) commence à s'intéresser aux problèmes de « Online Privacy » et dans un rapport paru en 1998, elle pointe du doigt le fait que la majeure partie des opérateurs de sites en ligne collectent des données personnelles, mais que peu en informent les consommateurs et encore moins dressent de véritables politiques de confidentialité.[9] La même année, le « Children's Online Privacy Protection Act » (COPPA) qui interdit aux opérateurs de sites internet ou de services en ligne, ayant connaissance de la collecte et du traitement d'informations personnelles de mineurs de moins de 13 ans, les pratiques déloyales et trompeuses sur lesdits traitements,[10] est adopté aux États-Unis.

[7] Art. 25 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[8] *Ibid.* Art. 26.
[9] BLANKE M (J), « Safe Harbor and the European Union's Directive on Data Protection », *Albany Law Journal of Science & Technology* n°11, 2000, p.69.
[10] Art. 312.1 du Code des règlements fédéraux des États-Unis d'Amérique.

Les négociations transatlantiques aboutissent à un premier brouillon rendu public en novembre 1998. Au fil des discussions et des modifications, les différentes parties à la négociation parviennent finalement à un accord en mai 2000.[11] Cet accord se divise en deux grandes parties ; la première consiste en l'énumération de sept grands principes et la seconde se matérialise par une rubrique de « questions souvent posées » ou QSP qui contient quinze rubriques ayant pour finalité de compléter les grands principes, de les détailler ou de les expliquer.[12] Cette version fait l'objet d'une décision d'adéquation de la part de la Commission européenne le 26 juillet 2000 qui autorise la mise en œuvre du « Safe Harbour » malgré l'opposition du Parlement.[13]

Ainsi les entreprises américaines qui intègrent le Safe Harbour par le biais d'un mécanisme d'adhésion et d'autocertification doivent respecter des principes s'inspirant de la protection des données personnelles telle qu'elle est conçue dans la directive de 1995 afin de pouvoir opérer des transferts de données personnelles en provenance de l'Union européenne.[14]

Dès la conclusion de l'accord, les critiques ont fleuri.[15] En effet, au regard de la directive, les principes ainsi que les QSP qui y sont attachées, ne sont généralement pas suffisants puisqu'ils ne la reprennent pas point par point et consiste plutôt en un melting-pot des dispositions de la directive tout en laissant une latitude assez importante aux opérateurs américains et en prévoyant un large mécanisme d'exception au bénéfice des autorités américaines. De plus, la définition des termes est très vague comme s'il s'agissait uniquement d'une adéquation de surface. Même s'il fallait donc saluer l'effort, de nombreuses réserves issues de la doctrine notamment du côté européen étaient de mises, concernant l'adéquation juridique à la directive et les mécanismes coercitifs en découlant.[16] Du côté américain, les réserves émises concernaient plutôt l'applicabilité d'un tel accord par les organismes

[11] BLANKE M (J), « Safe Harbor and the European Union's Directive on Data Protection », *Albany Law Journal of Science & Technology* n°11, 2000, p.69.
[12] *U.S.-EU Safe Harbor Framework Documents*, www. 2016.export.gov, dernière mise à jour le 30 janvier 2009 https://2016.export.gov/safeharbor/eu/eg_main_018475.asp.
[13] Résolution A5-0177/2000 du Parlement européen, du 5 juillet 2000 sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis.
[14] FRAYSSINET (J), « Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les États-Unis : l'accord dit "sphère de sécurité" (ou safe harbour) », *Communication Commerce électronique* n°3, Mars 2001, chron.7 p.5.
[15] Avis WP32 du G29, du 16 mai 2000 sur le niveau de protection garanti par les principes du Safe Harbor.
[16] POULLET (Y), « Les Safe Harbor Principles : une protection adéquate ? », www.droit-technologie.org. https://www.droit-technologie.org/dossiers/les-safe-harbor-principles-une-protection-adequate/.

américains qualifiant les règles de conformité de coûteuses, d'impossibles à mettre en place et d'injustes.[17]

L'accord « Safe Harbor » est donc l'illustration parfaite d'un accord fragile politiquement et juridiquement, que des affaires relatives à la protection des données personnelles peuvent progressivement remettre en cause.

B) Les affaires importantes sous-jacentes à l'arrêt Schrems

Les affaires font les changements. L'évolution des standards de protection des données personnelles entre l'Union européenne et les États-Unis confirme cet adage. Si le « Safe Harbor » semblait fragile dès sa conception, il a montré ses limites dans deux affaires au moins, avant que les juges européens ne se chargent de la question et ne décident de l'invalider.[18] Elles démontrent à elles seules le cheminement ayant mené à cette décision. La première concerne le fichier Passenger Name Record (PNR) et a donné d'ailleurs lieu à une décision de la CJUE (1) et la seconde tristement célèbre du scandale PRISM (2).

1) L'affaire PNR USA/UE

C'est un cas intéressant pour au moins deux raisons :

La première tient à sa longévité même si ici il s'agira uniquement de traiter les moments forts matérialisés par l'arrêt de la Cour de justice de l'Union européenne.[19] En effet, ce projet date de l'après-11 septembre en 2001, sous l'impulsion des États-Unis. Ces derniers avaient exigé que les Européens fournissent les données personnelles des passagers des vols transatlantiques, afin de les intégrer dans leurs propres bases de données.[20] L'idée est de pouvoir coordonner les informations collectées par les agences de voyages et les compagnies aériennes sur les voyageurs telles que les itinéraires et les détails de paiements avec les informations détenues par les services de renseignement américains, pour identifier les voyageurs à haut risque en matière de terrorisme.[21] Mais encore aujourd'hui, il y a débat sur l'accord PNR

[17] ASSEY M (J.jr), DEMETRIOS A (E), « The EU-U.S privacy Safe harbour : smooth sailing in trouble waters? », *CommLaw Conspectus* n°9, 2001 p.158.
[18] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.
[19] CJUE, *Affaires jointes C-317/04 et C-318/04* du 30 mai 2006, Parlement européen c/ Conseil de l'Union européenne.
[20] ANONYME, « Lutte contre le terrorisme : Qu'est ce que le PNR, le fichier sur les passagers aériens ? », www.lemonde.fr, publié le 19 novembre 2015.
https://www.lemonde.fr/international/article/2015/11/19/qu-est-ce-que-le-pnr_4813315_3210.html
[21] Rapport avec preuve de la Chambre des Lords du 5 juin 2007 sur le « EU/US Passenger Name Record (PNR) Agreement », p.7.

USA/UE puisque dans un communiqué du 6 mars 2017, l'Association Européenne pour la Défense des Droits de l'Homme (AEDH) émettait de sérieuses réserves quant à l'accès à un nombre croissant de données par de plus en plus d'agents américains, ainsi que des mécanismes dérogatoires trop facilement utilisables. De plus, elle estimait que les reproches faits par l'avocat général de la CJUE sur l'accord PNR Canada/UE (qui reprend par ailleurs des éléments de raisonnement de l'arrêt Schrems[22]) pourraient légitimement trouver à s'appliquer dans ce cas, et potentiellement aboutir à une invalidation par les juges s'ils devaient à nouveau statuer sur l'accord.[23]

La deuxième tient précisément à la portée de l'arrêt des juges européens dans les affaires jointes du Parlement européen contre le Conseil de l'Union et contre la Commission.[24] Une longue bataille débutée en 2003 entre les différentes instances européennes, les unes prônant une approche respectant les droits fondamentaux, les autres plaidant pour une approche économique plus laxiste, débouche sur un accord adopté en 2004 qui fait l'objet d'une décision d'adéquation de la part de la Commission. Cette dernière est portée devant la Cour par le Parlement. La Cour invalide cette décision d'adéquation au motif notamment que l'opération de transfert des données personnelles vers une autorité publique ou judiciaire, conformément à l'article 3 § 2 de la directive relative à la protection des données personnelles est exclue du champ d'application du texte et que par conséquent, la Commission n'avait pas à prendre une décision d'adéquation sur le fondement de la directive.[25] La Cour choisit ici la finalité au détriment de l'activité privée comme point de départ de la collecte de données et exclut donc toute protection. D'ailleurs, force est de constater que cette ambivalence en termes de transferts de données personnelles a poussé la Commission et le Conseil à proposer une décision-cadre, ayant pour but d'encadrer les transferts de données personnelles sur la coopération policière et

[22] Voir à ce titre les conclusions de l'avocat général M. Paolo Mengozzi dans l'avis 1/15 du 8 septembre 2016 sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, www.curia.europa.eu.
[23]ANONYME, « PNR-UE ; un bilan préoccupant », http://www.aedh.eu, publié le 6 mars 2017. http://www.aedh.eu/pnr-ue-usa-un-bilan-preoccupant/
[24] CJUE, *Affaires jointes C-317/04 et C-318/04* du 30 mai 2006, Parlement européen c/ Conseil de l'Union européenne.
[25] VALÉRIE (M), « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, 2006, p.535.

judiciaire en matière pénale et d'imposer une condition de protection adéquate,[26] [27] qui rappelle le principe de protection adéquate posé par l'article 25 de la directive, qui est la base du Safe Harbor.[28] La conséquence de la non-applicabilité de la directive est que les données personnelles des citoyens européens transférées dans le cadre d'un tel accord ne sont pas protégées, puisque le fondement de la protection adéquate s'en trouve nécessairement écarté. L'argument de la Cour est critiquable puisque pour écarter ce fondement, il ne prend que la finalité du transfert en compte, qui est le transfert à une autorité publique, sans s'attacher à l'activité de l'opérateur économique. Dès ce moment, il y a une discordance entre les transferts de données officiels à une autorité publique transitant par un opérateur économique exerçant une activité nécessitant la collecte de données, et le reste des transferts qui eux, tombent sous le coup de la directive et pour lesquels le Safe Harbor trouve à s'appliquer. Mais quand ces données sont officieusement récupérées par des autorités publiques américaines dans le cadre d'un programme de surveillance, on se rend compte que le raisonnement de la Cour prend l'eau.

2) Le scandale PRISM

Le 6 juin 2013, le journal britannique « The Guardian » publie un article qui marque le début du plus grand scandale de surveillance de masse connu à ce jour. Cet article révèle comment les services de renseignements américains et plus précisément la National Security Agency (NSA) collectent les enregistrements téléphoniques de millions de consommateurs de l'opérateur Verizon au sein des États-Unis, mais également entre les États-Unis et le reste du monde. Cette injonction provient de l'ordonnance d'un juge spécifiant la transmission des copies électroniques du détail des enregistrements téléphoniques ainsi que des métadonnées attachées. Cette injonction est assortie d'un ordre de fourniture d'informations permettant l'identification des personnes.[29]

---

[26] CLAVET (S), « Les conséquences de l'accord Passenger Name Record sur la protection des droits fondamentaux en Europe », *Droits Fondamentaux, Revue électronique du CRDH*, rubrique études, www. droits-fondamentaux.u-paris2.fr, 2010 p.5.
https://droits-fondamentaux.u-paris2.fr/sites/default/files/droits_fondamentaux/fichiers/etudes_cooperation_antiterroriste_transatlantique_2.pdf

[27] Proposition de décision-cadre COM/2005/0475 du Conseil et de la Commission du 4 octobre 2005 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

[28] Art. 25 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[29] GREENWALD (G), « NSA collecting phone records of millions of Verizon customers daily », www.theguardian.com, publié le 6 juin 2013.
https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

On se trouve donc dans le cadre d'une collecte de masse de données personnelles à des fins de surveillance par le gouvernement américain. Le lendemain, un autre article est publié, expliquant que la même agence de renseignement a bénéficié d'un accès direct aux systèmes de plusieurs géants du numérique tels que Google, Facebook et Apple par un programme nommé PRISM pour « Planning Tool for Resource Integration, Synchronization, and Management » qui servait de porte d'accès aux données de ces entreprises (on parle en anglais de « backdoor »). Les communications étaient en effet collectées directement depuis les serveurs de ces multinationales.[30] Si certaines de ces entreprises reconnaissent avoir divulgué des données personnelles au gouvernement américain tout en respectant scrupuleusement chaque demande au regard de la loi, d'autres nient complètement avoir connaissance d'un tel programme ou d'avoir fourni quelques données que ce soient. C'est le cas de Apple et de Yahoo.[31]

Fallait-il juridiquement s'insurger de la collecte de masse de ces données personnelles par l'agence de renseignement américain ? En d'autres termes : est-ce que cette collecte était légale ? L'affaire des écoutes et du programme PRISM a soulevé beaucoup de questions en droit américain.

Concernant les enregistrements, si l'on se réfère à la section 215 du USA PATRIOT Act de 2001, elle autorise le gouvernement américain à obtenir une ordonnance de la Cour de surveillance du renseignement étranger (CSRE) ordonnant à un tiers comme un opérateur téléphonique de transmettre n'importe quel enregistrement (ou « chose tangible ») jugé pertinent dans le cadre d'une investigation en matière de terrorisme international, de contre-espionnage et de renseignement étranger.[32]

Concernant l'accès aux données collectées par les géants de la « Tech », la section 702 du Foreign Intelligence Surveillance Act prévoit que l'avocat général (près la CSRE) et le directeur du renseignement national peuvent autoriser conjointement pour une période d'un an maximum à compter de la date effective de l'autorisation, le ciblage de personnes dont on sait

[30] GREENWALD (G), MASCASKILL (E), « NSA Prism program taps in to user data of Apple, Google and others », www.theguardian.com, publié le 7 juin 2013.
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[31] CHERRY (D), *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online*, The Basics, Syngress, 2014, pp. 125 et 127.
[32] ANONYME, « Are they allowed to do that? A breakdown of selected government surveillance programs », www.brennancenter.org.
https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf

raisonnablement qu'elles se situent en dehors des États-Unis pour obtenir des informations intéressant les renseignements étrangers.[33]

Nous ne nous attacherons pas à connaître de la légalité ou de la constitutionnalité de ces textes, mais seulement à dire qu'ils existent et servent de fondements juridiques à toutes ces mesures bien que plusieurs juges fédéraux aient pointé le caractère abusif de ces textes notamment la section 215 du Patriot Act, et que la section 702 du FISA connaît beaucoup de limitations.

Du côté européen, cette collecte massive concernait nécessairement des flux transfrontières rentrant dans le champ d'application de la directive de 95 et intéressant le Safe Harbor puisque la finalité des transferts était de base commerciale. Cependant, le Safe Harbor prévoit une exception assez large. En effet, l'accord stipulait que l'adhésion aux principes pouvait être limitée dans la mesure nécessaire à la sécurité nationale, à l'intérêt public ou aux exigences d'une loi en vigueur.[34] Cela exclut de facto la possible violation du Safe Harbor par les entreprises américaines certifiées. Donc finalement la protection adéquate ne concernait pas plus les transferts ultérieurs à des organisations gouvernementales que les transferts dont la Cour jugeait que leurs finalités étaient le traitement par une autorité publique ou judiciaire.

On peut donc démontrer en premier lieu, que le Safe Harbor montrait de sérieuses limites en matière d'adéquation à la directive puisque les exceptions, dont celles de sécurité et d'intérêt public ne connaissaient aucun garde-fou. En second lieu, on constate qu'au regard de ces révélations, l'argumentation des juges européens dans l'arrêt PNR s'écroule comme un château de cartes. En effet, il semblerait qu'exclure du champ d'application de la directive les transferts passant par des opérateurs privés tiers au motif que la finalité est le traitement par une autorité publique est une argumentation qui peut paraître vide de sens quand le scandale PRISM révèle que tous les transferts y compris ceux faits dans le cadre de la directive font l'objet de collecte après coup par une autorité publique, par le biais d'une ordonnance judiciaire, et que ces derniers sont de faits autorisés par les exceptions prévues par le Safe Harbor.

D'un côté il y a donc un accord très imparfait et d'un autre, des juges européens qui n'ont pas d'autres choix que de l'invalider puisqu'en l'état, les données personnelles des

[33] Art. 702, H.R. 6304 (110th), Acte d'amendements du FISA de 2008.
[34] *U.S.-EU Safe Harbor Framework Documents*, www. 2016.export.gov, dernière mise à jour le 30 janvier 2009. https://2016.export.gov/safeharbor/eu/eg_main_018475.asp.

européens dans le cadre des flux transfrontières avec les États-Unis ne sont protégées ni par la jurisprudence ni par le Safe Harbor.

C) L'arrêt Schrems : Coup de tonnerre sous un ciel menaçant

Juste après les révélations Snowden, un étudiant autrichien déjà bien connu pour les multiples actions entreprises contre Facebook, décide de déposer à nouveau une plainte devant l'autorité irlandaise de protection des données personnelles (DPC).[35] Facebook ayant son siège européen en Irlande, c'était nécessairement par la CNIL irlandaise qu'il fallait passer pour faire interdire le transfert de ces informations aux États-Unis qui n'offraient pas selon lui, de protection contre la surveillance de masse révélée au travers du programme PRISM. Mais la DPC irlandaise considère alors qu'elle se trouve liée par la décision d'adéquation de la Commission européenne et que de ce fait elle n'a pas de compétence de contestation, le droit communautaire primant sur le droit national.[36]

S'en suit alors un recours devant la High Court of Ireland, plus haute juridiction irlandaise, qui pose une question préjudicielle aux juges européens afin de savoir si la décision d'adéquation du Safe Harbor empêchait une autorité nationale de contrôle de son pouvoir d'enquête sur des transferts relatifs à cet accord au regard des articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union.[37] Au-delà de la réponse insistant sur l'indépendance des autorités nationales dans l'examen du respect de ces transferts, les juges européens vont étudier d'office l'adéquation du niveau de protection offert par le Safe Harbor par rapport à la directive de 95, dans un contexte de surveillance de masse dévoilé par l'affaire Snowden. La réponse est nette et précise. Le Safe Harbor n'apporte pas une protection adéquate au sens de la directive.[38]

Cette solution est à rapprocher d'un arrêt de 2014 *Digital Rights Ireland* dans lequel les juges européens avaient invalidé la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la

---

[35] PIXELS, « Max Schrems, le « gardien » des données personnelles qui fait trembler les géants du Web », www.lemonde.fr, publié le 05 octobre 2015. https://www.lemonde.fr/pixels/article/2015/10/06/max-schrems-le-gardien-des-donnees-personnelles-qui-fait-trembler-les-geants-du-web_4783391_4408996.html

[36] PERRAY (R), UZAN-NAULIN (J), « Transfert de données - Arrêt Schrems : Cour(s) magistral(e) de droit à la protection des données personnelles » *Communication Commerce électronique* n° 12, Décembre 2015, étude 21, p.2.

[37] DEBET (A), « L'invalidation du Safe Harbor par la CJUE : tempête sur les transferts de données vers les États-Unis », *La Semaine Juridique Edition Générale* n° 46-47, 9 Novembre 2015, 1258, p.2109.

[38] DEBET (A), « L'invalidation du Safe Harbor, un nouveau « grand arrêt », de la CJUE dans le domaine de la protection des données », *Communication Commerce électronique* n° 11, Novembre 2015, comm. 94.

fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, au motif que la conservation de ces données et l'accès par les autorités nationales compétentes sont disproportionnés par rapport à l'objectif d'intérêt public et aux impératifs de sécurité publique du texte. En conséquence, il y avait une atteinte grave aux droits fondamentaux à la vie privée et à la protection des données à caractère personnel.[39]

Dans l'arrêt Schrems, contexte oblige, la CJUE va appliquer la même solution en démontrant que les autorités américaines ont accès très généralement aux données qui sont transférées dans le cadre de l'accord autorisé par la décision d'adéquation de l'Union européenne, que les personnes concernées n'ont pas de voie de recours et que les garde-fous sont inexistants. En effet dans le cadre du Safe Harbor, la résolution des litiges est limitée au caractère commercial de ces derniers.[40] Or, la cour rappelle que :

> « conformément à l'annexe I, quatrième alinéa, de la décision 2000/520, l'applicabilité desdits principes peut être limitée par, notamment, « les exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis », ainsi que par « les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir ».[41]

Les juges en déduisent donc que la décision de la Commission fait valoir la primauté des exigences américaines en matière de sécurité nationale sur les principes de l'accord Safe Harbor par le caractère bien trop large de l'exception. Il en résulte donc que l'ingérence est caractérisée et généralisée et que de facto, l'étude de la législation interne états-unienne aurait dû prendre une place plus importance dans l'influence de la décision de la Commission notamment sur les limitations à cette ingérence. Il s'agit dès lors de reconnaître que l'accord ne respecte pas le niveau de protection adéquate au sens de la directive, elle-même interprétée à la lumière de la Charte, et qu'il convient d'invalider la décision d'adéquation de la Commission.

---

[39] CJUE, *Affaires jointes C-293/12 et C-594/12* du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a..

[40] PERRAY (R), UZAN-NAULIN (J), « Transfert de données - Arrêt Schrems : Cour(s) magistral(e) de droit à la protection des données personnelles » *Communication Commerce électronique* n° 12, Décembre 2015, étude 21, p. 4.

[41] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.

Dans cet arrêt il n'est donc ni question de la finalité, ni de l'activité de l'opérateur comme il est retenu dans l'arrêt PNR.[42] Peut-être que la Cour aurait dans ce sens, pu placer l'accord PNR sous l'égide de la directive de 95 par un raisonnement juridique analogue ce qui aurait permis de pointer le caractère généralisé de l'ingérence américaine 10 ans auparavant.

Le résultat est l'invalidation de l'accord Safe Harbor, sans mise en place de délai de conformité. La reconstruction d'un accord est primordiale et doit être rapide.

[42] CJUE, *Affaires jointes C-317/04 et C-318/04* du 30 mai 2006, Parlement européen c/ Conseil de l'Union européenne.

II) Le besoin de reconstruction rapide d'un accord

Le besoin de reconstruction d'un accord s'est notamment caractérisé par la nécessité de continuité des flux transfrontières de données (A). Comme l'idée de refonder un accord existait déjà avant l'arrêt Schrems, mais que rien n'a été enclenché, nous sommes passés d'une révision planifiée à un accord précipité (B).

A) La nécessité de continuité des flux transfrontières

Le premier acteur européen à s'exprimer sur l'après-Schrems est le Groupe 29 (G29). Comme son nom l'indique, il fut créé sous l'égide de l'article 29 de la directive 95/46/EC. Ce dernier instaurait la mise en place d'un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, consultatif et indépendant et composé d'un représentant d'une autorité de contrôle de chacun des États membres.[43] Remplacé à l'entrée en vigueur du RGPD par le Comité européen de protection des données personnelles[44], il avait notamment pour mission d'examiner toute question concernant l'application de ladite directive afin d'aider à l'uniformisation dans son application.

Dans un communiqué du 16 octobre 2015, le G29 insiste implicitement sur la nécessité de continuité des flux transfrontières avec les États-Unis, notamment en appelant de toute urgence les États membres et les institutions européennes à ouvrir des discussions avec les Américains afin de trouver au plus vite un nouvel accord qui respecte les exigences de la Cour de justice de l'Union européenne.[45] Il rappelle également que les règles dérogatoires prévues par l'article 26 de la directive restent valables et confie la responsabilité aux autorités nationales de contrôle, le soin de veiller à leur bonne application.[46] C'est par exemple le cas de l'adoption de règles internes d'entreprise ou binding corporate rules (BCR).[47] De plus, si le responsable de traitement peut prouver que la personne a indubitablement donné son consentement, comme repris à l'article 69 de la loi Informatique et Libertés française, le transfert peut avoir lieu.[48] Le

[43] Art. 29 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[44] Art. 68 du Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[45] Communiqué du G29 du 16 octobre 2015.
[46] *Ibid.*
[47] Article 26 de la « Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995.
[48] FLIPO (O), « Après le « Safe Harbor », le « Privacy Shield » », Dossiers d'actualité *LexisNexis*, 27 mai 2016.

G29 est suivi dans la foulée de ces déclarations par une communication de la Commission expliquant concrètement comment mettre ces mesures en œuvre en novembre 2015.[49]

Les autorités nationales quant à elles prennent la mesure de l'importance d'analyser les impacts et les conséquences de la fin du Safe Harbor à l'image de la CNIL qui publie un communiqué sur son site internet au lendemain de celui du G29, afin d'expliquer en premier lieu le sens et la valeur de l'arrêt Schrems et de conclure en second lieu qu'il y faut : « déterminer précisément les conséquences juridiques et opérationnelles de cet arrêt sur l'ensemble des transferts intervenus dans le cadre du "safe harbor." »[50]

En effet bien que le Safe Harbor ait essuyé beaucoup de critiques, il avait quand même un aspect pratique indispensable : il permettait les transferts en dehors de l'Union dans un pays qui n'offre pas de niveau de protection adéquate sans pour autant devoir se plier à des mécanismes contraignants d'autorisations par les autorités nationales selon l'État membre dans lequel on se trouve.[51]

En conséquence, on comprend que la nécessité de continuité des flux relève autant d'une crainte de voir les flux stoppés pour cause de défaut de base légale les autorisant, que de la réorientation de tous ces transferts vers des bases légales relevant des exceptions prévues par la directive. L'idée est dès lors de faciliter le plus possible les flux en sensibilisant les acteurs qui transféraient des données personnelles vers les États-Unis au travers du Safe Harbor, en les orientant vers des solutions alternatives dans l'attente des négociations d'un nouvel accord.

En effet, si proche des révélations sur l'affaire Prism, l'arrêt Schrems a contribué à une certaine défiance envers les opérateurs américains traitant des données personnelles de citoyens européens. De fait ces opérateurs et notamment ceux proposant des services de cloud, se retrouvent potentiellement en difficulté économique puisque les clients souhaitent plutôt se diriger vers des prestataires suscitant la confiance, donc automatiquement dans un pays offrant un niveau de protection adéquate afin de stocker leurs données[52]. C'était là le deuxième aspect

[49] Communiqué de presse de la Commission européenne du 6 novembre 2015, - la Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire Schrems.
[50] CNIL, « Invalidation du « safe harbor » par la Cour de Justice de l'Union européenne : une décision clé pour la protection des données », www.cnil.fr, publié le 07 octobre 2015.
https://www.cnil.fr/node/15823
[51] GASTAUD (F), « Quelles conséquences pratiques pour le transfert de données aux États-Unis suite à l'invalidation du « Safe Harbor » par la CJUE ? », www.village-justice.org, publié le 7 octobre 2015.
https://www.village-justice.com/articles/Quelles-consequences-pratiques,20591.html
[52] REES (M), « La CJUE invalide le Safe Harbor américain : quelles conséquences ? », www.nextincpact.com, publié le 6 octobre 2015.

pratique du Safe Harbor : celui de regrouper la confiance accordée individuellement aux opérateurs économiques en un seul mécanisme permettant une autocertification sous la forme d'un HUB, puisque toutes les autorisations étaient regroupées sur une seule plateforme permettant leur libre consultation.[53] Ce mécanisme est d'ailleurs repris et amélioré par le Privacy Shield (voir infra. Sc. 2 § 1). Par conséquent, c'est plus généralement toutes les entreprises américaines utilisant le cadre juridique du Safe Harbor qui se retrouvent pénalisées soit environ 4000[54], que ce soit pour transférer des données personnelles de clients européens, mais également celles de salariés au sein de l'Union à des fins de traitement de ressources humaines.[55]

Dans cet entre-deux, les enjeux sont d'ailleurs de taille puisque toutes les compagnies américaines ne se battent pas à armes égales dans la réorientation vers les solutions proposées par le G29. En effet, mettre en place des clauses contractuelles comme prévu à l'article 26 nécessite de décomposer toute la cartographie des transferts selon que l'on soit en présence de données relatives à des clients ou à des salariés.[56] La procédure semble alors longue et potentiellement coûteuse pour l'entreprise. De la même façon, la mise en place de BCR est surtout réservée aux très grosses entreprises. De facto, les petites et moyennes entreprises américaines rencontrent beaucoup plus de difficultés pour légaliser les transferts effectués vers les États-Unis.

Il semblerait cependant qu'un grand nombre de groupes se soit dirigé vers des BCR. En effet, fin 2014, l'entreprise Atos déclare être la première société informatique à obtenir la certification BCR.[57] Mais dans le rapport annuel de la CNIL de 2015, ce ne sont pas moins de 78 groupes qui sont déclarés comme ayant adopté ce type de règles contraignantes.[58] Nul doute que le chiffre a explosé en à peine un an, à la suite de l'arrêt Schrems. La mesure d'orientation au moins pour ces multinationales semblait dès lors avoir porté ses fruits.

---

https://www.nextinpact.com/news/96763-la-cjue-invalide-safe-harbor-americain-quelles-consequences.htm

[53] Voir à ce titre la rubrique *Search the U.S-EU Safe Harbor* list consultable sur le site www.export.gov

[54] MCGOOGAN (C), « What does the end of Safe Harbor mean for you? », www.wired.co.uk, publié le 6 octobre 2015.
https://www.wired.co.uk/article/what-does-the-end-of-safe-harbour-mean

[55] BOWMAN M. (C), « US-EU Safe Harbor invalidated: What now? », www.privacylaw.proskauer.com, publié le octobre 2015.
https://privacylaw.proskauer.com/2015/10/articles/european-union/us-eu-safe-harbor-invalidated-what-now/

[56] *ibid.*

[57] « Atos, 1ère société informatique à obtenir la certification BCR pour sa capacité à garantir la protection des données personnelles de ses clients », www.atos.net, publié le 20 novembre 2014.
https://atos.net/fr/2014/communiques-de-presse/communiques-generaux_2014_11_20/pr-2014_11_20_01

[58] *Rapport d'activité 2015* de la CNIL, www.cnil.fr, p.5
https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf

Cependant, conscients des difficultés, l'autorité de contrôle anglaise Information Commissioner's Office (ICO) publie des conseils pendant la période d'intérim rappelant aux opérateurs de tels transferts, de ne pas paniquer. L'autorité de contrôle ne considérant pas que l'arrêt Schrems ait entrainé une hausse importante des menaces concernant les données personnelles, elle ne va pas sanctionner tous les transferts sous prétexte que l'accord a été invalidé.[59] Cela montre que les organismes européens ont conscience que la continuité des transferts est nécessaire et qu'il n'y a finalement pas de volonté de sanction des opérateurs américains dans la mesure où ils sont les premières victimes de cette invalidation.

Les négociations pour un nouvel accord reprennent très vite afin de rétablir la légalité et donc la continuité des flux de données personnelles entre les États-Unis et l'Union européenne. Le Safe Harbor ayant déjà fait l'objet de vives critiques de la part de la doctrine, les institutions européennes avaient commencé à se concerter afin de lui apporter un peu de sang neuf. Mais l'arrêt Schrems en ayant décidé autrement, la conclusion d'un accord a été finalement précipitée. Le G29 avait d'ailleurs quant à lui le 16 octobre, à la suite de la décision, appelé à la discussion sur les termes de cet accord, prévoyant des garanties plus importantes pour les personnes et avait fixé la date butoir au 31 janvier 2016.[60]

B) D'une révision planifiée à un accord précipité

Il faut remonter à 2012 pour trouver les premières volontés de réviser le Safe Harbor. En effet dans la première proposition d'une nouvelle législation européenne encadrant les données personnelles du 25 janvier 2012, la Commission au vu des résultats de l'analyse d'impact et de la consultation des parties intéressées, rapporte que ces dernières considèrent les règles applicables aux transferts internationaux comme trop complexes. Cette complexité constitue un obstacle à leur activité étant donné le nombre de traitement et de transferts nécessaires en provenance de l'Union vers le reste du monde.[61] Cela laisse présager le pire quant à l'avenir du Safe Harbor en matière de garanties pour les personnes sur les transferts de données transatlantiques. Mais, la Commission rassure quelque peu dans le considérant 78 de la même proposition qui rappelle que malgré l'augmentation du nombre de transferts du fait du

[59] ICO « Data transfers to the U.S and Safe Harbor – interim guidance », www.ico.org.uk, publié le 10 février 2016.
https://ico.org.uk/media/1560653/data-transfers-to-the-us-and-safe-harbor-interim-guidance.pdf
[60] *Rapport d'activité 2015* de la CNIL, www.cnil.fr, p.36.
https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf
[61] Proposition de règlement COM(2012) 11 du Parlement européen et du Conseil du 25 janvier 2012 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 (règlement général sur la protection des données) p.4.

développement économique mondial et de la coopération internationale, il est nécessaire que la protection des données des Européens ne faiblisse pas, et de rajouter que : « En tout état de cause, les transferts vers des pays tiers ne peuvent avoir lieu que dans le plein respect du présent règlement »[62]. Implicitement, cela signifie que le règlement prévoit *a minima* le même degré de protection que la directive en matière de transferts internationaux. Mais la compréhension de la planification de la réforme de l'accord transatlantique se fait à la lecture de l'article 41 sur les transferts assortis d'une décision d'adéquation du niveau de protection. En effet, ce dernier prévoit des dispositions qui vont bien au-delà de ce qui est prévu par le Safe Harbor telles que les recours effectifs et opposables des personnes concernées aussi bien sur les traitements de nature commerciale que sur ceux relatifs à la sécurité publique, la défense nationale ou le droit pénal plus généralement.[63] Un autre élément important évoqué est celui de la primauté du droit qui semble directement adressé aux États-Unis, collectant sous couvert de lois d'application parfois extraterritoriale comme le FISA, un nombre colossal de données personnelles de citoyens du monde entier.[64]

La planification d'un nouvel accord ou du moins d'une révision se vérifie d'ailleurs en 2013 à la suite des révélations Snowden puisque la Commission publie une communication relative au fonctionnement du Safe Harbor du point de vue des citoyens de l'Union et des entreprises établies sur son territoire. Tout commence avec un rappel du fonctionnement du Safe Harbor aussi bien sur son articulation avec la directive de 95 que sur ses principes et son mécanisme d'autocertification, en soulignant le caractère contraignant de l'accord pour ceux qui décident de s'y soumettre y compris les autorités publiques.[65] Au regard des exceptions déjà soulevées à titre de critique, c'est très discutable, d'autant plus qu'à ce moment, les révélations concernant les programmes de surveillance américains continuent de pleuvoir.

La Commission reconnaît ensuite que le contexte actuel, faisant référence en filigrane aux révélations estivales de la même année, mais également aux changements profonds qu'a connu le transfert transatlantique de données, doit obliger à réexaminer l'accord. En effet, force est de constater deux ans avant la décision couperet, que les données personnelles sont passées au premier plan dans l'économie numérique, que le nombre d'entreprises ayant adhéré au Safe

[62] *Ibid.* Considérant 78.
[63] *Ibid.* Art. 41
[64] BARRAT (O), « Informatique en nuage : mettez de côté le PATRIOT Act, penchez-vous sur le FISAA », *Sécurité et stratégie* 2013/3 (14), p.72.
[65] Communication COM(2013)847 de la Commission au Parlement européen et au Conseil du 27 novembre 2013 relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire. p.2

Harbor a été multiplié par huit et que les conséquences d'un potentiel arrêt des flux transatlantiques aurait des conséquences économiques désastreuses[66] (*voir à ce titre infra. Partie 2 ; chapitre 1 ; Section 1 I) sur les conséquences économiques dommageables en cas d'illégalité des flux*). La Commission se base par la suite sur des travaux, des études, des rapports d'analyse d'impact depuis 2002 pour constater ces évolutions et les problématiques sous-jacentes. Preuve en est qu'elle était au fait de la nécessité d'un nouvel accord et que ce dernier était déjà planifié, puisque des études avaient notamment été commandées auprès de l'université de Namur en Belgique sous la direction du Professeur Poullet.[67] Cela étaye la thèse selon laquelle la Commission a temporisé jusqu'au dernier moment en espérant que l'orage passe, puisque bien informée de la situation, elle a fait preuve d'une certaine inertie, comme en témoignent ces différents documents. Après un long raisonnement, chiffres et statistiques à l'appui, la Commission conclut avec quelques recommandations en matière de transparence, à la charge des entreprises autocertifiées, notamment sur la publication des dispositions de protection de la vie privée, de la collecte jusqu'aux opérations de sous-traitance réalisées ; en matière de recours pour les citoyens d'accéder par le biais du site du responsable de traitement, à un prestataire de règlement extrajudiciaire des litiges avec certaines conditions sous-jacentes comme le contrôle poussé de la part du ministère du Commerce américain ; en matière de mise en œuvre de la certification afin d'éviter les problèmes de mauvaise conformité, de non-renouvellement ou de fraudes, par le biais de fausses déclarations ; en matière d'accès aux données par les autorités des États-Unis, par le biais d'un devoir d'information aux personnes concernées par les entreprises américaines sur la législation permettant aux autorités américaines d'accéder à leurs données et d'un rappel à ces mêmes autorités de ne pas abuser de la dérogation prévue par l'accord.[68]

Il y a de quoi rester perplexe à la lecture de cette communication puisqu'on comprend qu'une révision devait avoir lieu puisque nécessaire, mais le 8^{e} point concernant les recommandations fait plutôt état de rustines à coller sur le Safe Harbor afin qu'il soit plus adéquat. De plus, au moment où la communication est publiée, la procédure judiciaire menant à l'arrêt de 2015 est bien avancée puisque déjà examinée par la High Court of Ireland.[69] On peut dès lors se demander si la Commission n'essayait pas simplement de sauver les apparences

[66] *Ibid.* p.3
[67] *Ibid.* Voir note de bas de page n°7 en p. 3 du document
[68] *Ibid.* pp. 21 à 23
[69] Voir à ce titre l'annexe 1 du détail de la procédure de *l'affaire Schrems* devant la High Court of Ireland

à la suite de l'affaire Snowden, même si beaucoup d'éléments lui laissent tout de même le bénéfice du doute.

Quoi qu'il en soit, la communication de la Commission sur la nécessité de réformer l'accord Safe Harbor reste sans conséquence juridique jusqu'à l'invalidation de ce dernier. Il faut entendre par là que de simples discussions de façade ont été engagées avec les Américains. Il faudra attendre au plus tôt une déclaration post-Schrems du Commissaire de la justice Věra Jourová devant la Commission civile des libertés le 26 octobre 2015**,** qui annonce des négociations avec les États-Unis en vue d'un nouveau cadre juridique pour les flux de données transatlantiques, visant un plus haut niveau de protection. Faisant référence à la communication de 2013 combinée à la décision de la Cour de justice et à la venue prochaine du RGPD, la Commissaire annonce que le système d'autocertification sera conservé tout en garantissant un renforcement du contrôle de la part des autorités compétentes de part et d'autre de l'Atlantique, notamment par une meilleure communication avec la mise en place de rapports annuels conjoints. Plus importante, sur la raison principale de l'invalidation, à savoir l'accès systématique par les autorités publiques aux données des citoyens européens, elle incite à la mise en place de garde-fous, de recours pour l'empêcher, dans la droite ligne des recommandations de 2013, déjà sujettes à controverse, et également à la définition de conditions strictes et de limitations à cet accès.[70] Cette déclaration est d'ailleurs confirmée dans la communication de la Commission du 6 novembre 2015.[71]

Ces négociations aboutissent en effet à un nouveau cadre annoncé le 2 février 2016. Si l'on peut applaudir la rapidité des négociations, presque dans les temps arrêtés par le G29, on peut tout de même se poser des questions sur la teneur de ces dernières. En effet, elles ont probablement été faites dans un climat de tension politique avec un souci de remettre un accord sur pied au plus vite. Quand bien même la révision était planifiée et que des discussions étaient en cours, le résultat paraît bien précipité, d'autant plus que la communication est lacunaire, se bornant simplement à énumérer trois éléments peu détaillés répondant simplement aux exigences de la Cour à savoir : « Des obligations strictes pour les entreprises qui traitent des données à caractère personnel européennes, et un contrôle rigoureux ; un accès par les autorités

[70] Discours de la Commissaire V. Jourová du 26 octobre 2015 sur la décision de la CJUE sur le Safe Harbor devant la Commission des libertés civiles, de la justice et des affaires intérieures (Libe).

[71] Communiqué de presse de la Commission européenne du 6 novembre 2015, - la Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire Schrems.

américaines étroitement encadré et transparent ; une protection effective des droits des citoyens de l'Union et plusieurs voies de recours. »[72]

Beaucoup d'éléments sont ainsi oubliés ou peu détaillés notamment en matière de contrôle de l'engagement d'arrêt de la surveillance massive par les États-Unis ou encore le droit à un recours juridictionnel comme exigé par la Cour de justice de l'Union.[73] Cependant, un premier paquet de documents constituant le Privacy Shield est publié le 29 février 2016 par la Commission.

N. B. À toutes fins utiles, le paquet « Privacy shield » originellement publié sur le site de la Commission le 29 février 2016 n'est plus disponible. Veuillez donc vous référer au lien suivant sur le site dédié du Privacy Shield : https://www.privacyshield.gov/EU-US-Framework ou sur le site de l'« International Association of Privacy Professionals », https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/

NB 2 : Les textes sont en anglais uniquement.

[72] Communiqué de presse de la Commission européenne du 2 février 2016, – La Commission européenne et les États-Unis s'accordent sur un nouveau cadre pour les transferts transatlantiques de données, le « bouclier vie privée UE-États-Unis ».
[73] CASTETS-RENARD (C), « Données personnelles : accord entre la Commission et les États-Unis », *Recueil Dalloz* n°6/7675e, 11 février 2016 p.315.

Section 2 : Un pansement juridique visant une meilleure conformité

Il est certain que les acteurs en présence ont voulu pallier les reproches qui ont été adressés au Safe Harbor en visant une meilleure conformité à la législation européenne. On ne peut pas non plus nier que l'accord offre un plus haut niveau de protection général (I). Mais il s'agit surtout de trouver un équilibre acceptable (II) entre deux modèles de protection des données qui ne sont pas compatibles aux premiers abords.

I) Un accord offrant un plus haut niveau de protection général

L'accord offre un niveau de protection plus élevé notamment en ce qu'il apporte des avancées structurelles qui renforcent l'application des principes énoncés (A). De plus, ces principes renforcent les obligations des organisations certifiées (B).

A) Des avancées structurelles renforçant l'application des principes

À titre liminaire, il convient de noter que l'UE n'est plus seule à fonder l'accord sur une base légale. Si évidemment la différence de philosophie en matière de protection des données amène le département du commerce américain à reconnaître la seule existence de règles sectorielles à défaut d'une législation globale, ce dernier tient tout de même à préciser que le présent accord entre dans le champ de ses prérogatives conformément à la section 1512 du titre 15 de l'U.S Code qui dispose que :

« Cela doit être du champ de compétence et du devoir dudit département d'encourager, de promouvoir et de développer le commerce extérieur et intérieur […], et à ce titre, il (le Département du commerce) doit être investi de la compétence et du pouvoir des départements, agences, bureaux, et subdivisions des services publics ci-après désignés, et d'autres pouvoirs et responsabilités qui peuvent être prévus par la loi »[74].

Cela peut paraître anodin, mais l'article[75] vers lequel il renvoie fournit une liste conséquente de services gouvernementaux sous la tutelle du département du commerce si l'on rentre dans les champs prévus par la section 1512. Cela signifie que l'on assiste aux États-Unis à une ébauche d'administration fédérale en matière de protection des données personnelles, puisque par extension, l'organisation des flux transfrontières de nature commerciale avec l'Europe dans le cadre de l'accord, est confiée au département du commerce (DoC) qui devient,

[74] Art. 1512 U.S Code, Titre 15.
[75] Art. 1513 U.S Code, Titre 15.

au titre du développement du commerce international, l'autorité chargée de l'administration. Cela n'était pas le cas dans le Safe Harbor, où le Département se bornait simplement à rappeler son pouvoir légal de promotion du commerce international, dans le cadre duquel il avait établi le document contenant les QSP (*voir supra*)[76]. Cependant, sur le terrain, les pouvoirs d'investigations et de sanctions sont exercés par la FTC et le département des transports conformément à leurs champs de compétence.[77] Cela conditionne par ailleurs le champ d'application matériel du Privacy Shield.[78]

Le contrôle et les sanctions portent d'ailleurs sur de nouvelles obligations mises à la charge de l'entreprise. En effet, cette dernière ne doit maintenant plus se contenter de seulement déclarer publiquement sa conformité aux principes du Privacy Shield, mais elle doit également publier sa politique de confidentialité dans le respect des principes et les exécuter de manière efficace,[79] sous peine de sanction par la FTC.[80] Pour rappel, le DoC avait, vingt ans auparavant, émis des appréhensions quant au fait que les entreprises américaines n'informaient pas de la collecte de données ou n'avaient pas de politiques de confidentialité. Si on pouvait donc douter de la mise en œuvre de telles politiques dans le cadre du Safe Harbor, l'obligation de publication de ces dernières pour les entreprises adhérentes du Privacy Shield semble au moins partiellement régler le problème, à savoir celui de voir les entreprises s'en doter. L'histoire nous dira si la seconde partie du problème, à savoir celle de leur application par les entreprises reste d'actualité. Tout de même, on ne peut qu'ironiquement féliciter une solution à ces inquiétudes trouvée aussi rapidement.

Il est à noter que comme préconisé par la Commission dans la communication de 2013[81], la liste des entreprises certifiées fait l'objet d'un suivi plus attentif par les autorités américaines. Ce suivi se fait notamment en contrôlant davantage les fausses certifications ou les certifications périmées en exigeant un engagement annuel auprès du DoC de conformité au Privacy Shield. Par la suite, la liste est mise à jour avec, d'un côté les entreprises dont la certification est en vigueur et de l'autre, celles dont elle est expirée, ce qui permet plus de visibilité pour la personne

[76] Principes de *Privacy* du Safe Harbor publié par le Département du Commerce américain le 21 juillet 2000, disponible sur www.build.export.gov.
[77] Art. 2 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Overview.*
[78] Voir infra. Partie 1, Chapitre 2 section 1 I).
[79] Art. 2 des Principes de l'accord *EU-U.S Privacy Shield,* section *Overview.*
[80] GRIGUER (M), « Le Safe Harbor est mort, vive l'UE-US Privacy Shield Arrangement », *Cahiers de droit de l'entreprise* n° 2, Mars 2016, prat. 10, p.3.
[81] Communication COM(2013)847 de la Commission au Parlement européen et au Conseil du 27 novembre 2013 relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire. pp.22 et 23.

concernée. En cas d'expiration, les entreprises doivent retourner les données à la personne concernée.[82] Si le principe semble louable, sa mise en place est compliquée au regard de la difficulté à contrôler toutes les entreprises certifiées ou ayant été certifiées.

Une autre avancée de taille, d'ailleurs saluée comme telle par le G29 dans le communiqué du 13 avril 2016 se prononçant sur l'adéquation du Privacy Shield aux règles européennes,[83] est celle de la prise en compte de trois définitions-clés dans l'application du Privacy Shield et respectant la directive de 95. Ainsi, les données personnelles sont bien les données d'une personne identifiée ou identifiable. En effet, la conception américaine de PII (personal identifiable information) ne renvoie pas à la même définition.[84] De fait, cela permet de clarifier d'entrée ce qu'on entend par « donnée personnelle » d'autant plus que la directive européenne est directement citée. De même, les définitions de traitement de données et de responsable de traitement permettent d'encadrer plus précisément les acteurs qui adhéreraient au Privacy Shield, et leurs responsabilités.

Toutes ces avancées structurelles ont pour but le renforcement de l'application des principes ; principes eux-mêmes revus et détaillés afin d'apporter une protection plus complète dans le cadre des flux transatlantiques de données personnelles avec les Américains.

B) Des principes renforçant les obligations des organisations certifiées

Concernant les principes du Privacy Shield, à quelques différences sémantiques près, on retrouve les mêmes idées que celles présentes dans le Safe harbor. La différence est que le plus souvent, les principes généraux négociés entre la Commission et le DoC imposent aux organisations américaines un certain nombre d'obligations supplémentaires[85] ce qui ne réjouit d'ailleurs pas les petites et moyennes entreprises.[86]

[82] Art. 3 des Principes de l'accord *EU-U.S Privacy Shield*, section *Overview*.
[83] Communiqué du G29 sur l'opinion sur le *EU-U.S Privacy Shield* du 13 Avril 2016.
[84] METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85, p.2.
[85] GRIGUER (M), « Le Safe Harbor est mort, vive l'UE-US Privacy Shield Arrangement », *Cahiers de droit de l'entreprise* n° 2, Mars 2016, prat. 10, p.3.
[86] GRANT (G), « Tech companies like Privacy Shield but worry about legal challenges », www.cio.com, publié le 21 décembre 2016
https://www.cio.com/article/3152556/tech-companies-like-privacy-shield-but-worry-about-legal-challenges.html

1) Le principe de notification

Le principe de notification qui rappelons-le est à rapprocher du devoir d'information incombant au responsable de traitement, impose à l'organisation une rigueur bien plus importante dans la communication de l'utilisation des données et des droits qui y sont attachés. Il ne s'agit donc plus seulement d'informer la personne du type de donnée collectée, des finalités du traitement, de l'identité des tiers à qui elles sont transférées et les raisons ou encore des moyens mis à la disposition de la personne afin de limiter leur utilisation ou leur diffusion. Dorénavant, le responsable doit en premier lieu informer la personne concernée de sa participation au Privacy Shield et de sa volonté de soumettre toutes les données collectées aux principes encadrant l'accord.[87] En matière de transferts de données à un tiers, il doit également clarifier sa responsabilité lorsque de tels échanges ont lieu. À cela s'ajoute un devoir d'information quant au droit d'accès à ces données de la personne, et tout un volet sur les plaintes et les recours possibles. En plus de la manière de le contacter en cas de demandes ou de plaintes, il doit aussi indiquer l'instance de résolution des conflits à qui les adresser ainsi que les organes de supervision[88] et spécifier que ce recours est gratuit. Enfin, il faut donner les conditions selon lesquelles l'individu peut demander un arbitrage obligatoire. Plus intéressant, l'organisation doit également signaler qu'elle peut faire l'objet d'investigations de la part de la FTC ou tout autre organe autorisé, et que dans le cadre d'une requête légale (en matière de sécurité nationale par exemple) par une autorité publique, elle doit fournir les données personnelles de l'individu,[89] ce qui découle directement du Freedom Act venu assouplir les règles d'ingérence du Patriot Act en la matière puisque les entreprises n'étaient pas tenues d'informer les individus sur ces enquêtes.[90] Évidemment, cette information doit se faire en termes clairs et précis lors de la première collecte ou bien dès que possible suivant la collecte. Dans tous les cas, cela doit être réalisé avant une utilisation pour d'autres finalités que celles pour lesquelles elles ont été collectées. L'objectif de ce principe revisité est de donner plus de

[87] FISCHER (P), « From the safe harbour to the privacy shield: selected aspects of the EU-US privacy shield », *Revue de droit des affaires internationales* n°2, 2018, pp. 143 à 153.
[88] METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85, p.3
[89] Art. 1 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Principles*.
[90] Conférence organisée par le Centre de recherche en droit public de l'Université de Montréal, V*ie privée : Europe vs. Amérique*, intervenants, CASTETS-RENARD (C.), REIDENBERG (J.), le 25 mai 2016, à Montréal.

visibilité à la personne concernant l'utilisation faite de ces données, mais c'est surtout d'inciter les organisations participantes à une plus grande transparence au regard des principes prévus.[91]

2) Le principe de choix

Si comme son prédécesseur, l'organisation adhérente au Privacy Shield doit se contenter de permettre de choisir si les informations personnelles sont transférées à un tiers ou utilisées pour une autre finalité, le texte prévoit maintenant que la finalité doit seulement être substantiellement différente et pas seulement incompatible.[92] Cela a pour conséquence d'élargir le champ du choix laissé à la personne concernée puisque la différence de finalité peut s'apprécier de manière plus vague que l'incompatibilité et se rapprocher d'un droit d'opposition par extension[93]. Concernant le mécanisme de choix que la personne peut effectuer, c'est toujours une procédure d'opt-out qui est privilégiée, précisant tout de même qu'il doit être clair, précis et facile d'accès. Cependant sur ce point général, le Privacy Shield apporte une dérogation : ainsi, il n'est pas nécessaire de permettre un choix quand la transmission des données est faite à un tiers agissant pour le compte de l'organisation et sous ses instructions comme sous-traitant effectuant des tâches pour elle. Cependant, il faut nécessairement qu'il y ait un contrat entre le responsable de traitement et le sous-traitant.

L'exception à la règle en matière de choix laissé à la personne concerne les données sensibles. En effet, l'organisation doit obtenir un consentement exprès par une procédure d'opt-in de la part des individus, dans le cas où les données sont destinées à être transmises à un tiers ou utilisées pour une finalité autre que celles pour lesquelles elles ont été collectées ou ultérieurement autorisée par l'individu.[94] De plus, une organisation doit traiter comme une donnée sensible, toute donnée reçue par un tiers l'ayant identifié comme donnée sensible.[95]

Donc en termes de choix, on retiendra surtout l'élargissement du champ de celui-ci et la présence d'une dérogation, tant le fonctionnement juridique des mécanismes se rapproche de ceux du Safe Harbor. Cependant, il est à noter que concernant les données sensibles, le choix a

[91] Communication COM(2016)117 de la Commission européenne au Parlement européen et au conseil du 29 février 2016 relative aux flux de données transatlantiques : rétablir la confiance grâce à des garanties solides, p.8.
[92] Art. 2 des Principes de l'accord *EU-U.S Privacy Shield*, section *Principles* 2.
[93] METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85, p.3.
[94] CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p.444.
[95] Art. 2 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Principles*.

été fait de consacrer le terme de « consentement exprès », preuve que la clarification était de mise.

3) Le principe de responsabilisation sur les transferts ultérieurs

Concernant les transferts de données personnelles ultérieurs, l'ajout du terme d'« accountability » n'est pas anodin. Il montre à lui seul la volonté de responsabiliser les organisations et fait d'ailleurs figure de proue de la corégulation entre les responsables de traitements et les autorités publiques.[96] Il s'agit en l'espèce de faire du contrat la règle, ce qui induit nécessairement plus de formalités pour les organisations, mais cela s'inscrit dans la droite ligne d'une conception américaine juridique libérale. Donc dans le cadre d'un transfert de données personnelles d'un responsable à un autre responsable, les organisations doivent respecter les principes de notification et de choix. Mais désormais, elles doivent également former un contrat avec ce tiers responsable qui stipule que ces données ne peuvent être traitées que pour des finalités limitées et spécifiées en conformité avec le consentement donné par l'individu, et seulement si ce tiers fournit le même niveau de protection que celui des principes de l'accord. De plus, il doit être prévu qu'en cas de défaillance dans l'exécution des principes, le tiers doit informer l'organisation et doit stopper le traitement ou bien prendre des mesures raisonnables et appropriées, pour y remédier. Cependant, concernant les transferts vers un sous-traitant, la solution est un peu différente sans doute parce qu'un contrat est supposé déjà exister. Le responsable de traitement doit transférer les données pour des finalités limitées et déterminées, vérifier que ce sous-traitant fournit au moins le même niveau de protection que ce que les principes prévoient et prendre des mesures raisonnables et appropriées pour s'assurer que le sous-traitant traite réellement les données personnelles transférées conformément aux obligations de respect des principes par le responsable. Même si la liberté contractuelle est plus grande, il n'en reste pas moins que les transferts ultérieurs sont plus encadrés,[97] d'une part puisqu'en fonction de la qualité du tiers à qui les données sont transférées, il existe deux procédures bien distinctes et d'autre part puisque les contrats peuvent déboucher sur des contrôles de conformité drastiques. Enfin, en combinaison avec le septième principe, une organisation adhérant au Privacy shield a la responsabilité sur le traitement de la donnée qu'elle a reçu et par conséquent, sur les transferts à un tiers agissant à son nom et pour son compte.

[96] MAXWELL (W), TAIEB (S), « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* n°3, Mars 2016, p.123.
[97] CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p. 444.

Elle reste responsable si son agent traite des données contrairement aux principes, sauf si l'organisation prouve qu'elle n'est pas à l'origine du dommage.

4) Le principe de sécurité

Le principe de sécurité impose aux organisations traitant des données personnelles de prendre des mesures raisonnables et appropriées pour les protéger de la perte, du détournement et de l'accès non autorisé, de la divulgation, de la modification et de la destruction. Mais désormais, elles doivent également prendre en compte les risques du traitement et la nature des données complétant ce faisant, les exigences posées à l'article 17 de la directive de 95.[98]

5) Le principe d'intégrité des données et de limitation par rapport aux finalités

Là encore, des progrès ont été faits en faveur d'une plus grande protection, en matière d'intégrité des données dont le principe a été étendu à la limitation de la collecte. Les données personnelles collectées par l'organisation sont limitées aux informations en rapport avec les finalités de traitement. Une organisation ne peut pas traiter de données personnelles d'une façon incompatible avec les finalités pour lesquelles elles ont été collectées ou autorisées après coup par l'individu. L'organisation doit prendre des mesures raisonnables pour assurer que les données sont fiables quant à l'utilisation prévue, précises, actuelles et complètes. De plus, l'organisation doit adhérer aux principes aussi longtemps qu'elle détient de telles informations, ce qui de facto induit un droit de portabilité, voire même d'effacement dans les cas où l'organisation ne peut plus se prévaloir du Privacy Shield. Mais la vraie nouveauté est l'ajout d'un paragraphe sur la durée de conservation et les exceptions. Ainsi, la donnée peut être conservée sous une forme identifiée ou identifiable seulement pour la durée pour laquelle elle est utile par rapport à la finalité de traitement comme défini plus haut. Cela n'empêche pas les organisations de traiter des données pour une période plus longue dans la mesure où ce traitement sert raisonnablement des finalités archivistiques dans l'intérêt public, journalistique, littéraire et artistique, scientifique, de recherche historique ou d'analyses statistiques. Dans tous ces cas, le traitement doit respecter les autres principes et règles énoncés par l'accord. Les organisations doivent prendre les mesures raisonnables et appropriées pour respecter cette règle.

[98] Article 17 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Là encore, on se rapproche notamment des règles européennes, ce qui a pour but d'assurer une protection plus forte par la mise en place d'un terme entrainant l'effacement des données.

6) Le principe de l'accès

Sur le droit d'accès, les règles sont les mêmes, à savoir que les personnes doivent avoir un accès aux données personnelles les concernant, qu'une organisation détient et doivent pouvoir les corriger ou les supprimer quand elles sont inexactes ou si les droits de personnes autres que la personne concernée, pourraient être violés, sauf si les moyens ou les dépenses pour fournir un tel accès seraient disproportionnés au risque encouru selon le cas d'espèce. Cependant, en plus du critère d'inexactitude, le droit à la curiosité entraine l'exercice des autres droits mentionnés si les données ont été traitées, contrairement aux principes de l'accord.

7) Le principe de recours, d'exécution et de responsabilité

C'est sans surprise le principe comportant le plus de changements puisque c'est celui qui apporte les garde-fous dont les juges européens avaient estimé qu'ils n'étaient pas suffisants dans l'arrêt Schrems.[99] Pour résumer donc, on a ici un changement de paradigme en ce qui concerne la protection, puisque les recours sont apportés aux individus qui sont affectés par la non-conformité aux principes et non plus, dont les données personnelles sont affectées par la non-conformité. Dans le cadre de ces recours, les plaintes doivent être examinées et solutionnées rapidement, et ce de manière gratuite pour l'individu, ce qui tranche avec le caractère abordable du recours prévu par le Safe Harbor. De plus pour satisfaire aux exigences de suivi par les autorités américaines, des procédures afin de vérifier que les attestations et les déclarations des organisations à propos de leurs politiques de confidentialité sont exactes et qu'elles sont exécutées de la même manière qu'elles sont présentées à la personne, en particulier en cas de non-conformité, sont mises en place. Ces vérifications concernent également les obligations de corriger les problèmes provenant de l'échec de respecter les principes par les organisations annonçant leur adhérence et potentiellement les conséquences pour ces organisations ; obligations mettant à la charge des organisations des audits de conformité internes et externes ce qu'a également félicité le G29.[100] Les sanctions doivent être suffisamment dissuasives pour assurer la conformité aux principes par les organisations. Il y a donc la mise en place d'un dialogue plus important entre les organisations certifiées et les

[99] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.
[100] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.

autorités américaines, mais également avec les autorités de contrôle européennes. En effet, les organisations et les opérateurs de recours indépendants sélectionnés devront répondre rapidement aux renseignements et requêtes d'information demandées par le DoC concernant le Privacy shield. Toutes les organisations doivent également répondre rapidement aux plaintes sur leur conformité aux principes, présentée par une autorité de contrôle d'un État membre par le biais du DoC. De plus, les organisations ayant choisi de coopérer avec des autorités de contrôle européennes[101], incluant les organisations qui traitent des données de ressources humaines, doivent s'adresser directement à ces autorités dans le cadre d'investigation et de résolution des plaintes. On devine donc que si on a choisi de traiter avec une autorité européenne, c'est donc elle qui servira de pivot entre l'organisation et les autorités américaines si besoin est, notamment parce que le DoC établit un point de contact pour les DPA, pour tout problème de non-conformité par les organisations. La FTC traite prioritairement les demandes provenant du DoC et des DPA et échangera les informations au regard de ces demandes avec l'autorité référente en respectant les obligations de confidentialité.

De plus, si une organisation fait l'objet d'une ordonnance de la FTC ou d'une cour concernant une non-conformité aux principes, les organisations seront tenues de publier toute section du bouclier de protection des données se rapportant à un rapport de conformité ou d'évaluation soumis à la FTC. Cela rappelle un peu la méthode américaine d'affichage de criminel après une condamnation. On peut légitimement douter de l'opportunité d'une telle mesure.

II) La recherche d'un équilibre acceptable

La recherche d'un équilibre acceptable, c'est à dire un compromis entre la liberté de circulation des données personnelles régie de manière libérale aux États-Unis et la nécessité d'une protection globale de ces données par le droit propre à l'Europe, débouche sur un rapport de force sur le choix des mécanismes de garanties de l'accord (A) ainsi que sur la prise en compte de l'arrivée proche du Règlement général sur la protection des données imposant des règles plus protectrices (B).

[101] Voir à ce titre les conditions supplémentaires de l'auto-certification et les règles de coopération avec une DPA, Art. 5 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Supplemental Principles*.

A) Un rapport de force US/UE sur les mécanismes de garanties de l'accord

Le Privacy Shield est empreint d'une dualité conciliant deux modèles légaux de protection des données personnelles[102], qui réside dans le choix de responsabiliser davantage les organisations, mais également de prévoir des mécanismes de garanties impliquant uniquement les autorités publiques de part et d'autre de l'Atlantique découlant directement des révélations Snowden. L'ensemble de ces mécanismes a été considéré malgré tout, comme une avancée importante par le G29.[103]

1) La responsabilisation des entreprises participantes

Comme établi précédemment, l'optique de responsabilisation des organisations américaines est accrue. C'est notamment le cas à travers le mécanisme sous-jacent d'autocertification et de vérification ainsi qu'à travers des mécanismes de recours et de la procédure d'arbitrage de l'annexe 1, sous peine de s'exposer à des sanctions.

a) Le mécanisme d'autocertification et l'autovérification

C'est le mécanisme central du Privacy Shield. Jugé conforme par les juges européens[104], il a été repris dans le Privacy Shield, mais avec quelques points supplémentaires. Il est toujours accompagné d'un mécanisme de vérification.

A) L'autocertification

L'autocertification est le mécanisme par lequel une entreprise américaine va soumettre au DoC un document signé par un mandataire social dans lequel elle s'engage à respecter le Privacy Shield dans son ensemble. Ce document doit contenir une liste d'informations indispensables telles que le nom de l'organisation, ses activités, sa politique de confidentialité, la publication de cette politique sur un site internet ou encore la méthode de vérification mise en place pour s'assurer de l'accord.[105] Ce document doit être renouvelé tous les ans afin de s'assurer de la validité de l'autocertification et la liste est mise à jour par le ministère auquel sont rattachées toutes les entreprises autocertifiées. Il est à noter qu'il n'y a pas de vérification

[102] SCHWARTZ M. (P), PEIFER (K.N), « Transatlantic Data Privacy Law », *The George Town Law Journal*, volume 106, 2017, pp. 115 à 179, p.164.
[103] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.
[104] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.
[105] Art. 6 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Supplemental Principles*.

systématique de la part du DoC. Cependant, cette certification tombe sous le coup de la loi américaine relative aux fausses déclarations,[106] ce qui signifie donc qu'elle est légalement encadrée, ce qui va avoir une importance particulière en matière de recours par la personne concernée (voir infra).

B) L'autovérification

Il convient de placer le préfixe « auto » avant le mot vérification puisqu'en réalité, c'est l'organisation qui décide des procédures qui vont être mises en place afin de respecter le document d'autocertification, respectant lui-même les principes du Privacy Shield. En effet, les organisations doivent effectuer des évaluations internes globales, précises et accessibles, indiquant que la politique de confidentialité respecte les principes de l'accord. Elle peut également choisir une vérification de conformité externe dont les missions seront similaires. Il est à noter que tous les documents concernant ces vérifications doivent être conservés, en vue de potentielles investigations.[107] D'ailleurs, les bilans de ces vérifications pointant également l'effectivité des recours mis en place pour l'individu sont à joindre chaque année, dans le cadre du renouvellement de la certification.

Ces mécanismes ensemble sont le fer de lance de la responsabilisation des entreprises participantes. En effet, ils permettent de mettre à la disposition des autorités compétentes notamment la FTC ou une autorité de contrôle européenne, si telle est l'option prise par l'organisation au moment de son autocertification,[108] des documents nécessaires pour effectuer des investigations à des fins de contrôle.[109]

b) Recours et procédure d'arbitrage de l'annexe 1

Dans le cadre des recours prévus par le Privacy Shield, la personne concernée a plusieurs solutions en fonction de la situation dans laquelle elle, et l'organisation se trouvent et cela constitue sans aucun doute un apport à la meilleure conformité de l'accord à la législation européenne.[110] La personne concernée peut déposer une plainte à l'entreprise directement si des mécanismes de recours ont été mis en place par elle.[111] L'organisation a alors 45 jours pour

[106] Art. 1001, U.S.C, Titre 18.
[107] Art. 7 des Principes de l'accord *EU-U.S Privacy Shield*, section *Supplemental Principles*.
[108] Art. 5 des Principes de l'accord *EU-U.S Privacy Shield*, section *Supplemental Principles*.
[109] GRIGUER (M), « Le Safe Harbor est mort, vive l'UE-US Privacy Shield Arrangement », *Cahiers de droit de l'entreprise* n° 2, Mars 2016, prat. 10, p. 3.
[110] Voir à ce titre les publications de la Professeure Céline CASTETS-RENARD sur le sujet.
[111] Art. 11 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Supplemental Principles*.

étudier la plainte.[112] Il s'agit ici de responsabiliser l'entreprise en lui laissant le choix de jouer le jeu de l'autorégulation ou de s'exposer à des sanctions au titre du droit américain et du non-respect aux principes du Privacy Shield (voir infra sur les effets juridiques). Mais le recours à la corégulation est aussi une option puisque la personne peut également introduire un recours auprès d'un organisme indépendant de règlement des litiges qui se voit confier des prérogatives en matière de sanctions, et qui est désigné par l'organisation[113] quand cette dernière n'a pas de procédure interne de traitement des plaintes et que par conséquent la personne concernée ne peut pas se prévaloir d'un tel recours. La Commission relève tout de même que l'ensemble des actions correctrices et coercitives envers l'organisation dans le traitement de ces plaintes s'il y a lieu, doivent être suffisamment fortes afin de garantir la conformité aux principes.[114] Comme prévu par les principes généraux et repris dans la décision d'adéquation., le recours proposé auprès d'un organisme tiers doit être gratuit pour la personne introduisant une réclamation.[115] L'organisme indépendant de règlement des litiges doit alors rendre une décision. Si cette dernière n'est pas appliquée par l'organisation, l'organisme doit notifier cette non-conformité aux autorités américaines ou à un tribunal compétent. Le DoC devra le cas échéant retirer l'organisation de la liste du Privacy Shield au titre de pratiques déloyales et frauduleuses.

De plus, les citoyens européens peuvent également déposer leurs plaintes auprès d'une autorité de contrôle nationale.[116] Cependant, ce mécanisme est actionnable à la condition de remplir deux critères au choix. Il faut soit qu'il s'agisse de traitement relatif à des ressources humaines collectées dans le cadre d'une relation de travail, soit par une soumission volontaire de l'organisation à la surveillance d'une autorité de contrôle. Dans ce cas, l'organisation doit se conformer à l'avis rendu par un panel d'autorités de contrôle au niveau de l'Union dans un délai de 60 jours. Dans ce cas, l'organisation doit se conformer à la position retenue dans l'avis dans un délai de 25 jours. À défaut, le panel soumet l'affaire à une autorité ou un tribunal américain compétent qui prendra les mesures nécessaires.[117] Cependant, dans un souci de conformité avec

[112] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p.9.
[113] *Ibid.* p. 9.
[114] *Ibid.* p. 9.
[115] Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *General Principles*.
[116] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p. 10.
[117] MONELEONE (S), PUCCIO (L) (Service de recherche du Parlement européen, EPRS), « Du Safe Harbour au Privacy Shield : Avancées et insuffisances des nouvelles règles de transfert des données UE-États-Unis », PE 595.892, Janvier 2017, p. 29.

les exigences posées par l'arrêt Schrems concernant le contrôle des transferts de données par les autorités de contrôle[118], ces dernières peuvent également recevoir les plaintes des personnes concernées sans pour autant que le panel ne soit compétent pour émettre des avis sur les réclamations. Dans ce cas, il convient donc que ces autorités transmettent ces réclamations au DoC ou à la FTC. Le DoC s'est par ailleurs engagé à recevoir et examiner les plaintes sur la non-conformité et le non-respect aux principes. Cela passe par la mise en place d'une interface permettant de centraliser les plaintes qui seront étudiées par les autorités américaines.[119] Ce point de contact devra informer l'autorité de contrôle du suivi du traitement de la plainte dans un délai de 90 jours à compter de la saisine.

En plus de cette volonté de responsabilisation, il faut noter que le rôle de la FTC dans l'exécution de ces recours semble tout de même primordial. En effet, investie des principaux pouvoirs d'enquête et de coercition, elle peut exiger la mise en conformité par le biais d'ordonnance ou par l'intermédiaire d'un juge fédéral. Pour rappel, la non-conformité aux principes tombe sous le coup de la section 5 du FTC Act réprimant les actes de concurrence déloyale et les pratiques trompeuses et frauduleuses[120] les entreprises ayant adhéré au Privacy Shield et ne respectant pas leurs engagements et les politiques choisies, tombent donc logiquement sous le coup de cette loi.[121] Par conséquent, les personnes concernées ont également la possibilité de formuler une réclamation directement devant la FTC même si priorité est donnée aux plaintes provenant des organismes indépendants, du DoC ou des autorités de contrôles. Il y a là en revanche une verticalité entre la FTC et les entreprises américaines. Il est d'ailleurs légitime de se demander si ces possibilités ne créent pas une distorsion importante entre la protection des citoyens européens et américains. En l'espèce, seul l'accord justifie l'extension du droit américain applicable. Dans le même ordre d'idée, les mécanismes de recours semblent compliqués dans les potentiels effets juridiques qu'ils produisent. En effet que l'on soit dans un cas de figure ou un autre, et selon que la FTC ou le DoC se prononcent, les sanctions ne sont pas les mêmes. Le DoC va se contenter de radier de la liste quand une autorité de contrôle conclut en un manquement grave de l'organisation, mais si l'autorité de contrôle décide de soumettre l'affaire à la FTC, les sanctions peuvent être

[118] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.
[119] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p. 11.
[120] Art. 45 U.S.C, Titre 15.
[121] CASTETS-RENARD (C), « L'adoption du Privacy Shield sur le transfert de données personnelles », Recueil Dalloz n°28, Août 2016, p. 1696.

beaucoup plus lourdes puisque ce sont les pouvoirs de contrôle et de coercition de droit américain qui s'appliquent. De la même manière dans le cadre de la non-conformité à une décision provenant d'un organisme indépendant de règlement des litiges, la sanction peut être double.[122] Dans tous les cas, ce sont aux différentes autorités états-uniennes qu'il appartient de contrôler l'effectivité des sanctions et leur bonne application.[123]

En dernier ressort, si tous ces mécanismes n'ont pas apporté de solutions, la personne concernée bénéficie d'un recours auprès du Panel d'arbitrage du bouclier de protection des données (Privacy Shield arbitration Panel) institué à l'annexe 1 de l'accord. Seules les personnes concernées peuvent déposer des plaintes devant ce panel[124] ; cela exclut de facto le recours aux intermédiaires mentionnés plus haut. Ce panel est composé d'un à trois arbitres sur vingt arbitres. Ils sont choisis par la FTC et le DoC. Il est à noter que ce panel n'est pas un tribunal. Il ne peut donc qu'ordonner une réparation non monétaire du préjudice. Par la suite, la personne concernée peut demander l'exécution de la sentence arbitrale devant un tribunal américain[125].

Ce que l'on peut retenir, c'est donc que dans les procédures de recours prévues par le Privacy Shield et détaillées par la Commission, il y a une volonté de placer l'organisation au centre et de la responsabiliser. En effet, le principe est, et doit rester la liberté de circulation. On comprend donc pourquoi, c'est aux organisations dans la moitié des cas de prévoir leurs propres modes de fonctionnement. Quand tel n'est pas le cas, on note tout de même la volonté d'instaurer une forte coopération entre les organisations adhérentes et les autorités qu'elles soient américaines ou européennes.

[122] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p. 10.
[123] *Ibid.*
[124] . MONELEONE (S), PUCCIO (L) (EPRS), « Du Safe Harbour au Privacy Shield : Avancées et insuffisances des nouvelles règles de transfert des données UE-États-Unis », Janvier 2017 PE 595.892, p. 30.
[125] *Ibid.*

2) Des mécanismes de garanties impliquant les autorités américaines et européennes

Le Privacy Shield se devait de répondre aux critiques de la Cour sur l'accès automatique et systématique aux données des Européens par les autorités américaines ainsi qu'au manque de suivi sur l'application qu'un tel accord nécessite.

a) Limitation d'accès aux données par les autorités américaines et mécanisme de l'Ombudsperson

La Commission européenne a obtenu après le scandale PRISM, des garanties directes de la part des institutions américaines poussées à concéder plus qu'à leur habitude et à revoir la législation concernant la collecte de données par les autorités publiques. Pour rappel la collecte automatique, systématique et sans garde-fous des données des citoyens européens est une des raisons principales ayant poussé la Cour européenne de justice a invalidé l'accord Safe Harbour.[126] Il convenait donc pour la Commission de négocier un accord respectant la décision Schrems. En effet, après avoir décidé de l'adéquation d'un accord permettant ce genre de mesure exorbitante pendant près de quinze ans, la crédibilité européenne était en jeu. D'autre part, il s'agissait pour les Américains de se racheter une conduite par le biais de mesures nationales ayant également pesé dans la recherche d'un nouvel accord et dans la décision d'adéquation de la Commission. En 2014, le président Obama signe la directive stratégique présidentielle n° 28 (PPD-28)[127]. Cette directive à force obligatoire, a pour but de limiter les opérations de renseignements d'origine électromagnétique, donc la collecte via les médias électroniques notamment liés directement au programme PRISM qui permettait un accès en « backdoor » aux serveurs des grandes sociétés du numérique mettant en évidence les relations qu'elles entretiennent avec les autorités américaines de renseignement.[128] Dans la continuité de cette directive, les États-Unis se sont engagés dans les négociations du Privacy Shield à ne collecter et ne traiter les données européennes que pour un usage nécessaire et proportionné conformément à ce que la directive « Obama » prévoit.[129] À titre d'exemple, le texte américain

[126] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.
[127] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p. 13.
[128] LEROY (F), *Surveillance : Le risque totalitaire*, Éditions actes sud, juin 2018 p.9.
[129] CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p. 444.

impose la minimisation des données personnelles traitées consistant à réduire leur temps de conservation par les autorités américaines, mais prévoit également que la collecte doit se baser sur une finalité de renseignement extérieur ou de contre-espionnage. [130] De plus, en 2015, l'USA Freedom Act est adopté. Ce dernier a entre autres pour but de venir interdire en partie la collecte en vrac d'enregistrements comme prévu par le Patriot Act et notamment la section 2015, même si son objectif général tel que cité en introduction du texte est plus large.[131] Après que les États-Unis aient décidé de montrer patte blanche au monde entier, ils proposaient dans une lettre adressée à la Commission[132] de prévoir un médiateur indépendant spécialisé dans la réponse aux problématiques de données collectées par les autorités de renseignements à des fins de sécurité nationale, mécanisme d'exception consacré par le Privacy Shield[133] : il s'agit donc de l'Ombudsperson.

L'Ombudsperson est indépendant des services de renseignements et n'a de comptes à rendre qu'au Secrétaire d'État au développement économique, à l'énergie et à l'environnement. Sa fonction est de travailler étroitement avec les instances traitant les requêtes à propos de l'accès par les autorités publiques aux données personnelles en provenance d'Europe.[134] Il doit accuser réception des demandes de citoyens européens qui ont été transmises par l'intermédiaire des autorités de contrôle aux citoyens directement après en avoir étudié la recevabilité. Il est donc le médiateur principal dans la conduite de la potentielle investigation. En fonction de la demande, il peut donc demander des informations et un accès aux documents en conformité avec le Freedom of information Act qui prévoit des possibilités d'accès à des documents d'agences fédérales pour toute personne, quelle que soit sa nationalité. S'il y a lieu, il va transférer toutes demandes accusant une violation de la législation américaine à l'autorité publique concernée.[135]

Bien que le Privacy Shield contienne toujours une exception sur la collecte de données par les autorités pour des raisons tenant notamment à la sécurité nationale, c'est sur la base de l'évolution de la législation américaine que la Commission a considéré que le minimum d'exigence imposé par la Cour en matière de limitations quand une législation comporte une

[130] Presidential Policy Directive n°28, PPD-28 du 17 janvier 2014 sur les activités de renseignements électroniques.
[131] Voir Art. 1 du Freedom Act.
[132] Lettre de John F. Kerry au Commissaire à la protection des données V. Jourová du 7 juillet 2016.
[133] Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Overview.*
[134] Principes de l'accord *EU-U.S Privacy Shield,* section *Ombudsperson Mechanism Annex A.*
[135] *Ibid.*

ingérence dans les droits fondamentaux au sens de la charte[136], était rempli. De plus, le mécanisme d'Ombudsperson est de nature à participer à une protection juridictionnelle effective des citoyens européens aux États-Unis.[137]

Le mécanisme de l'Ombudsperson est édifiant puisqu'il montre que l'équilibre acceptable, c'est être sur le fil de ce qui est juridiquement acceptable en matière de protection européenne des données personnelles. En effet, le raisonnement de la Commission base l'efficacité du mécanisme sur des présomptions d'effectivité du droit américain. Mais c'est bien ce mécanisme qui permet de supposer que le droit américain est adéquat et que les garanties apportées sont conformes aux principes du Privacy Shield en instaurant ce qui ressemble à un embryon de contre-pouvoir du côté américain ; embryon de contre-pouvoir d'influence européenne puisqu'on constate qu'il possède au moins théoriquement certaines prérogatives, notamment en matière d'accès aux informations, que l'on retrouve prêtées aux autorités de contrôle européennes[138]. En plus de ce mécanisme, l'instauration d'un réexamen annuel conjoint révèle que les Américains ont dû faire des concessions à la faveur de l'Union européenne.

b) Le réexamen conjoint

« De même, au regard du fait que le niveau de protection assuré par un pays tiers est susceptible d'évoluer, il incombe à la Commission, après l'adoption d'une décision au titre de l'article 25, paragraphe 6, de la directive 95/46, de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifiée en fait et en droit. Une telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard. »[139]

Cette critique forte à l'égard de la Commission par les juges européens est à la base du mécanisme du réexamen conjoint. En effet sur la validité de l'accord, la Cour reprochait évidemment le manque de suivi de l'application de l'accord tandis que la Commission s'était

[136] Il s'agit ici des articles 7 et 8 qui étaient visés par la Cour dans l'arrêt Schrems.
[137] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, p. 28.
[138] Art 28 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[139] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.

tiré une balle dans le pied en admettant de manière faussement cachée que le Safe Harbor n'était pas valide.[140]

Cela a donc mené la Commission et les Américains à décider un examen annuel du Programme afin de s'assurer que l'accord encadre bien les problématiques pour lesquelles il a été créé et que les deux parties puissent le cas échéant l'adapter aux enjeux et aux changements auxquels il devrait faire face.[141] La commission en fait d'ailleurs longuement mention dans la décision d'adéquation indiquant qu'en outre de la vérification annuelle, et du suivi constant nécessaire avec les autorités américaines, un examen périodique annuel conjoint de la décision d'adéquation devra être également être instauré.[142] C'est donc bel et bien une double vérification périodique à laquelle les instances européennes et américaines devront procéder. Il est d'ailleurs précisé que ce réexamen annuel conjoint fera l'objet d'un rapport public qui devra être présenté au Parlement européen et au Conseil.

Ce mécanisme est surtout mis en place afin de vérifier que les autorités américaines respectent bien leurs engagements en ce qui concerne les limitations de collecte de données personnelles des citoyens européens dans le cadre des exceptions prévues par le Bouclier, preuve que la philosophie européenne sur les données personnelles met l'accent sur la protection et le respect des droits fondamentaux, plutôt que sur la liberté de circulation teintée d'un voile protectionniste. En effet, la Commission précise que lors d'un examen conjoint, si des manquements de la part des autorités américaines sont constatés, elle se réserve le droit de suspendre, d'abroger ou de modifier la décision.[143] Du point de vue américain, la seule condition était que le libre flux de données soit acceptable, afin de stimuler le commerce et l'innovation comme le soulignait Penny Pritzker, alors au poste de Secrétaire au commerce des États-Unis, lors d'une conférence de presse à Bruxelles[144]. Elle avait d'ailleurs confirmé que la

[140] Communication COM(2013)847 de la Commission au Parlement européen et au Conseil du 27 novembre 2013 relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire.
[141] Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, lettre de la FTC au Commissaire à la protection des données V. Jourová du 23 Février 2016.
[142] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis p. 33.
[143] *Ibid.* p. 34.
[144] Remarques par la Secrétaire américaine au commerce Penny Pritzker à la conférence de presse du 12 juillet 2016 du Département du Commerce américain sur l'accord *EU-U.S. Privacy Shield.*

condition était remplie, cette dernière représentant pour les Américains la condition la plus importante. [145]

Il semblerait dès lors que ce mécanisme soit un garde-fou spécialement mis en place afin de respecter les exigences de la Cour concernant les limites de traitement par les autorités américaines. En ce sens, il doit être analysé que la Commission se porte garante de la bonne application des principes par les États-Unis en endossant le costume de gendarme du Privacy Shield. Cela montre la volonté de créer des règles contraignantes sur la tête des autorités américaines afin d'éviter des abus en matière de surveillance généralisée.

B) Le Privacy Shield et la prise en compte du Règlement général sur la protection des données

Ce sont en premier lieu le G29 ainsi que le contrôleur européen de la protection des données (CEPD) qui alertent sur la nécessité de prendre en compte l'arrivée du nouveau règlement général sur la protection des données (RGPD) qui est voté en 2016 entre le moment où l'accord est trouvé et le moment où la décision d'adéquation de la Commission est adoptée. Dès lors, des interrogations se posent quant au niveau adéquat de protection. En effet, ce qui peut paraître adéquat sous l'égide de la directive de 95 ne l'est pas forcément sous l'égide du nouveau règlement. Ainsi, comme le souligne le G29, la nouvelle législation en vigueur a pour ambition d'être plus protectrice des données personnelles des citoyens européens en instaurant de nouvelles notions comme le droit à la portabilité, des obligations supplémentaires pour les responsables de traitement comme le respect du principe de Privacy by Design.[146] Le CEPD quant à lui soulève le fait que le nouveau texte est plus exigeant et plus détaillé concernant les décisions d'adéquations et le fonctionnement d'autorité de contrôle indépendante dans le pays dans lequel les données sont transférées.[147] En effet, l'article 45 du nouveau règlement insiste beaucoup plus sur la nécessité de fonder l'adéquation, sur l'étude d'une législation pertinente relative à l'accès aux données par les autorités publiques du pays en matière de sécurité nationale, de sécurité publique et de défense[148] ; dont les États-Unis sont évidemment la cible directe. Les juges ayant déjà invalidé l'accord précédent car il ne respectait pas les standards

[145] SCHWARTZ M. (P), PEIFER (K.N), « Transatlantic Data Privacy Law », *Geo. L.J.* volume 106, 2017, pp. 115 à 179 p.165.
[146]Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.
[147] Avis 4/2016 du Contrôleur européen à la protection des données du 30 mai 2016 concernant le « bouclier vie privée UE-États-Unis » (Privacy Shield), Projet de décision d'adéquation.
[148] Art. 45 du RGPD.

nécessaires à la protection adéquate au regard de l'article 25 de la directive, il fallait donc prendre en compte un niveau de protection plus élevé afin de ne pas seulement se borner à respecter les critères édictés par la directive. Certains auteurs américains notamment ont cependant considéré que les deux articles étaient analogues puisqu'ils obligeaient à un niveau de protection adéquat[149]. Ce propos est discutable au prisme de ce qui a été mentionné plus haut. Il ne s'agit pas en effet de lire l'article 45 stricto sensu, mais bien d'étudier le cadre juridique avec lequel il fait corps. De plus, il semble erroné de se borner au simple critère de protection adéquat, quand on constate que l'article est en réalité beaucoup plus détaillé comme l'explique le CEPD. On réalise alors que la prise en compte du RGPD du côté des États-Unis a crispé les esprits puisque du côté de la doctrine, on estime que la nouvelle législation européenne creuse un écart encore plus grand entre les conceptions européennes et états-uniennes, ne facilitant pas l'adoption de telles règles communes.[150] Paul Schwartz considère d'ailleurs que la conception américaine libérale permet d'innover dans de nouvelles formes de traitement de données et notamment dans les nouveaux domaines d'activités qui sont aux États-Unis par définition non régulés sectoriellement, puisque nouveaux. En filigrane, il insinue subtilement que dans le cadre d'une régulation globale comme celle mise en place en Europe, cela serait considéré comme une atteinte à la protection des données plutôt que comme une innovation.[151]

Toujours est-il, que la Commission avec l'esprit conciliateur que l'on lui connaît, a suivi dans la décision d'adéquation les recommandations du G29, conseillant un examen de l'accord peu après que le RGPD ne soit adopté. Voilà donc qui permettait de gagner du temps par rapport à l'entrée en vigueur du RGPD de manière à ne pas faire du Privacy Shield un accord temporaire, alors que c'est parfois la destinée que l'on lui prêtait du côté européen dès sa révélation par la Commission,[152] ou à ne pas en faire un accord remplacé par d'autres mécanismes comme les BCR le tournant ainsi en fiasco.[153]

---

[149] LINN (E.), « A Look into the Data Privacy Crystal Ball: A survey of possible Outcomes for the EU-U.S Privacy Shield Agreement », *Vanderbilt Journal of Transnational Law*, volume n°50, 2017, pp. 1311 à 1358, p. 1320.
[150] PHILOUZE (A.L.), « The EU-US Privacy Shield: Has Trust Been restored », *The European Data Protection Law Review*, volume n°3, 2017, pp. 463 à 472, p. 466.
[151] SCHWARTZ M. (P.), « The EU-US Privacy collision: a turn to institutions and procedures », *Harvard Law Review*, volume n°126, 2013.
[152] CASTETS-RENARD (C.), « Le Privacy Shield », *DallozIP/IT*, n°3, Mars 2016 p.113.
[153] VOSS W. (G.), « The future of transatlantic data flows: Privacy Shield or bust », Journal of internet Law vol.19, n°11 May 2016, pp. 9 à 18, p. 16.

CHAPITRE II : Le Privacy Shield : un accord encore fragile

Le Privacy Shield est un accord qui reste très fragile dans la mesure où il subsiste encore de nombreux doutes quant à sa conformité suffisante à la législation européenne (Section 1), mais également car il y a de nombreuses carences dans son application et dans son contrôle au niveau américain (section 2)

Section 1 : Les doutes quant à la conformité suffisante à la législation européenne

Si des doutes sont émis, c'est parce que les garanties appropriées sont jugées insuffisantes (I), mais également car les mécanismes d'exceptions de l'accord qui sont prévus en faveur des autorités américaines sont très controversés (II).

I) Des garanties appropriées insuffisantes

Bien qu'offrant un plus haut niveau de protection en vue de se conformer à la législation et aux exigences des juges européens, le Privacy Shield semble assez insuffisant sur de nombreux points. En effet, de fortes réserves étaient déjà émises dès la version initiale du texte en février 2016 (A). L'évolution législative des deux parties a également affecté le fonctionnement de ces garanties (B).

A) Des réserves émises dès la conclusion de l'accord

Le moins que l'on puisse dire, c'est que le nouvel accord n'a pas fait l'unanimité, que ce soit au sein de la doctrine ou même entre les différents acteurs européens. En effet, si un certain nombre d'améliorations étaient saluées, certains auteurs, ainsi que le G29 soulevaient déjà des interrogations.

Sur la forme dans un premier lieu, l'accord est extrêmement complexe à décortiquer et a fortiori, à comprendre.[154] Il est effectivement composé en plus des principes, d'un certain nombre de textes, de lettres d'engagements, d'annexes dont on peut d'ailleurs se demander quelle réelle force elles ont. En effet lors des négociations du Privacy Shield, en 2015-2016, l'élection présidentielle aux États-Unis arrive à grands pas et cela signifie que les responsables d'administration ayant pris les engagements épistolaires au titre du Privacy Shield, arrivent pour

[154] CASTETS-RENARD (C), « L'adoption du Privacy Shield sur le transfert de données personnelles », *Recueil Dalloz* n°28, Août 2016, p. 1696.

la plupart en fin de mandat,[155] et on peut donc légitimement se demander si ces engagements seraient renouvelés. De plus, on ne connaît pas la valeur de ces engagements, et la Commission, dans sa décision d'adéquation, se borne simplement à rappeler leur importance sans jamais les qualifier juridiquement.[156] Dès lors, la confiance accordée aux Américains semble quelque peu aveugle. À juste titre, certains fervents défenseurs de la protection des données personnelles avaient exprimé des inquiétudes sur le fait que de simples engagements ne constituaient pas une assurance nécessaire du respect de l'accord du côté américain.[157] C'est entre autres pour cette raison que la Commission dans son premier rapport annuel avait en introduction mentionné que le changement d'administration opéré en janvier 2017 avait rendu cet examen conjoint particulièrement pertinent.[158] Le G29 avait par ailleurs dans l'avis rendu le 13 avril 2016, relevé que le fait que les principes et les garanties soient mentionnés tantôt dans le corpus de textes du Privacy Shield, tantôt dans la décision d'adéquation, était de nature à complexifier structurellement l'accord et à le rendre obscur et non-accessible pour les personnes concernées, pour les organisations et pour les autorités de contrôle nationales.[159] Finalement, l'accord assez indigeste débouche sur deux possibilités pour les acteurs concernés ; le premier est de le décortiquer texte par texte, le traduire le cas échéant et enfin le comprendre ; le second est de faire confiance à des guides, à des résumés émanant d'organismes divers et variés, officiels ou officieux. On déplorera de fait que le problème n'ait été soulevé dans aucun de deux examens annuels ayant déjà été effectués à l'heure actuelle puisqu'il semble primordial que l'exercice des garanties actives comme les recours pour les personnes passe par un texte juridique clair. De plus, on peut souligner que l'accessibilité au texte est toujours compliquée. En effet, les annexes et autres documents ont disparu du site de la Commission, excepté la décision d'adéquation et seul le site officiel du gouvernement américain permet d'accéder à une version de l'accord. Cela crée de fait une distorsion entre les textes classés en annexe que la Commission avait publiés en 2016 et ce qui est publié sur le site américain ne reprenant pas la même classification. En réalité, et comme relevé par le G29 en décembre 2017, le Privacy

[155] *Ibid*.
[156] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.
[157] DEIGHTON (A.), « The EU-US Privacy Shield - is it strong enough? », *Privacy & Data Protection*, volume n°16, issue n°4, Mars 2016, pp.8 à 10.
[158] Rapport COM(2017)611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* p. 3.
[159] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.

Shield s'adresse aux entreprises en occultant le fait qu'il doit aussi s'adresser aux personnes concernées auxquelles il doit notamment apporter des garanties suffisantes.[160]

Ensuite, des interrogations subsistaient quant à la transparence à la charge des entreprises envers les personnes concernées. Le G29 relevait que l'entreprise autocertifiée américaine devrait être plus explicite concernant notamment l'exercice les droits de rectification, de suppression quand la donnée est inexacte ou traitée contrairement aux principes.[161] En effet, aucun détail n'est donné sur ce qui est considéré comme contraire aux principes et dans quels cas les personnes concernées peuvent exercer leurs droits. Il est évident que dans ce cas par exemple, l'argument purement marketing de la possibilité d'exercice des droits peut être mis en avant, sans que cela ne reflète la réalité, tandis que des entreprises européennes devant respecter la législation européenne se retrouveraient dans une situation concurrentielle moins favorable de fait, puisque devant de toute façon respecter une législation plus contraignante.[162] D'ailleurs lors du premier rapport conjoint de 2017, la Commission avait pointé du doigt le fait que les entreprises dont la certification était pendante, donc toujours en cours d'examen par le DoC et de facto absentes de la liste tenue par ce dernier, pouvaient tout de même mentionner publiquement cette certification.[163] Dès lors, l'obligation de transparence et d'information destinée notamment à éviter les fausses certifications se trouvait en partie vidée de son utilité. Pour cette raison, la Commission avait recommandé que la publication de la certification ne puisse pas être effectuée avant la finalisation de la procédure auprès du DoC. Si ce problème semble depuis avoir été réglé[164], cela montre que les doutes émis du côté européen se justifiaient et continuent de se justifier par un manque de rigueur procédurale combiné à un gouffre juridique entre la protection accordée en droit de l'UE et celle accordée en droit américain.

En termes de limitation de la conservation des données et de potentiels transferts ultérieurs vers des pays tiers, le G29 et la doctrine relevaient également que les garanties apportées n'étaient pas suffisantes quant au fait que les entreprises suppriment bien les données

---

[160] REES (M.), « Privacy Shield : le sombre bilan des CNIL européennes, la menace d'un recours », www.nextinpact.com, publié le 6 décembre 2017. https://www.nextinpact.com/news/105768-privacy-shieldle-sombre-bilan-cnil-europeennes-menace-dun-recours.htm

[161] *Ibid.*

[162] CASTETS-RENARD (C), « L'adoption du Privacy Shield sur le transfert de données personnelles », Recueil Dalloz n°28, Août 2016, p. 1696.

[163] Rapport COM(2017)611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* p. 4.

[164] Rapport COM(2018)860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le deuxième examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* p. 2.

au bout d'une période de temps donnée et qu'il y avait certes des obligations renforcées sur l'organisation certifiée de s'assurer que son sous-traitant respecte bien les finalités qui sont établies par voie contractuelle, mais ne prévoit aucune obligation à la charge de l'entreprise quand le transfert ultérieur de données est également transfrontière.[165] Cela signifie que si le contrat doit assurer le même degré de protection comme le souligne la Commission dans sa décision d'adéquation[166], nul n'est fait mention d'une obligation de l'entreprise de vérifier si le pays dans lequel le transfert ultérieur est effectué, apporte un niveau de protection adéquat. Cependant, il faut apporter une nuance. En effet, l'essence du Privacy Shield est d'apporter un cadre juridique à la libre circulation des données personnelles entre les États-Unis et l'Union européenne afin de protéger les citoyens européens et non d'instaurer la législation européenne aux États-Unis. De cette façon, on voit mal comment l'on pourrait justifier une telle extension européenne du droit applicable envers les organisations certifiées et envers les États dont les organisations sont destinataires de ces transferts ultérieurs. Cela pourrait d'ailleurs être perçu comme une forme d'ingérence.

Une des garanties les plus importantes et sur lequel la Commission fonde beaucoup d'espoir[167], le mécanisme d'Ombudsperson (*voir supra*), est, elle aussi, sujette à un certain scepticisme du côté européen. En effet, dans l'avis du 13 avril 2016, le G29 consacre beaucoup de lignes à l'étude du mécanisme. Force est de constater qu'il en ressort des réserves sur plusieurs points.[168] Nous nous concentrerons ici seulement sur la réserve concernant le caractère d'indépendance de l'Ombudsperson et de l'exercice des pouvoirs en découlant. En premier lieu, la Commission dans sa décision d'adéquation n'a pas suivi les recommandations du G29 sur les modalités de désignation et de fin de fonctions qui ne garantissaient pas l'exercice des fonctions à l'abri de toute influence extérieure.[169] En effet, il s'agit du sous-secrétaire nommé médiateur par le Secrétaire d'État américain comme en témoigne la lettre à la Commission de juillet 2016 de John Kerry qui avait nommé sa sous-secrétaire Catherine A. Novelli au poste de médiateur.[170] De plus, il est bien spécifié que l'indépendance de l'Ombudsperson est consacrée

[165] ALVAREZ (D.), « Safe Harbor is dead; Long live the Privacy shield », www.americanbar.org, publié le 20 mai 2016.
https://www.americanbar.org/groups/business_law/publications/blt/2016/05/09_alvarez/
[166] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis. p. 5.
[167] *Ibid.*
[168] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.
[169] METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85 p. 4.
[170] Lettre de John F. Kerry au Commissaire à la protection des données V. Jourová du 7 juillet 2016.

seulement envers la communauté du renseignement, mais qu'il rend des comptes au Secrétaire d'État.[171] Cela pose un problème de transparence assez flagrant quand l'on connaît l'étroitesse des relations entre l'exécutif américain et les services de renseignement qu'elles soient bonnes ou mauvaises.[172] De plus, le Privacy Shield ne créant pas de critère spécial de révocation du médiateur, cela signifie que ce dernier est révocable dans les mêmes conditions que celles de sa fonction de sous-secrétaire.[173] Cela laissait donc redouter un mécanisme de garantie de façade dépourvu en réalité de caractère contraignant notamment dans l'exercice de vrais pouvoirs d'investigations.[174] Les limites de ce mécanisme se sont déjà manifestées après les présidentielles Américaines de 2017 démontrant par ailleurs son instabilité. En effet, en janvier 2017, un médiateur temporaire a été désigné de façon à assurer la transition dans le changement d'administration. Toutefois, la Commission relève dans l'examen annuel conjoint d'octobre 2017 qu'un médiateur permanent n'a toujours pas été désigné.[175] Le G29 avait quant à lui été plus critique dans l'avis suivant l'examen conjoint[176], rappelant les mêmes réserves qu'en 2016 et rappelant également que par son statut et ses pouvoirs, l'Ombudsperson ne peut être considéré comme un recours efficace devant un tribunal, comme exigé par l'article 47 de la Charte européenne des droits fondamentaux.[177] En effet, durant l'examen conjoint, les Américains avaient expliqué que la procédure d'accès aux documents par l'Ombudsperson avec les services en cause était classée secrète. Ce manque de transparence avait soulevé des doutes quant à la fiabilité du mécanisme. Mais en 2018 lors du deuxième examen conjoint, le plus récent donc, l'accent est encore une fois uniquement mis sur le caractère intérimaire du poste par la Commission. En effet depuis l'arrivée de la nouvelle administration à la tête des États-Unis d'Amérique, la Commission ne note aucune avancée sur le caractère permanent de la nomination du médiateur, mais souligne que le gouvernement américain reconnaît le besoin

[171] Décision d'exécution (UE)2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.
[172] LE VOGUER (G.), « Donald Trump et les services de renseignement : une relation sous tension », *revue LISA*, volume 16, n°2, 2018.
[173] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.
[174] *Ibid.*
[175] Rapport COM(2017)611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* p. 6.
[176] REES (M.), « Privacy Shield : le sombre bilan des CNIL européennes, la menace d'un recours », www.nextinpact.com, publié le 6 décembre 2017.
https://www.nextinpact.com/news/105768-privacy-shieldle-sombre-bilan-cnil-europeennes-menace-dun-recours.htm
[177] Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du *EU – U.S. Privacy Shield* p. 4.

d'un progrès rapide dans cette nomination permanente.[178] Le Comité Européen à la Protection des Données (CEPD) instauré par le RGPD, reprend quant à lui les mêmes conclusions que le G29. Pour lui, le statut de l'Ombudsperson et ses pouvoirs ne permettent toujours pas de considérer qu'il est un recours efficace devant un tribunal au sens de l'article 47 de la Charte, et ce pour les mêmes raisons que l'année précédente, même s'il note une avancée en matière de transparence sur la procédure d'accès aux données par l'Ombudsperson qui a été « partiellement » révélée.[179]

On se rend donc compte que depuis que les premières réserves ont été émises, il n'y a pas d'améliorations significatives des garanties imparfaites prévues par le Privacy Shield. Véritables velléités de négocier ou politiques délibérées des petits pas pour satisfaire les uns et les autres en évitant l'inertie totale, les constats sont là et les leçons sont à tirer puisque l'accord a déjà été attaqué. En effet, en 2018, la commission des libertés du Parlement européen avait demandé sa suspension estimant qu'il n'assurait pas une protection suffisante, au lendemain de l'affaire *Cambridge analytica*,[180] tandis que d'autres faisaient de la renégociation de l'accord un argument de campagne lors de la dernière élection présidentielle française.[181] Cependant, quand en 2018, le Secrétaire du commerce américain Wilbur Ross considérait le RGPD comme une barrière au commerce international, on comprend que les avancées se fassent au compte-goutte.[182]

Par ailleurs, l'assurance de ces garanties a tendance à se déliter de plus en plus du fait de l'évolution législative des États-Unis notamment.

B) L'évolution législative américaine affectant les garanties de l'accord

Il faut constater que si l'accord en lui-même n'a pas beaucoup évolué depuis son adoption, il n'en est pas de même en matière de législations étatiques que ce soit du côté

---

[178] Rapport COM(2018)860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le deuxième examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* pp. 4 et 5.
[179] Rapport du Comité européen de la protection des données du 22 janvier 2019 sur le deuxième examen annuel conjoint du *EU – U.S. Privacy Shield*, p. 19.
[180] REES (M.), « Au Parlement européen, la commission Libe demande la suspension du Privacy Shield », www.nextinpact.com, publié le 12 juin 2018.
https://www.nextinpact.com/news/106586-au-parlement-europeen-commission-libe-demande-suspension-privacy-shield.htm
[181] Communiqué du Conseil national du numérique sur le sujet « pourquoi le Privacy Shield doit être renégocié » du19 septembre 2017, www.cnnumérique.fr.
https://cnnumerique.fr/pourquoi-le-privacy-shield-doit-etre-renegocie
[182] WILBUR (R.), « EU Data privacy laws are likely to create barriers to trade », www.ft.com, publié le 30 mai 2018.
https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c

européen ou du côté américain. En effet, l'UE a adopté en 2016 le nouveau règlement général sur la protection des données (RGPD) poursuivant les mêmes objectifs que la directive, mais adaptant les textes aux évolutions technologiques et instaurant une protection plus forte des données personnelles des citoyens européens.[183] Ce nouveau règlement est entré en vigueur en mai 2018. Du côté américain, des lois et décrets sont entrés en vigueur affectant directement ou indirectement la protection des données personnelles. Dans ce paragraphe il sera uniquement question de lois fédérales régissant de facto le Privacy Shield puisque prévalant généralement sur le droit des États.[184] Il se trouve que ces dernières ont plutôt tendance à réduire la protection des données personnelles en n'empêchant pas la surveillance généralisée ou en réduisant les possibilités de recours pour les citoyens européens. Il en résulte donc que le Privacy Shield est affaibli dans sa force contraignante, ce qui n'aide pas à maintenir la stabilité nécessaire dans l'exercice des garanties qu'il devrait apporter notamment en matière de collecte de données par les autorités américaines.

1) La réautorisation de la section 702 du FISA

Pour rappel, la section 702 du Foreign Intelligence Surveillance Act habilite le Procureur général des États-Unis et le Directeur du renseignement national à autoriser conjointement, le ciblage de personnes dont on peut raisonnablement croire qu'elles se situent en dehors des États-Unis, dans le but d'obtenir des informations de renseignement extérieur.[185] Cette règle est encadrée par cinq limitations, la dernière notamment, imposant que le ciblage soit fait conformément au quatrième amendement de la constitution des États-Unis d'Amérique.[186] Cet amendement garantit les droits des citoyens sur leur personne, leur domicile, leurs papiers et effets, dans le cadre des perquisitions et saisies. Aucun mandat ne sera délivré, si ces dernières ne sont pas motivées sur la base d'une présomption sérieuse, corroborée par serment ou déclaration, ou sans que le mandat ne décrive particulièrement le lieu à perquisitionner et les personnes ou les choses à saisir.[187] Cela constitue le rempart de protection de la vie privée pour les citoyens américains. Les deux hauts fonctionnaires doivent

[183] FÉRAL-SCHUHL (C.), *Cyberdroit 2018/19*, édition n°7, Praxis Dalloz, Juillet 2018 pp. 22.23.
[184] La récente loi Californienne sur la protection des données personnelles fera l'objet d'une étude plus poussée dans la deuxième partie du mémoire.
[185] DONOHUE K (L.), « Section 702 and the collection of international telephone and internet content », *Harvard Journal of Law and Public Policy*, volume 38, issue 1, 2015, pp. 117 à 275, p.24.
[186] Art. 1881a. U.S Code, Titre 50 U.S.C.
[187] 4e amendement de la Constitution des États-Unis d'Amérique, traduction effectuée par le Professeur Jean-Pierre Maury à l'université de Perpignan et disponible à l'adresse suivante : http://mjp.univ-perp.fr/constit/us1787a.htm.

également mettre en place des procédures de limitation du ciblage et certifier que ces procédures respectent bien les limitations prévues dans le texte. Cela passe également par des examens de l'application des procédures au moins deux fois par an.[188] Enfin, cette autorisation doit être approuvée par le Congrès. Cependant, les recours prévus ne sont pas exerçables par les individus, mais bien par les compagnies de communications électroniques à qui les informations relatives au ciblage sont demandées, ce qui fait sens au regard de la finalité du texte.[189]

L'autorisation de la section 702 du FISA, arrivait à expiration à la fin de l'année 2017 et devait donc faire l'objet d'une réactivation (ou réautorisation) au début de 2018.[190] La Commission et le G29 avaient conseillé aux États-Unis au terme de l'examen conjoint de 2017, de profiter de cette réactivation pour y insérer des amendements contenant les dispositions de la PPD28 signée par le Président Obama en 2014,[191] afin que cette dernière soit plus protectrice des données personnelles des personnes face au système de renseignement et de surveillance américain. Quand bien même le « Privacy and Civil Liberties Oversight Board » (PCLOB)[192] dans un rapport de 2014 avait détaillé ce que le texte du FISA signifiait par procédure de minimisation, et les expliquant notamment techniquement par le fait que les services de renseignements tels que la NSA dans l'utilisation de programmes comme PRISM ou UPSTREAM, ne peuvent que collecter des données par mots-clés relatifs aux finalités définies sans aller au-delà, ce qui exclut la collecte en vrac,[193] la garantie donnée n'était pas suffisante pour les Européens.

Mais le 11 janvier 2018, le Congrès américain approuve la réautorisation de la section 702 du FISA sans prendre en compte les doléances des Européens formulées dans le cadre du premier examen du Privacy Shield,[194] et l'entrée en vigueur est marquée par la

[188] DONOHUE K (L.), « Section 702 and the collection of international telephone and internet content », *Harvard Journal of Law and Public Policy*, volume 38, issue 1, 2015, pp. 117 à 275, p.24.
[189] *Ibid.* p. 27.
[190] Proposition de résolution 2018/2645(RSP) du Parlement européen, du 26 juin 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis.
[191] Voir à ce titre le Rapport COM(2017)611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* et le Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du *EU – U.S. Privacy Shield.*
[192] Le Privacy and Civil Liberties Oversight Board (PCLOB) est une agence indépendante au sein du pouvoir exécutif établie par le Congrès en 2004 afin de conseiller le Président ou d'autres branches de l'exécutif et de s'assurer que les problématiques en termes de respect de la vie privée sont prises en compte.
[193] Rapport du PCLOB du 2 juillet 2014, sur le programme de surveillance mené conformément à la section 702 du FISA p. 51.
[194] Proposition de résolution 2018/2645(RSP) du Parlement européen, du 26 juin 2018.

signature des amendements par le Président Trump.[195] Si du côté de la doctrine américaine, on salue les progrès des amendements effectués en faveur de la protection des données personnelles en termes de transparence, de garde-fous techniques notamment,[196] la nouvelle est assez mal reçue côté européen, puisque le Parlement dans sa proposition de résolution du 26 juin 2018 regrette d'une part que les garanties prévues par la directive PPD28 ne soient pas incluses, mais également que les amendements ne portent que sur des points procéduraux sans s'attaquer à la substance du problème.[197] Au regard de ces premiers éléments, il semble que les États-Unis aient fait le dos rond le temps que l'orage Snowden passe avant de réintroduire des points législatifs leur permettant de s'affranchir de certaines contraintes fixées en matière de renseignement. Plus inquiétant, c'est l'absence de recours pour les citoyens non américains des collectes effectuées sous l'égide de la section 702 du FISA. De facto, on comprend d'autant plus la nécessité du bon fonctionnement de l'ombudsperson dont la force est de pouvoir déboucher sur une action en justice devant les tribunaux américains.

2) Les ordres exécutifs 12333 et 13768

Il faut souligner qu'en termes de garanties et notamment de recours, les mêmes problématiques se posent avec l'ordre exécutif américain n° 12333 qui a également pour fonction d'étendre la force de frappe du gouvernement américain en matière de renseignement extérieur et sert également de base légale à la NSA dans l'interception de communications électroniques.[198] Enfin, les garanties des citoyens européens en termes de recours se sont encore amenuisées puisqu'en 2017, le Président Trump signe un autre ordre exécutif n° 13768 sur le renforcement de la sécurité publique à l'intérieur des États-Unis. Ce dernier dans sa section 14 exclut expressément toutes les personnes qui ne sont pas des citoyens américains ou des résidents permanents des mécanismes de protection au titre du Privacy Act.[199][200]

[195] LIPTAK (A.), « President Donald Trump has signed the FISA reauthorization bill », www.theverge.com, publié le 20 janvier 2018.
https://www.theverge.com/2018/1/20/16913534/president-donald-trump-signed-fisa-amendments-reauthorization-act-of-2017-section-702
[196] MARGULIES (P.), « Reauthorizing the FISA Amendments Act: A Blueprint for enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities », Journal of Business & Technology Law, volume 12, issue 1, 2016 pp. 23 à 52, p. 2.
[197] Proposition de résolution 2018/2645(RSP) du Parlement européen, du 26 juin 2018.
[198] WEN J. (C.), « Secrecy, Standing, and executive Order 12,33 », 89 Southern California Law Review, volume 89, 2016, pp. 1099 à 1138, p. 1108.
[199] Section 14 du *Executive order 13768: Enhancing Public Safety in the Interior of the United States* du 25 janvier 2017.
[200] Le Privacy Act est une loi de 1974 qui établit un code de bonnes conduites gouvernant la collecte et le traitement d'informations dans le cadre d'un système d'enregistrement géré par une agence fédérale. Notamment

Il faut donc retenir que les autorités américaines ont beaucoup de possibilités légales différentes de collecter des données sur des citoyens européens certes, mais également de bloquer les garanties qui sont prévues à ce titre par le Privacy Shield et par la décision d'adéquation sur la base des engagements américains. Il faut être lucide quant au fait que le Privacy Shield est nécessairement fragilisé par l'instauration d'un mécanisme d'exception de collecte par les autorités américaines sur le fondement de la sécurité nationale et que les garanties apportées ne sont pas suffisantes puisque les législations ont tendance à nuire au fonctionnement normal de l'accord. C'est donc difficilement compréhensible qu'un accord présentant de telles insuffisances, de telles instabilités au regard de la réalité des faits soit considéré comme étant suffisamment conforme à la législation européenne puisqu'il paraît souffrir de trop d'exceptions extérieures aux garanties qu'il doit apporter pour qu'une décision d'adéquation puisse être établie notamment au regard de l'article 45 du RGPD qui prône l'évaluation de :

> […] l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ; […][201]

Le moins que l'on puisse dire, c'est qu'à la lecture de ces critères, les engagements pris par les Américains et rentrant dans le corpus de l'accord, apparaissent comme étant très discutables en termes de conformité à la législation européenne.

---

toutes les informations relatives à la tenue de ces registres sont rendues publiques. Pour en savoir plus, sur le site du ministère de la justice américain : https://www.justice.gov/opcl/privacy-act-1974.

[201] Art. 45 du RGPD

II) Des exceptions controversées, insérées dans l'accord

Comme vu précédemment, l'instauration d'une exception dans le Privacy Shield sur la collecte des données par les autorités américaines, est le point de départ de la fragilité de l'accord (A). Mais cette fragilité est également renforcée par la limitation du champ matériel de l'accord (B).

A) L'exception de collecte des données personnelles par les autorités américaines

Le paragraphe 5 de la rubrique « Vue d'ensemble » du Privacy Shield est sûrement celui donnant le plus de grain à moudre à ses détracteurs et à juste titre. En effet, ce dernier prévoit que le respect de ces principes peut être limité dans la mesure où la sécurité nationale, l'intérêt public, ou des exigences légales l'imposent. L'exception s'applique également dans le cas où le pouvoir règlementaire ou la jurisprudence créent des obligations ou accordent des pouvoirs explicites, conflictuels avec le Privacy Shield. Mais dans ce cas, l'organisation certifiée doit démontrer que sa non-conformité est cantonnée à la satisfaction d'une telle obligation.[202] Il est à noter que même si le Ministère de la Justice a apporté des clarifications quant à l'exception pour exigence légale, dans une lettre à la Commission, qui résume toutes les branches du droit américain dans lesquelles une telle exigence existe,[203] l'exception de sécurité nationale et d'intérêt public pose encore de vrais problèmes.

À la lecture de ce paragraphe, on comprend que ce n'est pas le corps du Privacy Shield qui risque de satisfaire aux exigences de la Cour de justice de l'Union européenne, puisque cette dernière avait en effet relevé que la protection adéquate ne pouvait pas être considérée comme existante si l'accord ne s'appliquait qu'aux entreprises américaines, sans que les autorités publiques américaines n'y soient soumises et que les exigences relevant de ce type d'exception instauraient la primauté des intérêts américains sur l'accord rendant de fait possible les ingérences dans les droits fondamentaux des personnes.[204] Cependant dans l'arrêt Schrems, la Cour laissait tout de même à la Commission l'opportunité de justifier dans le cadre d'un prochain accord, d'une protection juridique contre ces ingérences aux États-Unis,[205] mais

[202] Art. 5 des Principes de l'accord *EU-U.S Privacy Shield* publié par le Département du Commerce américain, section *Overview*.
[203] Lettre du secrétaire d'État américain à la justice au Commissaire à la protection des données V. Jourová du 19 février 2016.
[204] Communiqué de presse 117/15 de la Cour de Justice de l'Union européenne du 6 octobre 2015 sur l'affaire C-362/14.
[205] *Ibid.*

également aux Américains de clarifier leur position sur le sujet.[206] Mais tel que l'évolution de la législation américaine le montre, il semblerait que cette justification à une telle exception soit de plus en plus difficile à apporter. Preuve en est, la Commission dans le deuxième examen conjoint a préféré se concentrer sur le mécanisme d'Ombudsperson[207], qui semble désormais le seul recours à l'exception du paragraphe 5 faisant tenir le Privacy Shield debout malgré les faiblesses qui ont été exposées précédemment.[208]

Cette exception pose d'autant plus de problèmes qu'elle concerne des traitements qui devraient être détachés de ceux visés pour un but commercial. En effet, si de telles dérogations existent au sein d'un accord visant des traitements commerciaux, cela a tendance à brouiller la frontière entre ce qui relève du commerce et ce qui relève de la finalité de sécurité nationale.[209] Encore une fois, cela dépend de la finalité principale du traitement, visée par l'accord. En effet, la critique émise à l'encontre des juges européens dans l'affaire PNR était de ne pas avoir réussi à concilier les différentes finalités du traitement, en se bornant à ne reconnaître que la finalité de transfert de données aux autorités officielles, en omettant la finalité commerciale. Pour des raisons différentes, le Privacy Shield échoue également à concilier les deux finalités puisque pour le même traitement, selon que le destinataire soit l'entreprise ou une autorité publique, les règles peuvent très fortement différer. Quand bien même l'article 2 du RGPD dispose que le règlement ne s'applique pas dans le cas de traitements effectués : « par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. », dans le cas du Privacy Shield, les traitements sont effectués pour des finalités commerciales avant tout, et par conséquent ce dernier doit trouver à s'appliquer. Dès lors, la mesure d'exception ne semble pas justifiée sur le plan du droit européen.

Afin de trouver une solution, le G29 a longuement fait état de cette exception et a dégagé dans son avis d'avril 2016, avant que la Commission ne prenne la décision d'adéquation, quatre critères qui pourraient être de nature à autoriser une telle exception. En premier lieu, le traitement doit avoir une base légale claire, précise, et accessible, ce qui signifie que toute

[206] METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85 p. 3.
[207] Rapport COM(2018)860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* pp. 4 à 6.
[208] *Voir supra §1 sur les garanties appropriées insuffisantes.*
[209] CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p. 444.

personne doit pouvoir envisager comment et pourquoi les données seront traitées par les autorités après leur transfert par l'organisation certifiée. En deuxième lieu, le traitement doit être nécessaire et proportionné par rapport aux finalités légitimes poursuivies et un équilibre entre ces finalités et le respect des droits des personnes concernées doit être trouvé. En troisième lieu, un mécanisme de supervision indépendant, efficace et impartial doit être mis en place ; en l'occurrence, il s'agit évidemment du mécanisme de l'Ombudsperson. Enfin, des recours efficaces doivent être disponibles pour la personne et notamment concernant la défense des droits devant un organisme indépendant[210] ; rôle également assuré par l'Ombudsperson. Dès lors, on comprend l'acharnement de la Commission à faire en sorte de démontrer que ce dernier est bel et bien fiable et remplit les critères tirés de la jurisprudence Schrems.

En effet, les deux premiers critères établis font écho aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, proclamant respectivement le respect à la vie privée et familiale et la protection des données à caractère personnel.[211] En ce sens, chaque réexamen conjoint doit être l'occasion de vérifier l'évolution de la législation américaine puisque l'exception renvoyant nécessairement au droit américain, c'est sur ce dernier que l'examen au regard de la Charte doit porter. Cependant, il s'agit plutôt d'une constatation suivie de recommandations. Il n'y a pas de velléités de changement notables à la lecture des examens conjoints effectués jusqu'alors. En effet, la boîte de Pandore ayant déjà été ouverte par les Européens par la simple acceptation de l'exception, il n'y a finalement pas de fondements juridiques communs de nature à empêcher ces collectes et ces traitements par les autorités américaines.

Les deux derniers critères renvoient eux à l'article 47 de la même Charte. C'est le droit à un recours effectif et à accéder à un tribunal impartial. Il dispose que :

> « Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. Une aide juridictionnelle est accordée à ceux qui ne disposent

[210] Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du *EU–U.S. Privacy Shield*.
[211] Voir à ce titre les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice. »[212]

Depuis que le Privacy Shield est rentré en vigueur, c'est bien souvent sur cet article que l'évaluation de l'exception de sécurité nationale par le G29, puis le CEPD est effectuée et que les Européens se montrent les plus insistants, que ce soit la Commission ou le groupe dédié, instauré par la législation européenne. En effet, le mécanisme d'Ombudperson comme vu précédemment ne semblant pas remplir les conditions de l'article 47 ni les prérequis d'un tribunal au sens de la jurisprudence européenne.[213] Les critères conditionnant la tolérance à l'exception de collecte et de traitement des données personnelles par les autorités américaines pour des raisons de sécurité nationale notamment, ne seraient pas entièrement satisfaits, et il est fréquemment demandé aux Américains d'apporter plus de garanties et de transparence.[214]

Il en résulte donc pour l'heure, malgré quelques fausses intimidations émanant de la Commission à l'image de la commissaire Vera Jourova, à l'été 2018, qui menaçait les États-Unis de la suspension de l'accord tout en précisant ne pas vouloir en arriver à de telles extrémités,[215] que l'exception dont la doctrine a soulevé le problème dès le point de départ de l'accord,[216] n'a pas encore été de nature à compromettre l'accord.

À ce point du développement, il semble important de préciser que tous les acteurs du Privacy Shield sont au fait des tenants et des aboutissants découlant de cette exception et cela dépasse de loin les simples considérations juridiques. En effet, il semble évident qu'au regard de cette exception et de la loi américaine, la collecte et les traitements massifs par les autorités américaines ne sont pas empêchés, alors que c'est bien sur cette base que le Safe Harbor a connu son « triste » sort. De même, il est évident que les Américains font tout pour que l'Ombudsperson ne fonctionne pas de manière optimale, mais remplisse le strict minimum requis et que le PCLOB soit cantonné à un rôle politique dans le cadre du Privacy Shield, en

---

[212] Art. 7 de la Charte des droits fondamentaux de l'Union européenne.
[213] CJCE, *Affaire C-24/92* du 30 mars 1993, Pierre Corbiau c/ Administration des contributions ; CJCE, *Affaire C-506/04* du 19 septembre 2006, Graham J. Wilson c/ Ordre des avocats du barreau de Luxembourg.
[214] Rapport COM(2018)860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le deuxième examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield*.
[215] LAUSSON (J.), « Privacy Shield : la Commission européenne met en garde les États-Unis », www.numerama.com, publié le 31 juillet 2018. https://www.numerama.com/politique/402402-privacy-shield-la-commission-europeenne-met-en-garde-les-etats-unis.html
[216] Voir les articles suivants : METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85 ; CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p. 444.

témoigne l'agitation autour de la nomination d'un ultime membre permettant de remplir le quorum requis juste avant le réexamen conjoint de 2018.[217]

Si cette exception permet très probablement aux autorités américaines de continuer à traiter beaucoup de données de citoyens européens, c'est également rendu possible par la limitation assez importante du champ matériel du Privacy Shield.

B) La limitation du champ matériel du Privacy Shield : Une aubaine pour les autorités américaines.

Le Privacy Shield est un accord au champ d'application matériel limité, voire trop limité. Ayant été négocié comme son prédécesseur à des fins de libre circulation des données personnelles transatlantiques dans un cadre commercial, l'accord est cantonné aux entreprises ayant une activité commerciale de fourniture de biens ou de services et qui relèvent de la compétence de la FTC ou du Département des transports américains,[218] qui se sont engagés dans le cadre du Privacy Shield. D'emblée, il existe donc un flou sur les conditions de participation des différentes agences fédérales américaines au Privacy Shield puisqu'il est plusieurs fois mentionné que les organisations certifiées doivent rendre des comptes à la FTC, au Département du transport ou à d'autres agences dotées de pouvoirs similaires.[219] On en déduit donc que les agences doivent s'engager explicitement envers la Commission européenne.

Sans rentrer dans les détails du droit américain, la règlementation sur la protection des données personnelles est sectorielle et à ce titre on la retrouve notamment en matière de droit de la consommation, au titre de la régulation sur les pratiques commerciales déloyales et trompeuses, prévue dans le FTC Act.[220] La FTC se considère d'ailleurs comme le « Cop on the Privacy Beat » en référence à son large champ d'action sur les violations à la vie privée.[221] Cette compétence a d'ailleurs été rappelée et élargie en 2015 puisque dans une affaire *FTC c.*

---

[217] BRACY (J.), « Senate confirms PCLOB members ahead of Privacy Shield second-annual review », www.iapp.org, publié le 12 octobre 2018.
https://iapp.org/news/a/senate-confirms-three-pclob-members-ahead-of-privacy-shield-second-annual-review/
[218] CNIL « Le Privacy Shield », www.cnil.fr, publié le 24 mai 2017.
www.cnil.fr/fr/le-privacy-shield
[219] Lettre du Secrétaire américain au commerce au Commissaire à la protection des données V. Jourová du 7 juillet 2016.
[220] Art 45a. U.S.C, titre 15.
[221] PAHL (T.), « Your cop on the privacy beat », www.ftc.gov, publié le 20 Avril 2017.
https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat

Wyndham[222], la Cour d'appel pour le troisième circuit a donné raison à la FTC de condamner la société *Wyndham* pour violation de données personnelles de leurs clients à la suite d'une cyberattaque dirigée contre elle.[223] Pour cette raison, les organisations certifiées au titre du Privacy Shield exerçant une activité rentrant dans son champ de compétence sont sous son contrôle et par conséquent, celles ne respectant pas l'accord sont susceptibles de s'exposer aux sanctions prévues au titre des pratiques commerciales déloyales et trompeuses.

Cependant, certains types d'activités commerciales, notamment celles des banques, des compagnies aériennes, des compagnies d'assurance, des services de télécommunications et des organisations à but non lucratif, qui ne génèrent pas de profit[224] sont exclus de sa compétence par le FTC Act, comme il est rappelé dans une lettre de la FTC à la Commission.[225]

Il faut noter que parmi ces exceptions, une seule rentre tout de même dans le cadre du Privacy Shield. C'est celle concernant les activités commerciales de compagnies aériennes. Même si la FTC n'est théoriquement pas compétente, des règles sectorielles sont prévues pour les activités de transport par les airs, et notamment la section 41712 du titre 49 de l'U.S Code calque son modèle des pratiques déloyales et trompeuses sur celui du FTC Act.[226] Or, toujours selon la même base légale, c'est le Département du transport américain qui détient les pouvoirs d'investigation et de sanction en la matière.[227] En pratique, c'est à l'agence qui y est rattachée, l'« Office of Aviation Enforcement and Proceedings » (OAEP), que sont délégués ces pouvoirs.[228] Cela signifie donc que les compagnies aériennes autocertifiées au titre du Privacy Shield peuvent être poursuivies sous la section 41712 en cas de manquements aux principes de l'accord.

Il en résulte que les services de renseignements voulant collecter des informations auprès de ces organisations sur la base de l'exception de sécurité nationale doivent se conformer aux maigres exigences au titre de l'accord.[229] Même si l'on peut très fortement douter de

---

[222] United States Court of appeals, third circuit, *Affaire 799 F.3d 236 (3d Cir. 2015)* du 25 août 2015, FTC v. Wyndham Worldwide Corp.
[223] ANGELA, « La sécurisation des données personnelles aux États-Unis : la FTC s'immisce dans le débat », www.avocat-transatlantique.com, publié le 29 Novembre 2015. https://www.avocat-transatlantique.com/2015/11/securisation-donnees-personnelles-etats-unis-ftc-simmisce-debat/
[224] Art 45a. U.S.C, titre 15.
[225] Lettre de la FTC au Commissaire à la protection des données V. Jourová du 7 juillet 2016.
[226] Art. 41712 U.S. Code, titre 49.
[227] *Ibid.*
[228] Statement on Privacy, Office of Aviation Enforcement and Proceedings, www.transportation.gov. https://www.transportation.gov/sites/dot.gov/files/docs/Statement%20on%20privacy%20page%20OAEP.pdf
[229] *Voir supra.*

l'efficacité des garde-fous à l'exception de sécurité nationale au titre du Privacy Shield, ils ont au moins le mérite d'imposer aux Américains de rendre des comptes lors des examens annuels conjoints. A contrario, cela signifie que sur les traitements par les autorités publiques dont la collecte est effectuée auprès d'entreprises échappant au cadre du Privacy Shield, ils sont entièrement libres de procéder de la manière qu'ils décident.

Par exemple, les activités de télécommunications sont régies aux États-Unis par le Telecommunications Act de 1996. Ce texte avait en premier lieu pour but d'ouvrir le secteur des télécommunications à la concurrence afin de doper son développement. Les acteurs exerçant une activité sous l'égide de ce texte sont sous le contrôle de la Federal Communication Commission (FCC). [230] Ce texte prévoit bien des mesures de protection des données des utilisateurs de services de télécommunications. En effet, la section 222 de l'Act prévoit que tout opérateur de télécommunications a le devoir de protéger la confidentialité des données privées du consommateur sous réserve d'exceptions.[231] On aurait pu alors espérer que le Privacy Shield puisse également couvrir le domaine des télécommunications étant donné le développement exponentiel de ce dernier[232], dont les services de contenus numériques nécessairement attachés sont certainement les plus datavores. Cependant, il semblerait que ce qui conditionne le parapluie du Privacy Shield soit les engagements pris directement par les agences fédérales en charge de faire respecter la législation. La conséquence est que tous les traitements de données sur les citoyens européens effectués par des opérateurs américains de télécommunications échappent à toute protection. C'est d'autant plus vrai qu'en 2017, Trump a abrogé les règles de la FCC en matière de vie privée et interdit pour le futur à la FCC, de prendre des mesures similaires.[233] Donc, on se retrouve dans une situation dans laquelle les autorités américaines peuvent continuer à collecter les données notamment téléphoniques des Européens en toute impunité. Pour rappel, les scandales Snowden avaient débuté par la révélation selon laquelle la NSA collectait les enregistrements téléphoniques des clients de l'opérateur Verizon, sur une base journalière.[234]

---

[230] *Telecommunications Act* de 1996, www.fcc.gov
https://www.fcc.gov/general/telecommunications-act-1996
[231] Section 222, *Telecommunications Act* de 1996.
[232] CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n°10, Octobre 2016 p. 444.
[233] FUNG (B.), « Trump has signed repeal of the FCC privacy rules. Here's what happen next », www.washingtonpost.com, publié le 4 avril 2017.
https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.5c893c7065ab
[234] GREENWALD (G), « NSA collecting phone records of millions of Verizon customers daily », www.theguardian.com, publié le 6 juin 2013.

De la même façon, en matière d'activité bancaire, le journal Der Spiegel révélait en 2013 que la NSA avait également surveillé les transactions financières mondiales par le biais de la société SWIFT qui assure la transmission des données bancaires entre quelque 8000 établissements bancaires[235] et en 2017, des hackers publiaient des documents révélant que la NSA continuait à surveiller les transferts bancaires mondiaux par le même biais.[236]

Le secteur des télécommunications et le secteur bancaire représentent sûrement à eux deux, une part importante de la transmission de données personnelles mondiale et par déduction entre les États-Unis et l'Union européenne. À titre d'illustration, on estime le nombre de paiements électroniques en 2020, à plus de 700 milliards, et l'évolution technologique et le développement des services de télécommunications y sont pour beaucoup.[237]

Énormément de traitements de données personnelles par les autorités américaines risquent donc de passer au travers de toute protection. En effet, l'exception de sécurité nationale large, appuyée par une législation laxiste ainsi que des pans entiers concernant la collecte et le traitement de données personnelles complètement exclus du Privacy Shield posent nécessairement la question de son efficacité au regard du droit. Force est de constater qu'il n'est pas de nature à inquiéter les autorités de renseignement américaines dans la collecte et le traitement des données.

https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[235] SANGARE (M.), « La NSA a aussi surveillé les transactions financières mondiales », www.mediapart.fr, publié le 17 septembre 2013.
https://blogs.mediapart.fr/mohamed-sangare/blog/170913/la-nsa-aussi-surveille-les-transactions-financieres-mondiales

[236] BALDWIN (C.), « Hackers release files indicating NSA monitored global bank transfers », www.reuters.com, publié le 14 Avril 2017.
https://www.reuters.com/article/us-usa-cyber-swift-idUSKBN17G1HC

[237] CBanque avec AFP, « Plus de 700 milliards de paiements électroniques dans le monde en 2020 », www.cbanque.com, publié le 9 octobre 2017.
https://www.cbanque.com/banque/actualites/64681/plus-de-700-milliards-de-paiements-electroniques-dans-le-monde-en-2020

Section 2 : Des carences dans l'application du Privacy Shield au niveau américain

On peut dégager deux catégories de carence. La première carence porte sur le contrôle des autorités américaines sur les entreprises américaines autocertifiées (I). La deuxième carence porte sur les stratégies de contournement de l'accord (II).

I) Un contrôle carencé sur les entreprises américaines autocertifiées

Même si le contrôle et la supervision se sont améliorés du côté des Américains depuis la mise en place de l'accord, il reste certaines carences lors des deux premiers exercices comme en témoignent les rapports annuels conjoints (A). Le contrôle carencé a éclaté au grand jour dans le cadre de l'affaire Cambridge Analytica (B).

A) Des carences dans le contrôle et la supervision des entreprises autocertifiées

Le contrôle et la supervision par les autorités américaines notamment sur les entreprises autocertifiées sont au cœur de l'application du Privacy Shield. Qui dit autocertification, dit confiance accordée aux organisations, mais cela signifie également que les autorités chargées de la bonne application des principes, que les entreprises se sont engagées à respecter, doivent exercer les prérogatives qui leurs sont confiées, afin de sanctionner les abus, mais également simplement surveiller le niveau de conformité globale dans le cadre du programme. Or, sur les deux dernières années d'exercice du Privacy Shield, les autorités américaines peinent parfois à convaincre les Européens de leurs engagements de contrôle et de supervision.[238] En effet, la première année, la Commission reprochait sous forme de recommandations au DoC, de ne se borner qu'à effectuer les vérifications sur les organisations en quête de la certification, mais d'appliquer une politique de « laisser-faire » par la suite.[239] Elle préconisait également la mise en place de questionnaires soumis aux organisations afin de s'assurer de la conformité, mais également de réclamer les rapports de conformité annuels mis à la charge des entreprises.[240] Pour rappel, ces derniers sont indépendants du processus de recertification annuel par l'entreprise, qui doit seulement mettre à jour toutes les informations, comme établi par les textes

[238] PÉPIN (G.), « Privacy Shield : un an plus tard, l'efficacité du bouclier européen reste difficile à mesurer », www.nextinpact.com, publié le 18 octobre 2017. https://www.nextinpact.com/news/105443-privacy-shield-an-plus-tard-efficacite-bouclier-europeen-reste-difficile-a-mesurer.htm

[239] Rapport COM(2017)611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* pp. 4 et 5.

[240] *Ibid.*

de l'accord.[241] Ils sont en principe facultatifs, mais dans une optique de détecter les problèmes de conformité au programme et de pouvoir apporter des solutions rapides et adaptées, il semble opportun que les autorités américaines les étudient au mieux. De plus, cela permettrait d'avoir une base interprétative dans la pratique du programme, afin d'émettre par la suite des lignes directrices à destination des organisations participantes, mais également de développer une politique d'interprétation commune avec les autorités européennes de manière à favoriser la coopération.

Selon le G29, c'est d'ailleurs ce mécanisme d'autocertification qui impose d'allouer des ressources suffisamment importantes afin de garantir un contrôle efficace sur les organisations certifiées. Mais il observe lors de la première année que les organisations ne dépendent finalement que des organismes indépendants de règlement des litiges sans de réels contrôles de la part du DoC.[242] Il observe également que le DoC laisse complètement de côté la compétence *ex officio* qui lui est dédiée. En effet, dans le cadre du Bouclier de protection, il est censé mener des vérifications de conformité auprès des organisations de manière aléatoire comme prévu au titre de la vérification.[243] Les États-Unis, d'après les rapports sur les travaux menés conjointement, justifie l'absence de contrôle par le DoC par l'absence de suspicion sur les organisations.[244] Cela signifie que le contrôle est subordonné à l'existence de soupçons quant à la conformité d'une organisation. Mais comment de tels soupçons peuvent-ils naître sans contrôle ? La réponse américaine semble en tout cas ne pas satisfaire les Européens qui attendent des autorités publiques en charge de la supervision de l'accord, un rôle proactif plutôt que la passivité dont ils ont fait preuve entre 2016 et 2017. En effet, le reproche n'est pas seulement adressé au DoC mais également à la FTC. Cette dernière n'a pas effectué de balayage de routine spécifique à la conformité au Privacy Shield, qu'elle conditionnait également à des suspicions en amont.[245]

Le G29 rappelle à ce titre que pour remplir les exigences des juges européens, les mécanismes de contrôle et de supervision doivent être efficaces[246] et cette efficacité doit nécessairement passer par un rôle proactif. Mais en dehors de cette passivité, le G29 pointe

[241] Art. 6 des Principes de l'accord *EU-U.S Privacy Shield*, section *Supplemental Principles*.
[242] Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du *EU – U.S. Privacy Shield* p. 10.
[243] Art. 7 des Principes de l'accord *EU-U.S Privacy Shield*, section *Supplemental Principles*.
[244] Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du *EU – U.S. Privacy Shield* p.10.
[245] *Ibid.*
[246] CJUE, *affaire C-362/14* du 6 octobre 2015, Maximillian Schrems c/ Data Protection Commissioner.

également le manque de rigueur de la part du DoC dans l'évaluation des politiques de conformité ayant lieu pendant la phase de certification, lesquelles devant nécessairement amener à plus de suspicions et donc à des contrôles *ex officio* plus fréquents par la suite.[247] D'ailleurs, il est notifié que le DoC dans le cadre de ces procédures ne fait pas de différence entre responsables de traitement et sous traitements[248] qui ont pourtant des obligations bien distinctes. À la fin de la première année, de nombreuses carences en matière de contrôle de la part des autorités américaines sont donc soulevées. La critique la plus importante concerne le fait qu'une fois qu'une organisation a passé le premier contrôle au titre de la certification, elle ne risque dans la pratique plus grand-chose, en cas de non-conformité, à cause du manque de vigilance des autorités américaines.

Cependant, une nette amélioration est visible lors du deuxième exercice. On peut d'ailleurs affirmer que le scandale Cambridge Analytica[249] y est pour quelque chose.

À la lecture du second rapport, on constate que beaucoup d'améliorations sont notées par la Commission. En effet, le DoC a par exemple mis en place des vérifications trimestrielles sur les organisations certifiées présentant le plus de suspicions de faire de fausses déclarations. De plus, il a également réglé le problème de la certification annoncée par les organisations tandis que la demande est encore pendante. Il est à noter également la mise en place de contrôles aléatoires sur plus de cent organisations certifiées.[250] Il a également transmis une cinquantaine de cas litigieux à la FTC afin que des actions soient prises conformément à son champ de compétence.

L'un n'allant pas sans l'autre, la Commission a également salué le travail de la FTC et sa démarche proactive de surveillance de conformité des organisations avec les principes découlant du Bouclier de protection.[251] Cette dernière a notamment envoyé des injonctions administratives à des fins de réclamation d'informations dans le cadre, on le suppose, d'investigations.[252] Cela reste de l'ordre de la supposition puisque la Commission n'explique pas pourquoi de telles injonctions ont été faites. Simples vérifications ou contrôles avérés ; on peut émettre l'hypothèse que ces injonctions soient un leurre destiné à montrer la bonne volonté

[247] Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du *EU – U.S. Privacy Shield* p.10
[248] *Ibid.*
[249] L'étude de l'affaire Cambridge Analytica sera traité au titre du B) suivant.
[250] Rapport COM(2018)860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le deuxième examen annuel relative au fonctionnement du *EU–U.S. Privacy Shield* p. 3.
[251] *Ibid.*
[252] *Ibid.*

des autorités américaines enquêtant parallèlement dans l'affaire Cambridge Analytica. En effet, si la Commission avait eu connaissance des raisons pour lesquelles de telles injonctions ont été émises, nul doute que cela aurait été notifié dans ce rapport. D'ailleurs, elle souligne le regret de ne pas avoir accès à de plus amples informations sur les investigations menées, ce qui est de nature à étayer cette thèse.[253]

Du côté de l'autorité de contrôle européenne à la protection des données personnelles, on peut s'étonner de la quasi-absence de critique sur le sujet. Depuis le début des négociations du Privacy Shield, le G29 a toujours été très critique vis-à-vis de l'accord, s'efforçant d'ailleurs à faire du droit et non de la politique, ce qui était appréciable pour contrebalancer le point de vue de la Commission toujours trop lissé et très politisé. Son prédécesseur instauré par le RGPD adopte une position ambivalente. Il reprend dans un premier temps les conclusions du G29 et salue les efforts faits du côté des autorités américaines en termes de contrôle et de supervision comme le fait la Commission, mais en détaillant point par point les actions concrètes qui ont été menées par le Département du Commerce américain.[254] Mais après avoir évoqué des efforts significatifs, le CEPD considère que tous les points listés constituent un bon point de départ, mais que ces contrôles et vérifications ne portent que sur la forme et pas sur le fond.[255] Alors que l'on s'attend à ce que l'autorité centrale européenne nous explique ce qui pourrait matérialiser des actions au fond en matière de contrôle, il n'en est rien. Le CEPD se borne à considérer qu'une attention particulière doit être apportée aux transferts ultérieurs, ces derniers étant un risque pour la protection des données s'ils sont à destination d'un État ne garantissant pas de protection suffisante, et qu'il faut par conséquent renforcer la surveillance sur la mise en œuvre pratique du principe de responsabilité sur ces transferts, faisant directement référence au scandale Cambridge Analytica. Le tout est accentué par le reproche fait au DoC de ne pas avoir utilisé son droit de demander une copie des clauses de « privacy provisions » des contrats de sous-traitance ; droit qui peut être tout à fait être considéré comme une action sur la forme et non sur le fond. On est donc en présence d'un reproche très abstrait sans solution ou recommandation proposées.

Concernant les actions de la FTC, le raisonnement semble plus solide puisque bien que saluant les actions menées, le CEPD considère ne pas être en mesure d'évaluer la surveillance et le contrôle de l'agence américaine, puisque cette dernière refuse de communiquer les détails

[253] *Ibid.*
[254] Rapport du Comité européen de la protection des données du 22 janvier 2019 sur le deuxième examen annuel conjoint du *EU – U.S. Privacy Shield*.
[255] *Ibid.*

quant à la manière de procéder dans le cadre des actions menées.[256] On peut tout de même regretter le fait que le CEPD ne fasse pas d'autres commentaires sur le manque de transparence de la FTC, ce qui, dans le cadre de l'affaire Cambridge Analytica, aurait été bienvenu.

D'ailleurs, ce scandale a encore une fois prouvé que les affaires font les changements. Il y a fort à parier que les améliorations entre 2017 et 2018 et fortement soulignés dans les rapports n'auraient pas eu lieu sans ces révélations. De même, le contenu des rapports eux-mêmes semble directement corrélé au scandale et à la résolution du Parlement de 2018 demandant la suspension de l'accord, si la protection adéquate n'était pas assurée au premier septembre 2018, tout en pointant le manque de contrôle et de supervision par les Américains.[257] Pour cela, cette affaire mérite que l'on s'y attarde, afin de mieux comprendre les limites du contrôle exercé au titre du Privacy Shield.

B) L'affaire Cambridge Analytica

Cambridge Analytica était une société britannique spécialisée dans l'analyse de données à grande échelle et le conseil en communication. Cette dernière dont le slogan est « Data drives all we do » se targuait de : *« changer les comportements grâce aux données »*. Elle utilisait pour cela des méthodes de psychométrie et de psychologie comportementale.[258] Elle vendait par exemple des outils d'influence comme Siphon, permettant d'analyser l'efficacité des publicités en ligne, Validity, un service de sondage d'opinion à grande échelle, Data Models, un inventaire regroupant des types d'électeurs et de consommateurs ou encore Custom Data Manipulation permettant la visualisation des centres d'intérêt du public étudié,[259] à des clients de tout horizon, des organisations gouvernementales ou non gouvernementales jusqu'aux entreprises privées.[260] L'entreprise connue pour influencer les processus démocratiques de leurs balbutiements jusqu'aux urnes,[261] a notamment vendu ses services de gestion de données en faveur de la

[256] *Ibid.*
[257] Proposition de résolution 2018/2645(RSP) du Parlement européen, du 26 juin 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis.
[258] AUDUREAU (W.), « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », www.lemonde.fr, publié le 22 mars 2018.
https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-cur-du-scandale-facebook_5274804_4408996.html
[259] *Ibid.*
[260] BARRAUD (B.), « Se souvenir de Cambridge Analytica », *la REM*, n°48, Automne 2018.
[261] Channel 4 News, « Cambridge Analytica Uncovered : Secret filming reveals election tricks », www.youtube.com, publié le 19 mars 2018.
https://www.youtube.com/watch?v=mpbeOCKZFfQ

campagne de Donald Trump en 2016, pour près de 6 millions de dollars et aurait également influencé la campagne en faveur du Brexit.[262]

Le 17 mars 2018, le journal britannique The Guardian révèle que 50 millions de profils Facebook ont été collectés pour le compte de l'entreprise Cambridge Analytica.[263] En effet, un analyste de données, Chris Wylie, ayant travaillé pour l'entreprise dans le cadre de la campagne de Donald Trump, alertait sur la collecte de millions de données issues de Facebook profitant d'une brèche dans l'accès aux données personnelles des utilisateurs, dans le but de programmer un logiciel permettant de prédire et d'influencer les votes des citoyens.[264]

La faille résultait notamment du laxisme de Facebook sur l'accès aux données de ses membres. S'il est acquis que Facebook, en contrepartie de sa gratuité, fonde son économie sur l'exploitation des données des utilisateurs, et la revente de ces dernières à des annonceurs, leur utilisation à des fins de propagande électorale par le biais de manipulation médiatique est différente.[265] C'est d'ailleurs dans le traitement massif des données (Big Data) à des fins politiques que le terme de *Datacratie* prend tout son sens.[266] En l'occurrence, la collecte était réalisée par le biais d'une application tierce se connectant à Facebook, *Thisisyourdigitallife*, ne consistant ni plus, ni moins, qu'en un test de personnalité développé par un professeur en psychologie de l'université de Cambridge, Aleksander Kogan via la société *Global Science Research*. Le test, présenté comme un exercice académique et proposé sur Facebook entre 2014 et 2015, était en réalité destiné à collecter les données des participants, ainsi que les données accessibles des contacts des participants. Au total, environ 87 millions d'utilisateurs du réseau social ont été exposés pour 270 000 personnes ayant effectivement répondu au questionnaire.[267] Lesdites données étaient ensuite revendues à Cambridge Analytica qui les utilisait à des fins de profilage politique.[268] Parmi les 87 millions d'utilisateurs concernés, 27 millions étaient

[262] AUDUREAU (W.), « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », www.lemonde.fr, publié le 22 mars 2018.
[263] CADWALLADR (C.), GRAHAM-HARRISON (E.), « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », www.theguardian.com, publié le 17 mars 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[264] *Ibid.*
[265] BARRAUD (B.), « Se souvenir de Cambridge Analytica », *la REM*, n°48, Automne 2018.
[266] *Ibid.*
[267] DEBET (A.), « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce électronique* n° 12, Décembre 2018, comm. 92, p. 2.
[268] MOURON (P.), « Pour ou contre la patrimonialité des données personnelles », *la REM*, n°46-47 Printemps - été 2018.

européens, ce qui pose nécessairement la question de l'application des principes européens en matière de protection des données personnelles.[269]

Tandis que l'affaire Cambridge Analytica soulève de très vives problématiques éthiques sur l'exercice de la démocratie, sur l'information politique du citoyen et plus généralement sur la manipulation médiatique à l'ère de l'utilisation massive des réseaux sociaux, elle pose également de vraies questions en matière de protection des données dans les flux transatlantiques. En effet, nous sommes ici en présence de deux sociétés ayant un siège européen et un siège aux États-Unis.[270] Cela signifie en premier lieu qu'elles sont soumises au droit européen à la protection des données personnelles et qu'elles sont susceptibles de transmettre des données personnelles aux États-Unis ; pour ce faire, Facebook est une organisation certifiée au titre du Privacy Shield, tandis que Cambridge Analytica, dissoute depuis, par le biais d'une procédure d'insolvabilité[271], était également certifiée.[272] Sur le fondement de la législation européenne d'abord, des auteurs ont constaté que de nombreuses dispositions de la directive de 95, que le RGPD a d'ailleurs renforcées, n'avaient pas été respectées. En effet, les utilisateurs n'étaient pas informés du transfert de leurs données à un tiers et la finalité de la collecte présentée comme étant la recherche scientifique, était trompeuse.[273] Il en résultait donc des violations sur les principes relatifs au traitement des données à caractère personnel, en ce que notamment, le traitement n'était ni licite, ni loyal et ni transparent, les données n'étaient pas collectées pour des finalités déterminées, explicites et légitimes et étaient bel et bien utilisées ultérieurement d'une manière incompatible avec les finalités annoncées. De plus, les données étant collectées de manière massive, le responsable de traitement ne respectait pas non plus l'adéquation, la pertinence et la limitation à ce qui est nécessaire au regard des finalités du traitement.[274] De la même façon, les contacts des utilisateurs, dont les données ont également été collectées, n'en ont été informés à aucun

[269] DELPECH (X.), « Un premier bilan décevant mais pas désespéré », *Juris association*, n°591, février 2019, p. 22.
[270] Facebook a son siège européen en Irlande et Cambridge Analytica initialement basé à Londres mais enregistrée dans l'état du Delaware ; Voir à ce titre : BARRAUD (B.), « Se souvenir de Cambridge Analytica », *la REM*, n°48, Automne 2018.
[271] AFP, « Après le scandale Facebook, Cambridge Analytica met la clé sous la porte », www.lemonde.fr, publié le 2 mai 2018.
[272] Voir à ce titre la liste des organisations dont la certification a expiré sur le site du Privacy Shield : https://www.privacyshield.gov/participant?id=a2zt00000008PdqAAE&contact=true#dispute-resolution-1.
[273] L'application et le questionnaire ont d'ailleurs été créés en dehors de toute étude scientifique officielle ; voir à ce titre, PÉPIN (G.), « Retour sur le scandale Cambridge Analytica et la (molle) réponse de Facebook », www.nextinpact.com, publié le 23 mars 2018.
https://www.nextinpact.com/news/106349-retour-sur-scandale-cambridge-analytica-et-molle-reponse-facebook.htm
[274] Art. 6 et et 7 de la Directive 95/46/ce ; Art. 5 et 6 du RGPD.

moment.[275] Il y a alors lieu de considérer que de très nombreuses dispositions du droit européen ont été violées. Par conséquent, on peut s'interroger sur le respect des principes du Privacy Shield et notamment le principe d'information de la personne concernée, le principe de choix, même si d'autres principes semblent également avoir été violés.[276]

Concernant Facebook, par le biais d'une notification de l'ICO infligeant une sanction de 500 000 livres au réseau social,[277] on apprend que, même si Facebook n'est pas le responsable de traitement, il est coupable d'avoir pu permettre un traitement illicite, réalisé par les véritables responsables de traitement. Il lui est également reproché de ne pas avoir mis en œuvre les mesures techniques et organisationnelles découlant du principe de sécurité des données personnelles européen.[278] D'autres bases légales sont invoquées afin de condamner Facebook, mais il ne sera pas fait ici état d'une liste exhaustive des griefs formulés à son égard. Il faut simplement noter qu'en sa qualité d'organisation certifiée au titre du Privacy Shield, les mêmes reproches peuvent être faits sur le non-respect des principes de l'accord.

Il faut dès lors souligner le manque de contrôle et de supervision des autorités américaines. En effet, l'affaire Cambridge Analytica est la cristallisation de toutes les remarques faites lors du premier examen conjoint par le G29, puisque les faits démontrent qu'à aucun moment des initiatives n'ont été prises par la FTC ou par le Ministère du commerce américain pour détecter d'éventuelles failles, notamment de la part du géant Facebook, au titre de l'accord. Pire encore, les autorités américaines justifiant l'absence de contrôle par l'absence de suspicions, il y avait des antécédents connus entre Facebook et la FTC notamment sur la conformité de la société au Safe Harbor.[279] En sus, dès 2015, le journal britannique « The Guardian » évoquait déjà l'origine douteuse des données exploitées par Cambridge Analytica ; Facebook avait alors demandé à la société de supprimer lesdites données collectées, ce qu'elle n'avait pas fait.[280]

---

[275] BARRAUD (B.), « Se souvenir de Cambridge Analytica », *la REM*, n°48, Automne 2018.
[276] *Voir supra sur le détail des principes.*
[277] ICO, « ICO issues maximum £500000 fine to Facebook for failing to protect user's personal information », www.ico.org.uk, publié le25 Octobre 2018.
[278] DEBET (A.), « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce électronique* n° 12, Décembre 2018, comm. 92, p. 4.
[279] SALINAS (S.), « Facebook Stock Slides After FTC Launches Probe of Data Scandal », www.cnbc.com, publié le 26 mars 2018.
https://www.cnbc.com/2018/03/26/ftc-confirms-facebook-data-breach-investigation.html
[280] PÉPIN (G.), « Retour sur le scandale Cambridge Analytica et la (molle) réponse de Facebook », www.nextinpact.com, publié le 23 mars 2018.
https://www.nextinpact.com/news/106349-retour-sur-scandale-cambridge-analytica-et-molle-reponse-facebook.htm

Outre-Atlantique, l'affaire a alors fait grand-bruit puisque c'est cette dernière qui a amené Mark Zuckerberg à témoigner devant le Congrès des États-Unis d'Amérique. En effet, juste après les révélations médiatiques, la procureure générale du Massachusetts avait promis une enquête à laquelle le procureur général de New York s'était joint.[281] De plus, la FTC avait également décidé d'ouvrir une enquête au titre de la prohibition des pratiques commerciales déloyales ou trompeuses envers des consommateurs.[282]

C'est la suite logique d'une première investigation faite en 2011 quand Facebook avait effectué des changements sur son site internet qui étaient contradictoires par rapport à ce qui avait été communiqué aux utilisateurs. En effet, même si les utilisateurs pouvaient dans les paramètres de vie privée, ne choisir de partager des informations qu'à leurs contacts, lesdites informations étaient quand même partagées à des tiers. De la même façon, les informations étaient toujours accessibles après qu'un utilisateur ait supprimé son compte. La FTC était également arrivée à la conclusion que Facebook ne respectait pas ses obligations au titre du Safe Harbor.[283]

Dans l'affaire Cambridge Analytica, la question se posait alors de savoir si les pratiques de Facebook rentraient dans le champ du décret de la FTC consenti par Facebook en 2011, l'exposant à des pénalités de 40 000 dollars par violation,[284] et de facto de savoir si le respect du Bouclier de protection était assuré. On comprend dès lors pourquoi la FTC et le DoC se sont montrés plus virulents dans le contrôle et la supervision sur les organisations dans le cadre de l'accord, après coup.

C'est pour toutes ces raisons tant légales que politiques, que l'on constate un changement radical de comportement de l'administration américaine dans la deuxième année d'exercice du Privacy Shield. Encore une fois, cette affaire nous rappelle que les États-Unis ne prévoient pas une protection suffisante des données personnelles et de la vie privée, tandis que ces problématiques deviennent de plus en plus importantes pour les consommateurs.[285] Ce n'est que parce que les autorités américaines sont de plus en plus conscientes de ces enjeux (notamment illustrée par l'audition de Mark Zuckerberg devant le Congrès et le manque de

[281] *Ibid*.
[282] Art. 45 U.S.C, titre 15.
[283] HOUSER A. (K.), VOSS W. (G.), « The End of Google and Facebook Or a New Paradigm in Data Privacy », *Richmond Journal of Law & Technology*, volume 25, issue 1, 2018, p. 47.
[284] SALINAS (S.), « Facebook Stock Slides After FTC Launches Probe of Data Scandal », www.cnbc.com, publié le 26 mars 2018.
https://www.cnbc.com/2018/03/26/ftc-confirms-facebook-data-breach-investigation.html
[285] Congrès n° 115, Senate Committee on the Judiciary & Senate Committee on Commerce, Science and Transportation, du 10 avril 2018 sur le sujet : *Facebook, Social Media Privacy, and the Use and Abuse of Data*.

maîtrise du sujet par les sénateurs), que le contrôle et la supervision évoluent dans le cadre du Privacy Shield. Cependant, les différents scandales et notamment l'affaire Snowden ont montré que la réaction est temporaire, jusqu'à ce que l'affaire retombe, et à l'heure actuelle, on est en droit de se demander si les réactions américaines ne sont pas qu'un simple feu de paille. Toujours est-il que la FTC doit durcir son contrôle au regard du droit américain en matière de protection des données personnelles. Logiquement, cela devrait avoir des répercussions directes sur l'application qu'elle fait du bouclier de protection ou du moins sur l'application qu'elle annonce lors des examens annuels conjoints, puisqu'elle manque clairement de transparence sur les procédures d'application, ce qui lui avait valu des reproches de la part du CEPD. Finalement, le dénominateur commun entre l'application du Privacy Shield et l'affaire Cambridge Analytica pourrait être résumé par la phrase de l'ancien dirigeant de l'entreprise britannique, Alexander Nix, filmé à son insu : « Il y a des choses qui n'ont pas nécessairement besoin d'être vraies, du moment qu'elles sont crues. »

II) Les stratégies de contournement de l'accord

Les Américains ont démontré leur capacité à contourner l'accord du Privacy Shield. Ils l'ont fait par exemple en adaptant la territorialité des données à leur avantage dans l'affaire Microsoft c. USA par l'adoption du Cloud Act (A), mais également en organisant le contournement des règles européennes par l'accord PNR (B).

A) Territorialité(s) des données dans l'affaire *Microsoft c. USA et Cloud Act*

L'affaire est relativement simple dans les faits. Le Département de la Justice, dans le cadre d'une enquête en matière de stupéfiants, réclamait en 2013 la copie de plusieurs e-mails d'utilisateurs de Microsoft à la firme californienne.[286] À cette fin, un mandat a été émis par les autorités américaines afin de contraindre l'entreprise à livrer ces données personnelles.[287]

Bien qu'il soit monnaie courante que des pièces numériques soient exigées dans le cadre d'une enquête pénale, il s'agit tout de même de respecter certaines règles notamment des règles de territorialité de la loi sur laquelle on se fonde. Le gouvernement dans cette affaire se base

[286] REES (M.), « Une étude dresse les enjeux, problèmes et dommages collatéraux de l'affaire Microsoft Ireland », www.nextinpact.com, publié le 07 décembre 2017.
https://www.nextinpact.com/news/105782-une-etude-dresse-lesenjeux-problemes-et-dommages-collateraux-laffaire-microsoft-ireland.htm
[287] MATSAKIS (L.), « Microsoft Supreme Court case has big implications for data », www.wired.com, publié le 27 février 2018.
https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/

sur le Stored Communication Act de 1986. Cette loi encadre la révélation des communications électroniques qui sont stockées par les tiers fournissant un service de communication électronique.[288] Elle prévoit notamment un cadre juridique, en cas d'investigations de la part du gouvernement américain, sur l'accès aux communications électroniques visées. La jurisprudence est venue étoffer le texte puisqu'elle a par exemple jugé que l'utilisation du SCA était inconstitutionnelle en violation du quatrième amendement de la constitution américaine, en ce qu'il autorisait le Gouvernement à obtenir les communications électroniques privées comme des emails sans mandat.[289] Cependant, des zones floues demeuraient quant à son utilisation, afin de récupérer des données stockées hors du territoire américain en raison de la territorialité de la loi. C'est d'ailleurs sur cette base que la firme de Redmond, CA, fonde son argumentaire. En effet, les communications ciblées par le mandat sont, selon Microsoft, stockées en Irlande et l'entreprise considère que la section 2703 du SCA ne couvre pas ce genre de situation extraterritoriale.[290] Si aux États-Unis, la question qui se pose devant les tribunaux se trouve au niveau de l'adaptation du texte de loi aux évolutions d'un monde interconnecté,[291] la problématique plus générale se situe sur la territorialité de la donnée et de facto sur le cadre juridique qui s'y applique. L'affaire a cristallisé l'affrontement de deux théories sur la territorialité de la donnée. La première théorie soutenue par le Ministère de la Justice américain est le lieu de l'accessibilité de la donnée. Il s'agit d'avancer l'argument, selon lequel peu importe que la donnée soit située sur le territoire d'un autre pays, c'est le lieu du siège social de la société qui permet l'accessibilité à la donnée et qui doit être pris en compte.[292] Il s'agit d'ailleurs ici de scinder l'argumentation en deux parties : la première partie étant que le transfert a bien lieu, mais que la territorialité de la donnée est présumée exister sur le territoire des États-Unis, ce qui exclut de facto une localisation physique à proprement parler ; la deuxième partie étant que la divulgation des communications aux autorités américaines se fait uniquement après que la donnée soit sur le sol américain, afin de parer tout problème quant à une potentielle application extraterritoriale de la loi nationale américaine matérialisée par le SCA.[293] La

[288] Art. 2701 et seq. U.S.C. titre 18.
[289] United States, Court of Appeals, sixth circuit, *Affaire 631 F.3d 266 (6th Cir. 2010)* du 14 decembre 2010, U.S. v. Warshak.
[290] GILLASPIE (A.), « Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law », *University of Kansas Law Review*, volume 66, 2017, pp. 459 à 483, p. 472.
[291] DASKAL (J.), « Microsoft Ireland, The Cloud Act, and International Lawmaking 2.0 », *Stanford Law Review Online*, volume 71, Mai 2018, pp. 9 à 16, p. 9.
[292] CHRISTAKIS (T.), « Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques Avis Juridique sur l'affaire Microsoft Ireland (Cour Suprême des Etats-Unis) », *livre blanc CEIS et The Chertoff Group*, décembre 2017. p. 22.
[293] *Ibid.* p. 22.

deuxième théorie, celle défendue par le géant américain Microsoft, est celle qui promeut la localisation physique de la donnée et de fait la non-accessibilité de la donnée par un mandat émanant des autorités américaines du fait de ses caractéristiques au regard de la loi américaine.[294]

En première instance cependant, le juge américain considère que même si le centre de données n'est pas établi sur le sol des États-Unis, il y a lieu de considérer que Microsoft en est le propriétaire et en a le plein contrôle sans qu'il faille se poser la question de la localisation de la donnée physique.[295] C'est donc bien la thèse défendue par le gouvernement qui se voit privilégiée puisque la jurisprudence américaine dans plusieurs affaires a considéré sans plus d'égard que lorsqu'un mandat est issu, la personne concernée doit fournir toute information qui est sous son contrôle.[296] Dans cette affaire, le juge considère que ce type de mandat n'implique pas le déploiement de la loi américaine dans le sens physique du terme.[297] Dès lors, on comprend vite que tant que le contrôle de ladite donnée peut s'exercer sur le territoire américain, l'extra-territorialité n'est pas reconnue. La question est dès lors la suivante : comment imaginer une articulation de ce type de législation avec le Privacy Shield puisque ce dernier est par essence basé sur l'existence de la localisation physique de la donnée. De facto, faire une application extraterritoriale de la loi américaine revient à contourner les dispositions prévues par le Bouclier et les maigres garanties données aux Européens concernant les exceptions prévues. Heureusement, pour les Européens, la réponse est apportée en appel puisque les juges infirment la décision du premier jugement.

Parmi les documents soumis aux juges en appel de Manhattan par Microsoft, l'un des éléments importants ayant fortement influencé la décision de la Cour est un *Amicus Curiae* rédigé par un comité d'informaticiens et de scientifiques ayant démontré que la donnée a bien un lieu de stockage physique. En effet, la deuxième partie du développement souligne que :

---

[294] GILLASPIE (A.), « Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law », *University of Kansas Law Review*, volume 66, 2017, pp. 459 à 483, p. 471.
[295] *Ibid.*
[296] United States Court of Appeals, second circuit, *Affaire 707 F.2d 663, 667 (2d Cir. 1983)* du 4 mai 1983, Marc Rich & Co., A.G. ; United States District Court, Southern District of New York, *Affaire 276 F.R.D. 143, 147-48 (S.D.N.Y. 2011)* du 25 juillet 2011, Tiffany (NJ) LLC v. Qi Andrew ; United States District Court, Southern District of New York, *Affaire 244 F.R.D. 179, 195 (S.D.N.Y. 2007)* du 30 janvier 2007, NTL, Inc. Securities Litigation ; United States District Court, Southern District of New York, *Affaire N.A., 584 F. Supp. 1080, 1085 (S.D.N.Y. 1984)* du 27 mars 1984, United States v. Chase Manhattan Bank.
[297] United States District Court, Southern District of New York, *Affaire 15 F. Supp. 3d 466 (S.D.N.Y. 2014)* du 25 avril 2014, Microsoft c/ United States.

« Ladite donnée est tout de même conservée via des médias de stockage physique traditionnels, typiquement sur des disques durs de serveurs au sein d'énormes "data centers" [...]. Le serveur de la donnée utilise alors son propre logiciel de structure de base de données qui a préalablement enregistré l'endroit où la donnée a été stockée auparavant dans le système d'organisation des fichiers pour déterminer quel fichier fait l'objet de la requête [...] Les données, telles que les e-mails, ont encore besoin d'être stockées sur des médias de stockage physique dans un ou plusieurs serveurs au sein d'un data center »[298]

Les juges rappellent dans un premier temps que la loi américaine doit être présumée d'application domestique uniquement, renvoyant à la jurisprudence de la Cour suprême[299] à défaut de prévoir une application extraterritoriale explicite ce que le SCA ne fait pas. La cour reconnaît ensuite que la localisation physique de la donnée soulève bien des problématiques d'extraterritorialité de la loi.[300] En effet, elle considère que pour récupérer les communications en cause, Microsoft doit dans tous les cas interagir avec Dublin que ce soit en les récupérant via ces systèmes intranet ou en se rendant physiquement en Irlande.[301] On peut d'ailleurs souligner l'intelligence des juges américains de ramener la problématique à des repères et à des contraintes physiques permettant de démontrer le caractère extraterritorial de l'application de la loi en le rattachant à des considérations un peu plus terre-à-terre. On comprend par le biais de cette décision qu'il est important de bien situer la localisation de la donnée au risque de créer des contournements à des accords internationaux par le biais de lois nationales. En l'espèce, au regard du Privacy Shield, la solution semble plus adaptée.

Le gouvernement après la décision de 2016, considérant que la décision d'appel représentait un coup contre la sécurité nationale, en appelait à la Cour Suprême afin de régler ce problème juridique et du même coup espérer une décision favorable.[302]

---

[298] WARRICK (P), « Brief for Amici Curiae computer and data science experts in support of appellant Microsoft Corporation », pour *l'affaire Microsoft corporation c/ United States of America*, publié le 15 décembre 2014.
[299] Supreme Court of the United States, *Affaire 561 U.S. 247 (2010)* du 24 juin 2010, Morrison v. National Australian Bank Ltd.
[300] GILLASPIE (A.), « Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law », *University of Kansas Law Review*, volume 66, 2017, pp. 459 à 483, p.474.
[301] United States Court of Appeals, second circuit, *Affaire 14-2985* du 14 juillet 2016, Microsoft vs. United States.
[302] DASKAL (J.), « Microsoft Ireland, The Cloud Act, and International Lawmaking 2.0 », *Stanford Law Review Online*, volume 71, Mai 2018, pp. 9 à 16.

Mais de décision de la Cour suprême sur le sujet, il n'y en aura probablement pas. En tout cas pas sur le fond de l'affaire, puisque dans une décision du 27 avril 2018, la Cour intime les parties à se référer à la loi promue par le Président Trump et rentrée en vigueur en mars 2018, venant amender le SCA.[303]

La loi en question n'est autre que le fameux « Claryfying Lawful Overseas Use of Data Act (CLOUD Act) qui a fait couler beaucoup d'encre. Ce texte est venu renforcer la loi déjà existante puisqu'il clarifie le fait que l'opérateur de services numériques doit communiquer aux autorités toutes les informations qu'il détient, dont il a la garde ou le contrôle, peu importe la localisation de la donnée, pourvu que l'autorité demanderesse soit munie d'un mandat à son encontre.[304] Dans les grandes lignes, ce sont les opérateurs qui se retrouvent entre deux feux puisque par exemple, l'article 48 du RGPD interdit ce genre de transferts.[305] Le Cloud Act crée un conflit de lois transatlantiques important. C'est pour cette raison qu'il prévoit une procédure de plainte pour les opérateurs à deux conditions : la première est que le client ou l'abonné dont les données sont concernées n'est pas un ressortissant américain et ne réside pas aux États-Unis. La deuxième est que la divulgation constitue un risque important de violation des lois par le fournisseur d'un autre État.[306] On a donc un garde-fou sous la forme de recours juridictionnel qui a le mérite d'exister, mais qui reste faible puisqu'il dépend des juridictions américaines, étant donné que c'est bien la validité du mandat qui sera étudiée. Avec le Cloud Act donc, c'est bien la localisation physique de la donnée qui est mise en cause et on peut s'interroger sur l'utilité du Privacy Shield pour réguler les exceptions qu'il prévoit. En effet, l'exception de conflit d'obligation et d'autorisation est bien prévue dans les textes, mais cette dernière est néanmoins subordonnée au « contrôle » par les Européens des pratiques américaines, les obligeant de fait à un peu de transparence. Mais le Cloud Act, qui a été pensé afin de contourner le RGPD, fait également fi des dispositions du Privacy Shield.

On peut se réconforter partiellement, puisque le Cloud Act prévoit explicitement que le Gouvernement américain peut conclure des accords bilatéraux avec des gouvernements étrangers même s'il n'est pas certain que ces derniers puissent être admis au regard du RGPD,[307]

---

[303] Supreme Court of the United States, *Affaire 584 U. S. (2018)* du 17 avril 2018, United States, Petitioner c. Microsoft Corporation, on writ of certiorari to the United States Court of Appeals for the second circuit.
[304] Art. 2713 U.S.C. titre 8.
[305] Art. 48 du RGPD.
[306] MISTRAL (J.P.), « Le Cloud Act, des questions et des réponses », www.village-justice.com, publié le 5 Février 2019.
https://www.village-justice.com/articles/cloud-act-des-questions-des-reponses,30601.html
[307] *Ibid.*

et des règles relatives aux transferts de données vers des pays tiers.[308] Une chose est sûre cependant, ces accords prendraient le pas sur le Bouclier de protection des données pour de tels transferts se fondant sur l'adage selon lequel : le droit spécial prime sur le droit général.

Il est cependant à craindre que ces accords soient à la faveur des États-Unis et qu'il en résulte des dérives comme dans le cadre de l'accord PNR.

B) L'accord PNR ou le contournement organisé des règles européennes

Le Privacy Shield est un accord qui encadre les traitements de données personnelles de nature commerciale. Par conséquent, tous les autres traitements se trouvent exclus du champ du Privacy Shield et nécessitent des aménagements juridiques particuliers afin qu'ils soient encadrés. Si précédemment il a été étudié des mécanismes de « by-pass » du côté états-uniens, il faut constater que certains traitements contournant par nature le Bouclier de protection sont tout de même soumis à des accords spécifiques entre les États-Unis et l'Union européenne soulevant également des problématiques qui leur sont propres. C'est le cas de l'accord PNR déjà évoqué.

Comme il a été étudié, cet accord PNR a fait couler beaucoup d'encre par le passé et continue à en faire couler. Pour rappel, PNR est l'acronyme pour *Passenger Name Record* qui désigne les données non vérifiées, fournies par les passagers aux compagnies aériennes lors des procédures de réservation et d'enregistrement.[309] Elles sont utilisées à des fins de renseignement sur les activités criminelles.[310] Le but d'un tel accord est pour les autorités américaines, de récupérer les données des Européens sur les vols transatlantiques, afin de les intégrer à leurs propres bases de données. Le premier accord a vu le jour en 2004 avant d'être annulé par la CJCE en 2006.

À la suite de la décision des juges européens invalidant l'accord PNR, un accord provisoire est trouvé le 19 octobre 2006. Si les juges européens avaient notamment justifié leur décision par l'incompétence de la Commission à prendre une décision d'adéquation validant le

[308] Art. 44 à 48 du RGPD.
[309] ANONYME, « Données personnelles des passagers aériens : accord entre les États-Unis et l'Europe », www.vie-publique.fr, publié le 9 mai 2012. https://www.vie-publique.fr/actualite/alaune/donnees-personnelles-passagers-aeriens-accord-entre-etats-unis-europe.html
[310] AUVRET-FINCK (J.), « L'échange d'information dans les accords PNR conclus par l'UE avec des États tiers », Colloque « l'échange des données dans l'espace de liberté, de sécurité et de justice de l'Union européenne », Grenoble, 17-18 novembre 2016.

texte[311], les craintes exprimées sur les mesures transitoires portaient bel et bien sur l'absence de garanties sur les droits fondamentaux des Européens, ainsi que sur un déséquilibre important en faveur des Américains inspiré par des méthodes de fonctionnement unilatéraliste comme pointé par un rapport de l'Assemblée nationale se prononçant sur le projet de décision du Conseil de l'Union européenne[312].

L'accord provisoire adopté pour une durée de sept années a finalement été remplacé par un accord permanent conclu le 8 décembre 2011 entre les autorités américaines et le Conseil de l'Union européenne et approuvé par le Parlement le 19 avril 2012.[313] Parmi les nouveautés de cet accord, on peut citer les maigres améliorations des garanties en matière de protection des données des Européens, comme des durées de conservation strictement établies ne pouvant pas dépasser dix ans ou encore des règles sur le transfert de données sensibles. En effet, en présence de données sensibles, ce sont les compagnies elles-mêmes qui envoient les données aux autorités américaines (méthode de « push »), ce qui se différencie d'un accès fourni aux autorités pour accéder au reste des données (« méthode du Pull).[314] Il est cependant à noter que des dérogations existent afin que les autorités américaines accèdent tout de même à des données par « Push ».[315] Cet accord prévoit également des recours administratifs et judiciaires et un droit de rectification auprès du ministère américain de la Sécurité intérieure si les informations sont inexactes.

Cependant, beaucoup d'interrogations préoccupent les esprits quant à sa compatibilité avec les exigences européennes relatives aux droits fondamentaux et par conséquent aux règles européennes en matière de protection des données personnelles. En 2017, l'AEDH pointait le fait que dans ses derniers rapports, la Commission rapportait des améliorations, mais ne les illustrait que très peu, ce qui montrait une certaine opacité de la part des différentes parties en présence. De la même manière, était souligné l'existence d'un mécanisme dérogatoire permettant au « Department of Homeland Security », d'obtenir plus d'informations que celles

[311] CJCE, *Affaires jointes C-317/04 et C-318/04* du 30 mai 2006, Parlement européen c/ Conseil de l'Union européenne
[312] Document E3575, Texte soumis en application de l'article 88-4 de la constitution par le Gouvernement à l'Assemblée nationale et au Sénat, déposé le 5 juillet 2007, distribué le 9 juillet 2007, www.assemblee-nationale.fr.
[313] ANONYME, « Données personnelles des passagers aériens : accord entre les États-Unis et l'Europe », www.vie-publique.fr, publié le 9 mai 2012. https://www.vie-publique.fr/actualite/alaune/donnees-personnelles-passagers-aeriens-accord-entre-etats-unis-europe.html
[314] Communiqué de presse du Parlement européen sur l'« Accord PNR avec les États-Unis : feu vert de la commission des libertés civiles » du 27 mars 2012.
[315] *Ibid.*

prévues à l'article 2 de l'accord. Cela signifie que par « Push », les autorités américaines peuvent récupérer les informations de passagers concernant des vols n'étant pas au départ ou à destination des États-Unis. De plus, la recrudescence d'agents américains ayant accès aux données laisse à penser que ces données normalement encadrées sont finalement assez facilement accessibles.[316] Si cela dénote certains manquements au respect des droits fondamentaux des citoyens européens, les acteurs européens et états-uniens devraient être prudents puisqu'en 2017, dans un avis du 26 juillet, la CJUE a considéré que l'accord PNR entre l'UE et le Canada ne pouvait pas être conclu en sa forme actuelle, car il constituait une ingérence trop forte dans le droit fondamental au respect de la vie privée.[317] En cas de procédure judiciaire, il y a dès lors un risque que la CJUE considère que l'accord PNR USA-UE ne respecte pas les droits fondamentaux des citoyens européens.

Comme le Privacy Shield, l'accord PNR américano-européen semble souffrir des mêmes lacunes juridiques causées par les mêmes volontés politiques. Il est donc nécessaire de se demander si la mise en place des accords d'encadrement n'a pas pour véritable finalité d'organiser le contournement, plutôt que de l'empêcher.

[316] AEDH, « PNR UE-USA : un bilan préoccupant », www.aedh.eu, publié le 6 mars 2017. http://www.aedh.eu/pnr-ue-usa-un-bilan-preoccupant/

[317] VALLAT (T.), « L'accord PNR prévu entre l'Union européenne et le Canada ne peut pas être conclu sous sa forme actuelle selon l'avis de la CJUE du 26 juillet 2017 », www. thierryvallatavocat.com, publié le 27 juillet 2017. http://www.thierryvallatavocat.com/2017/07/l-accord-pnr-prevu-entre-l-union-europeenne-et-le-canada-ne-peut-pas-etre-conclu-sous-sa-forme-actuelle-selon-l-avis-de-la-cjue-du-2

PARTIE 2 : Le Privacy Shield, un cadre dissimulant une approche politico économique

Si l'on passe outre les lacunes juridiques du Privacy Shield, il apparaît donc nécessaire de questionner sur sa véritable utilité. En effet, il n'apporte pas de cadre juridique révolutionnant la protection des données personnelles transatlantiques et se contente de poser des rustines là il est nécessaire d'en appliquer. Les intérêts du Privacy Shield sont par conséquent à chercher ailleurs que du point de vue du droit au sens strict.

Il est clair que l'accord a par exemple un intérêt économique non négligeable. Il permet la libre circulation des données personnelles entre les États-Unis et l'Union européenne (Chapitre 1), si tant est qu'une organisation se certifie. Mais on ne peut pas non plus occulter que le Privacy Shield s'inscrit dans une évolution de la protection des données aux États-Unis (Chapitre 2).

CHAPITRE I : La libre circulation des données personnelles grâce à un cadre juridique

Le Privacy Shield doit plutôt être assimilé à un cadre juridique qui facilite la libre circulation des données personnelles puisque cette dernière permet de satisfaire des intérêts transatlantiques distincts (section 1). De plus, ce dernier doit s'inscrire dans les évolutions technologiques ayant facilité cette libre circulation, comme le Big data et le Cloud Computing (section 2).

Section 1 : Libre circulation des données personnelles et intérêts transatlantiques distincts

Cette libre circulation nourrit des intérêts antagonistes. En effet, elle conditionne la pérennité des activités des structures américaines avec l'Europe (I). Mais son contrôle par le Privacy Shield joue également un rôle important dans la stratégie de développement de l'économie numérique (II)**.**

I) La pérennité des activités des structures américaines avec l'Europe

Il est certain que le Privacy Shield a pour vocation de permettre d'effectuer le plus de transferts possibles et d'assurer la pérennité des activités des structures américaines avec l'Europe, et à ce titre, on pourrait penser qu'il est destiné aux petites et moyennes entreprises (A). Cependant, il est surtout utilisé par de grosses structures (B).

A) Le Privacy Shield : un outil en apparence destiné aux petites et moyennes entreprises…

Pour rappel, il existe plusieurs solutions issues de la législation européenne pour que des organisations américaines puissent valablement transférer des données de l'Union européenne vers les États-Unis. On peut schématiquement considérer que les Bindings Corporate Rules (BCR) sont plutôt destinés aux entreprises multinationales transférant un grand nombre de données de manière régulière et fréquente, afin d'éviter notamment un formalisme trop lourd par la mise en place d'un code de conduite s'appliquant initialement à toutes les entités de l'organisation.[318] Cependant, le RGPD ayant officialisé les BCR,[319] il a également

[318] MAKSO (B.), « Exporting the Policy – International Data Transfer and the Role of Binding Corporate Rules for Ensuring Adequate Safeguards », *Pecs Journal of International & European Law*, volume 2016, 2016, p. 79
[319] Art. 46 et 47 du RGPD

étendu leur adoption, à des entreprises engagées dans une activité économique conjointe.[320] À l'autre extrême, les petites et moyennes organisations américaines qui ne transfèrent que peu de données personnelles depuis l'Europe, utilisent plutôt les clauses contractuelles types mises à la disposition par la Commission européenne, répondant aux garanties appropriées.[321] Ces clauses sont insérées dans les contrats par les responsables de traitements européens, lorsqu'ils transfèrent des données à une entité basée hors de l'Union européenne et vont mettre à sa charge des obligations contractuelles en matière de protection des données personnelles.[322]
Le problème de ces clauses est qu'elles doivent être insérées pour chaque contrat impliquant un traitement et sont différentes selon les acteurs en présence. En effet, la CNIL dispose sur son site internet de schémas évoquant tous les cas possibles pouvant nécessiter le recours à l'une de ces clauses types.[323] Il en résulte donc une complexité structurelle, ainsi qu'une multiplication de l'utilisation de cet outil. D'ailleurs, le Commissaire de la FTC avait déclaré en 2016, en appui des négociations sur le Privacy Shield, que ces clauses sont coûteuses, compliquées à mettre en œuvre et qu'elles ne sont pas appropriées pour tous les transferts de données.[324] En effet, elles ne permettent pas d'opérer des transferts de données de manière globale. Le côté pratique reste donc limité par le champ d'application des clauses contractuelles types, restreint à chaque traitement de données.[325]

C'est pour cette raison que selon les autorités officielles, les petites et moyennes entreprises américaines ont intérêt à se certifier au titre du Privacy Shield. En effet, la certification étant valable pour tous les transferts de données en provenance de l'Union européenne à destination d'une organisation américaine autocertifiée, cela permet de faire valoir auprès de partenaires européens une garantie juridique, sans passer par de nombreuses clauses contractuelles.[326] Dans ce sens, la Commission donne l'exemple d'un agent de voyage

[320] BOTCHORICHVILI (N.), « Transferts de données personnelles hors de l'Union européenne – Quelles nouveautés avec le RGPD », *Legicom* 2017/2, n°59, p. 1
[321] GRYNWAJC (S.), « GDPR : Surviving the likely demise of the Privacy Shield », www.transatlantic-lawyer.com, publié le 8 Juillet 2018.
https://www.transatlantic-lawyer.com/2018/07/surviving-the-likely-demise-of-the-privacy-shield/
[322] CNIL « Les clauses contractuelles types de la Commission européenne », www.cnil.fr, publié le 8 février 2016.
https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne
[323] *Ibid.*
[324] SEGALIS (B.), LINKSY (K.), « FTC Commissioner Julie Brill Comments on EUUS Privacy Shield », www.dataprotectionreport.com, publié le 4 Février 2016.
https://www.dataprotectionreport.com/2016/02/ftc-commissioner-julie-brill-comments-on-eu-us-privacy-shield/
[325] GRYNWAJC (S.), « GDPR : Surviving the likely demise of the Privacy Shield », www.transatlantic-lawyer.com, publié le 8 Juillet 2018.
https://www.transatlantic-lawyer.com/2018/07/surviving-the-likely-demise-of-the-privacy-shield/
[326] Pour rappel, les clauses contractuelles de la Commission sont valables sur des transferts concernant n'importe quel pays tiers.

européen qui transmettrait les données d'un client à un hôtel situé aux États-Unis et qui se serait enregistré au titre du Privacy Shield.[327]

Cela signifie qu'à partir du moment où la certification est validée, il peut y avoir autant de données transférées que nécessaire, avec autant de responsables de traitement situés sur le territoire de l'Union européenne. C'est donc un atout commercial non négligeable à faire valoir auprès de ces partenaires quand on sait que la transmission par voie électronique est en développement et que le volume de données envoyées augmente constamment. Il apparaît donc que le rôle du Privacy Shield peut s'apparenter à un outil peu coûteux et efficace renforçant la confiance entre les opérateurs économiques transatlantiques. En effet, il pourrait permettre de facto à des petites et moyennes entreprises américaines recevant beaucoup de données en provenance de l'Europe, mais n'ayant pas les moyens d'installer une filiale sur le territoire européen et d'instaurer des BCR, de continuer à échanger avec l'Europe.

Cependant, le Privacy Shield et son application restent encore trop flous pour convaincre les petites entreprises américaines de se certifier. En effet sans clarification légale, le bouclier de protection n'apporte pas un mécanisme fiable de transferts de données tant les incertitudes sur son avenir sont grandes.[328]

En termes de coût, l'adhésion au Privacy Shield n'est pas gratuite et le prix à payer augmente en fonction du chiffre d'affaires de l'organisation. Là encore, il y a la volonté que toute entreprise américaine puisse adhérer au bouclier de protection, puisque de 0 dollar à 5 millions de dollars de chiffre d'affaires, le tarif varie entre 250 dollars et 375 dollars, de 5 millions à 25 millions, il varie entre 650 dollars à 975 dollars. De plus, le palier maximum varie entre 3250 dollars et 4875 dollars pour une entreprise réalisant plus de 5 milliards de dollars de chiffre d'affaires.[329] Cependant, si on peut saluer la décision d'une augmentation graduelle du prix annuel en fonction de l'importance de l'organisation, on peut tout de même s'interroger sur la pertinence de cette dernière. En effet, elle ne renvoie pas à une réalité tangible de la situation des entreprises américaines. Il semble que la distorsion de prix ne soit pas trop importante entre une petite entreprise et une moyenne entreprise puisque la taille d'une entreprise aux États-Unis est calculée sur le revenu annuel et que les écarts de revenus servant

[327] Communiqué de Presse de la Commission européenne du 18 octobre 2017 sur : « EU-US. Privacy Shield : First review shows it works but implementation can be improved ».
[328] MCALLISTER (C.), « What about small businesses? The GDPR and its consequences for small U.S.-based companies? », *Brooklyn Journal of Corporate, Financial & Commercial Law*, volume 12, 1er septembre 2017, pp. 187 à 211, p. 199.
[329] FAQs – General, Q. How much will it cost to self-certify to the Privacy Shield, www. privacyshield.gov.

à graduer le tarif du Privacy Shield fassent fi des réalités économiques pratiques. Par exemple, selon Payscale, le revenu médian d'une petite entreprise aux États-Unis est d'environ 66 000 dollars et la majorité d'entre elles se situent entre 30 000 et 150 000 dollars.[330] Concernant la taille moyenne d'une entreprise, il n'y a pas de définition fédérale ; cela renvoie donc à des concepts universitaires avec par exemple l'« Ohio State University's National Center for the Middle Market », qui situe entre 10 millions et 1 milliard de dollars de chiffre d'affaires annuel une entreprise moyenne aux États-Unis.[331] À la vue de ces chiffres, comment justifier qu'une entreprise A ayant par exemple 15 000 dollars de chiffres d'affaires doit payer 250 dollars ce qui reste évidemment largement acceptable, mais qu'une entreprise B dégageant 25 millions de dollars ne paye que 975 dollars annuellement au titre de la certification. Il est dès lors difficile de justifier la graduation choisie, qui est loin d'être proportionnelle. D'aucuns argumenteront que l'outil du Privacy Shield reste tout de même accessible en termes de coûts pour toute entreprise qui voudrait se protéger juridiquement, quelle que soit sa taille, tout en développant son activité outre-Atlantique avec des partenaires européens, du moins en ce qui concerne le seul coût de la certification. En effet, ce coût ne tient pas compte des investissements humains, matériels et financiers, pour viser la conformité au Privacy Shield. Dès lors, les petites entreprises américaines notamment ne disposent pas de tels moyens afin de respecter les exigences de l'accord.[332] Là encore, du côté américain, les exigences européennes en matière de protection des données semblent freiner les ambitions de développement des entreprises américaines encore trop dépendantes de la libre circulation des données personnelles.[333]

Cependant, en pratique, même si l'outil était adapté à des petites et moyennes entreprises, ces dernières aux États-Unis n'échangent que rarement avec l'Union européenne à cause de leur taille, mais également de leur domaine d'activité, qui n'est pas propice à la collecte de données avec l'UE. Ainsi, en 2018, la plupart des petites entreprises créées aux États-Unis étaient destinées à des marchés locaux, comme la restauration ou la vente au détail.[334] Par

---

[330] Average Small Business Owner / Operator Salary, www.payscale.com
https://www.payscale.com/research/US/Job=Small_Business_Owner_%2F_Operator/Salary
[331] MERRITT (C.), « What Size Company Is Considered a Mid-Size Company », www.chron.com, mis à jour le 8 mars 2019.
https://smallbusiness.chron.com/size-company-considered-midsize-company-71776.html
[332] MCALLISTER (C.), « What about small businesses? The GDPR and its consequences for small U.S.-based companies? », *Brooklyn Journal of Corporate, Financial & Commercial Law*, volume 12, 1er septembre 2017, pp. 187 à 211, p. 200.
[333] *Ibid.*
[334] Current Small Business Trends and Statistics, 2019, www.guidantfinancial.com.
https://www.guidantfinancial.com/small-business-trends/

conséquent, parmi les entreprises certifiées, on retrouvera surtout des entreprises spécialisées dans les nouvelles technologies.

Malgré le fait que le Privacy Shield soit présenté comme un outil à destination de petites entreprises désirant développer leur activité outre-Atlantique, ces tendances sur l'état des petites entreprises notamment aux États-Unis et les caractéristiques rebutantes à la charge des organisations américaines, permettent d'expliquer que le Bouclier est surtout utilisé par de plus grosses structures.

B) … Mais surtout utilisé par de grosses structures

Si l'on parcourt la liste des entreprises actives adhérentes au Privacy Shield, le constat est le suivant. Toutes les grosses entreprises américaines du numérique comme Facebook ou Apple sont enregistrées. Mais si la liste du Privacy Shield regorge de multinationales américaines certifiées, il faut être prudent. En effet, il n'existe à ce jour aucune statistique émanant des instances européennes ou américaines sur les catégories d'entreprises certifiées, ou du moins ces dernières ne sont pas rendues publiques. On peut déplorer le fait qu'il soit impossible de mettre la main sur des études s'intéressant à la taille des entreprises certifiées ou bien au secteur d'activité concerné. Après de multiples sollicitations auprès des instances impliquées, nous nous sommes toujours vus refuser l'accès à toute information sur le sujet. Les instances européennes se contentent de renvoyer vers la Commission, qui elle-même conseille de s'adresser aux instances américaines responsables du Privacy Shield et ces dernières refusent catégoriquement.[335]

Cependant, une recherche manuelle des caractéristiques des entreprises présentes dans cette liste permet tout de même de dégager une tendance globale. Cette tendance révèle que les entreprises certifiées sont fréquemment des entreprises ayant un siège au sein de l'Union européenne ou des groupes bénéficiant de moyens financiers conséquents.[336]

L'utilisation du Privacy Shield est un outil de conformité au RGPD. En effet, une succursale européenne d'une entreprise américaine pour respecter la législation européenne doit s'assurer que la maison-mère à qui les données sont transférées permet bien de les recevoir. De la même manière, une entreprise américaine ayant la possibilité de s'implanter sur le marché

[335] Toutes les sollicitations faites auprès des instances concernées afin d'obtenir des informations dans un cadre universitaire, ont été refusées.
[336] En parcourant la liste, le constat est que beaucoup d'organisations certifiées font partie d'un réseau d'entreprises par exemple.

européen sait qu'elle devra respecter le droit des données personnelles communautaire. Cette conformité passe évidemment par le respect des règles en matière de transfert vers des pays tiers. Cette volonté de conformité au RGPD est d'ailleurs réelle et chiffrée puisque les 500 plus grandes entreprises américaines ont dépensé près de 8 milliards de dollars à partir de mai 2018 afin de s'assurer du respect de la loi européenne.[337]

En matière de transferts, si le Privacy Shield permet aux petites entreprises de trouver de nouveaux partenaires d'échange européens, il permet pour les grandes structures de fidéliser une clientèle afin de ne pas subir de mauvaises retombées économiques. Selon des études, les motivations des entreprises américaines de se mettre en conformité avec le RGPD naissent majoritairement de la volonté de satisfaire les attentes des clients en matière de protection des données et de la vie privée. Ainsi, 59 % des entreprises américaines affirment se mettre en conformité pour des raisons de fidélisation de la clientèle en répondant à leurs attentes, tandis que 41 % le font pour éviter les sanctions et les amendes.[338] Le Privacy Shield devant être considéré comme un outil de la conformité, il est tout à fait logique que ces entreprises américaines se certifient pour les mêmes raisons.

Une autre partie de la réponse sur le pourquoi les grandes entreprises se certifient au Privacy Shield, est peut-être à rechercher du côté du droit et des rapports de forces entre l'Union européenne et les États-Unis. Le 26 juin 2019, le rapport Gauvain pointe le caractère abusif des lois extraterritoriales américaines. Il démontre que les entreprises françaises souffrent notamment de la concurrence américaine puisqu'elles ne disposent pas d'outils juridiques efficaces pour se défendre contre les actions judiciaires extraterritoriales engagées contre elles.[339] Il est évident que l'application extraterritoriale de telles lois se fait pour favoriser les entreprises américaines au détriment de leurs concurrents puisque cela permet d'interférer dans la vie économique mondiale.[340]

En matière de données personnelles, le Cloud Act est par exemple explicitement cité dans l'accord. Par analogie, le Privacy Shield peut être perçu par les grandes entreprises américaines comme une opportunité de rester sous le parapluie des négociations

[337] ANONYME, « Global 500 companies to spend $7.8B on GDPR compliance », www.iapp.org, publié le 20 novembre 2017.
https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
[338] BECKER (M.), « GDPR Compliance: How it's Affecting U.S Companies », www.emarsys.com.
https://www.emarsys.com/resources/blog/gdpr-united-states-companies/
[339] Rapport du Député Raphaël Gauvain à M. le Premier Ministre Édouard Philippe du 26 juin 2019 sur « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriales ». p. 3.
[340] *Ibid.* p. 14.

transatlantiques qui continuent de cristalliser un rapport de force. Ainsi, il est avantageux de se certifier au Privacy Shield puisque l'on bénéficie de facto de négociations qui tendent le plus possible vers l'intérêt économique des structures américaines.

Quoi qu'il en soit, les Européens comptent également sur le Privacy Shield afin de développer l'économie numérique européenne.

II) Le rôle du Privacy Shield dans la stratégie de développement de l'économie numérique européenne

Du côté européen, on voit le bouclier de protection comme une opportunité d'exportation de l'économie numérique européenne (A), mais également comme une possibilité de restriction de l'économie numérique américaine (B).

A) Le Privacy Shield comme opportunité d'exportation de l'économie numérique européenne…

S'imposant comme la première puissance commerciale mondiale devant la Chine et les États-Unis, l'Union européenne a exporté en 2018, 406 milliards de biens avec son partenaire commercial privilégié : les États-Unis.[341] Plus encore, les accords de libre-échange transatlantiques se sont développés à l'image du TTIP et du TAFTA.[342] En matière de service, entre 2000 et 2014, les échanges entre l'UE et les États-Unis représentaient 31 % des échanges européens.[343] Cependant, le poids du numérique dans le PIB de l'UE est bien moindre que celui sur le PIB des États-Unis. En 2015, les technologies de l'information et de la communication représentaient 7,1 % du PIB américain, tandis qu'elles représentaient environ 4 % en Europe.[344] Cependant, le marché numérique européen n'est pas négligeable. Par exemple, rien que les données des citoyens européens pesaient près de 60 milliards d'euros en 2016 et devraient représenter 80 milliards d'euros en 2020. De plus, la valeur de l'économie européenne des données s'élevait à 300 milliards d'euros en 2016.[345] Le constat est donc que le marché existe et qu'il est prolifique. En revanche, le contrôle de ce dernier n'est pas assuré par des acteurs

---

[341] LEQUEUX (V.), « Le commerce extérieur de l'Union européenne », www.touteleurope.eu, publié le 14 Avril 2019.
https://www.touteleurope.eu/actualite/le-commerce-exterieur-de-l-union-europeenne.html
[342] *Ibid.*
[343] Infographie : échanges commerciaux Europe/États-Unis, *le Data Lab*, www.alternatives-economiques.fr.
[344] BONIS (P.), « L'internet européen : intérêts communs et acquis communautaires », *Annales des Mines – réalités industrielles*, n° 2016/3, Août 2016, pp. 19 à 23 p. 19.
[345] SEGOND (V.), « Des données personnelles très convoitées », www.lemonde.fr, publié le 29 mai 2017.
https://www.lemonde.fr/economie/article/2017/05/28/des-donnees-personnelles-tres-convoitees_5135092_3234.html

européens.[346] C'est une des raisons pour lesquelles le RGPD a été créé. Le règlement qui instaure un cadre autour de la libre circulation de ces données personnelles est une pierre à l'édifice du tant espéré « marché unique numérique ».[347] En effet, pour stimuler la compétitivité sur le marché mondial, il s'agit d'unir les forces européennes, puisque si la demande européenne représente 21 % du marché mondial en matière de numérique, les acteurs économiques ne représentent eux que 17 %.[348] Afin de booster cet écosystème numérique européen basé en grande partie sur le traitement de données personnelles, le véritable défi est de maintenir une protection élevée sur ce dernier, tout en restant compétitif. Mais force est de constater que ces intérêts ont fini par converger dans la stratégie européenne.[349] En effet, ainsi qu'il a déjà été soulevé par la doctrine, les dispositions relatives au champ d'application extraterritorial du RGPD ont apporté des moyens de résistance contre les GAFA, et aident au développement d'entreprises européennes du numérique, en régulant notamment le marché par la *Compliance*.[350] En effet, il s'agit de protéger les intérêts économiques de l'Union puisque le concept des géants de l'internet est très en avance aux États-Unis. Ces derniers représentent 10 % du chiffre d'affaires de l'économie numérique contre seulement 1 % en Europe[351] et aucune entreprise européenne ne fait partie des dix plus grandes capitalisations boursières mondiales qui font maintenant la part belle à ces très grosses entreprises du numérique.[352] Ces acteurs, qui sont parmi ceux qui brassent le plus de données personnelles à l'échelle mondiale, ne souffrent dès lors d'aucune véritable concurrence européenne au sein même du territoire communautaire. Si la Commission affiche très clairement son intention de favoriser les acteurs

---

[346] BONIS (P.), « L'internet européen : intérêts communs et acquis communautaires », *Annales des Mines – réalités industrielles*, n° 2016/3, Août 2016, pp. 19 à 23 p. 19.
[347] Communication COM(2015)192 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 6 mai 2015 sur la stratégie pour un marché unique numérique en Europe.
[348] BONIS (P.), « L'internet européen : intérêts communs et acquis communautaires », *Annales des Mines – réalités industrielles*, n° 2016/3, Août 2016, pp. 19 à 23 p. 19.
[349] Communication COM(2015)192 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 6 mai 2015 sur la stratégie pour un marché unique numérique en Europe.
[350] MONNERIE (N.), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, n°2018/4, volume 32 p. 444 ; FRISON-ROCHE (M.A), « Le droit de la compliance », *Recueil Dalloz* n°32, 29 septembre 2016, chronique p. 1871 ; PETIT (N.), « New Challenges for 21st Century Competition Authorities », *Working Paper*, 28 janvier 2013 ; ABA Section of Antitrust Law, « Antitrust Compliance: Perspectives and Resources for Corporate Counselors », *ABA Publishing*, Chicago, 2005, pp. 25-27 ; FRISON-ROCHE (M.A), « Le droit de la compliance au-delà du droit de la régulation », *Recueil Dalloz*, 2018, chronique. pp. 1561 et s.
[351] *Ibid.*
[352] AFALO (A.), « Apple, Amazon, Alphabet… les 10 entreprises les plus valorisées en bourse », www.leparisien.fr, publié le 3 août 2018.
http://www.leparisien.fr/economie/business/apple-amazon-facebook-les-10-entreprises-les-mieux-capitalisees-en-bourse-03-08-2018-7842417.php

européens,[353] il s'agit également de permettre leur développement hors de l'Union européenne. Or, l'invalidation du Safe Harbor a constitué une opportunité de renégocier les termes du contrat en matière de données personnelles avec les États-Unis qui était, du fait du rayonnement de l'affaire Snowden, en position de faiblesse. De plus, le RGPD a également pesé dans des négociations qui arrangent finalement bien les affaires des acteurs européens. En effet, le Privacy Shield imposant des obligations plus importantes que son prédécesseur, du moins sur le volet purement commercial, a un double impact favorable aux acteurs numériques européens voulant échanger avec les États-Unis. Le premier est qu'il verrouille le marché aux nouveaux entrants américains puisque pour pouvoir y pénétrer, il faut montrer patte blanche pour peu que l'on traite des données personnelles impliquant leur rapatriement sur le territoire américain. Pour décrocher des partenariats européens, l'adhésion au Privacy Shield reste le meilleur moyen de transférer un grand nombre de données pour ceux qui ne pourraient pas se prévaloir de BCR. Le deuxième est qu'il permet aux acteurs européens de s'assurer que les acteurs américains avec lesquels ils traiteront, pour peu qu'ils soient adhérents au Bouclier de protection, puissent recevoir les données faisant l'objet d'un transfert de manière légale. Cela exonère également de passer par les clauses contractuelles types qui, logique oblige, se retrouvent à la charge des entreprises européennes voulant transférer les données. En effet, ce sont les acteurs implantés sur le territoire de l'UE qui risquent la sanction, davantage que leurs partenaires potentiels situés aux États-Unis ; on peut donc considérer qu'il y a une inversion de la charge financière puisque dans un cas la mise en place de clauses contractuelles types, dans les contrats transatlantiques, sera à la charge des Européens, tandis que la certification au Privacy Shield sera à la charge des organisations américaines. Mais le plus important reste que la coopération est fondée sur une autorisation globale de transfert qui court pendant au moins un an après son émission par le Département du Commerce américain. Cela signifie qu'à partir du moment où les données sont transférées par un acteur européen à une organisation certifiée, l'acteur européen est certain de bénéficier de garanties vis-à-vis de son homologue américain sans qu'il soit besoin d'étudier la validité des clauses, par rapport à l'intégralité des traitements litigieux.

Un autre point primordial concerne la confiance des clients. Tandis qu'il est difficile de valoriser d'un point de vue mercatique des clauses contractuelles types, puisqu'elles sont par définition, rattachées à un contrat le plus souvent confidentiel, il est plus aisé d'utiliser l'argument d'un partenaire adhérent au Privacy Shield afin de susciter la confiance de clients

[353] ANONYME, « Marché unique numérique : un état des lieux », www.touteleurope.eu, publié le 15 mars 2018. https://www.touteleurope.eu/actualite/marche-unique-numerique-un-etat-des-lieux.html

potentiels. Dans la continuité du raisonnement de M. Romain Gola, Maître de conférences à l'Université d'Aix-Marseille, qui consiste à promouvoir la règlementation sur la protection des données personnelles d'un point de vue marketing, en rassurant les consommateurs et les investisseurs, ainsi qu'en l'utilisant comme gage de sérieux et de bonne foi[354], les acteurs peuvent dès lors valoriser leur certification.

Nul doute donc que le RGPD et le Privacy Shield doivent également servir de fer de lance dans le développement de l'économie numérique européenne et à son exportation. Des interrogations subsistent concernant les entreprises européennes voulant installer une filiale aux États-Unis. En effet, on pourrait cette fois penser qu'une telle implantation puisse poser des problèmes en matière de concurrence notamment puisque dans le domaine du numérique, l'Union européenne ne semble pas aujourd'hui, avoir de réelles positions.[355] Pour rappel, les données personnelles aux États-Unis sont considérées comme des biens commerciaux et par définition leur commerce est libre et sans contrainte. En effet, en 2016, le Congrès des États-Unis est revenu sur un règlement de la FTC qui visait à instaurer de nouvelles obligations à la charge des fournisseurs d'accès internet. Il a promulgué par la suite une loi autorisant la vente des données personnelles de ces utilisateurs de FAI, à des annonceurs, à des fins de ciblage publicitaires.[356] Cependant, le vent tourne, et il est à la faveur d'une protection accrue des données personnelles, comme en témoigne l'adoption récente de la loi californienne sur la protection des données personnelles des consommateurs qui garantit des droits importants,[357] ainsi que les récentes déclarations de Tim Cook et Satia Nadella militant pour un « RGPD américain ».[358] Ce sont autant de facteurs qui permettraient aux acteurs du Vieux continent de tirer pleinement profit de leur situation puisqu'aussi naïf soit-il, une filiale certifiée au titre du Privacy Shield dont le siège est en Europe a toutes les chances de respecter les principes du RGPD.

À l'inverse, les géants américains ayant des filiales sur le sol européen ressentent les premiers effets de ce que l'on pourrait qualifier d'un protectionnisme européen.

---

[354] GOLA V (R.), *Droit du E-commerce et du marketing digital*, Gualino, juin 2019.
[355] BONIS (P.), « L'internet européen : intérêts communs et acquis communautaires », *Annales des Mines – réalités industrielles*, n° 2016/3, Août 2016, pp. 19 à 23, p. 23.
[356] BARRAUD (B.), « Aux États-Unis, les données personnelles sont des biens commerciaux comme les autres », *La REM*, n°42-43, Printemps – Été 2017.
[357] DEBET (A.), « Quelle législation pour la protection des données aux États-Unis », *communication commerce électronique*, n°5, Mai 2019, comm. 36.
[358] SFADJ (R.), GOMBAUD-SAINTONGE (H.), « Le RGPD est une mine de valeurs », www.lesechos.fr, publié le 4 Juin 2019.
https://www.lesechos.fr/idees-debats/cercle/le-rgpd-est-une-mine-de-valeur-1026362

B) … Et de restriction de l'économie numérique américaine

Sous le prisme des entreprises américaines, la stratégie de l'Union semble résolument en faveur de ses acteurs économiques. Si le RGPD est venu ajouter un certain nombre de contraintes supplémentaires quant à la protection des données des citoyens européens, le Privacy Shield se situe dans la continuité en matière de transferts et de flux transfrontières. Pour rappel, le secrétaire du commerce américain Wilbur Ross avait déjà qualifié le RGPD d'obstacle au commerce international[359] et il n'y a pas de raison qu'il en soit autrement pour le Privacy Shield puisque cet outil impose des mesures à prendre à la charge des entreprises américaines sur les données transférées. Comme il a été vu précédemment, les principes du Privacy Shield sont une version édulcorée du RGPD. Cela est tout de même suffisant pour éviter que les données collectées en Europe et rapatriées aux États-Unis ne soient totalement hors de contrôle. Dès lors, il faut constater que l'Europe a eu dès le départ cette volonté d'ériger une barrière à sa frontière en matière de données personnelles même si cette dernière reste poreuse.[360] En effet, si le Chapitre 5 du Règlement prévoit les différentes dispositions pour qu'un transfert de données personnelles soit légal,[361] des réserves avaient été émises quant à la conformité du Privacy Shield aux exigences du RGPD et le Parlement avait notamment demandé sa suspension,[362] tandis que chaque année, le groupe des CNIL européennes émet de fortes critiques. Par conséquent, la réelle utilité du Privacy Shield doit être trouvée ailleurs que sur le terrain de la protection des données personnelles. Par son formalisme et ses principes imposés sans trop s'encombrer du respect strict du RGPD, on peut cependant admettre qu'il constitue un obstacle formaliste pour les entreprises américaines dans le transfert des données sur le territoire américain, également à rapprocher de cette volonté d'ériger une frontière. Comme vu précédemment, le Privacy Shield a pour effet de verrouiller le marché, et notamment pour les petites entreprises. En effet, toute proportion gardée, la masse de contraintes pesant sur les gérants d'entreprises américaines, qui rappelons-le, ne sont pas habitués à devoir faire tant de concessions sur le terrain des données personnelles, a pour conséquence le découragement de

[359] LAUSSON (J.), « Les États-Unis planchent aussi sur leur RGPD, mais dans une version moins stricte », www.numerama.com, publié le 30 juillet 2018. https://www.numerama.com/politique/400580-les-etats-unis-planchent-aussi-sur-leur-rgpd-mais-dans-une-version-moins-stricte.html

[360] MONNERIE (N.), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, n°2018/4, volume 32, p. 449.

[361] Voir à ce titre les art. 44, 45 et 46 du RGPD.

[362] Proposition de résolution 2018/2645(RSP) du Parlement européen, du 26 juin 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis.

ces dernières puisqu'il s'agit d'un fardeau trop lourd à porter.[363] Tandis que les petites et moyennes entreprises américaines représentaient 60 % des organisations adhérant au Safe Harbor, les nouvelles obligations au titre du Privacy Shield ont fait chuter la participation de ces dernières.[364] L'ancienne secrétaire au commerce Julie Brill évoque le manque de moyens des entreprises américaines dépendant de la libre circulation des données pour vendre des biens et des services, pour construire une force de travail mondialisée notamment.[365] Il y a donc une forte distorsion entre la volonté affichée par la Commission de mettre à la disposition de toutes les entreprises américaines un outil permettant d'assurer un gros volume de transferts et la réalité des faits. Les contraintes du Bouclier de protection ont plutôt tendance à renforcer les politiques protectionnistes que l'Union européenne tente de mettre en place, afin de favoriser le développement de ses acteurs sur le marché numérique. Pour résumer, il s'agirait donc de favoriser la création d'un marché numérique unique tout en réitérant la volonté d'utiliser le droit comme outil de souveraineté afin de contrer les opérateurs étrangers.[366] Il est certain que le Privacy Shield est une composante de cet outil.

Pour ce qui est des GAFA, dont l'UE sait pertinemment qu'ils contrôlent déjà le marché, il s'agit de s'assurer que les données seront toujours sous contrôle après avoir quitté le territoire européen. En effet, ces entreprises sont en position de monopole ou quasi-monopole mondial. Si certains arguent que cette position est méritée car ils n'ont ni tué la concurrence ni été protégés par une législation favorable,[367] il semble que c'est justement l'appréhension tardive par le droit qui est à la source de ces situations qui deviennent de plus en plus problématiques au point que certaines voix s'élèvent pour le démantèlement de certains GAFA.[368] L'enjeu est donc de contenir, plutôt que de concurrencer.

---

[363] MCALLISTER (C.), « What about small businesses? The GDPR and its consequences for small U.S.-based companies? », *Brooklyn Journal of Corporate, Financial & Commercial Law*, volume 12, issue 1, 1er Septembre 2017, pp. 188 à 211. p. 205.

[364] *Voir supra sur la pérennité des activités américaines.*

[365] BRILL (J.), « Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation, Keynote Address at Ghostery », *Hogan Lovells Data Privacy Day*, n°9, le 21 Janvier 2016.

[366] LE NOAN (E.), « Non à un protectionnisme numérique européen », www.lesechos.fr, publié le 23 Octobre 2018.
https://www.lesechos.fr/idees-debats/cercle/non-a-un-protectionnisme-numerique-europeen-142602

[367] LÉVÊQUE (F.), « François Lévêque : « Face aux GAFA, l'Europe doit accélérer la numérisation de ces entreprises », www. alternatives-economiques.fr, publié le 31 Décembre 2018.
https://www.alternatives-economiques.fr/francois-leveque-face-aux-gafa-leurope-accelerer-numerisati/00087513

[368] LELOUP (D.), UNTERSINGER (M.), « « Le pouvoir de Mark Zuckerberg est sans précédent » : un de ses cofondateurs appelle à démanteler Facebook », www.lemonde.fr, publié le 9 Mai 2019.
https://www.lemonde.fr/pixels/article/2019/05/09/le-pouvoir-de-mark-est-sans-precedent-un-des-cofondateurs-de-facebook-appelle-maintenant-a-le-demanteler_5460057_4408996.html

Pour autant, il semble que la tentative de régulation des GAFA américains sur le terrain du droit des données personnelles n'ait pas porté ses fruits. En effet depuis l'entrée en vigueur du RGPD, et ce malgré les violations régulières par ces géants américains de la règlementation européenne, les plaintes enregistrées ne ciblent en majorité pas ces entreprises. En 2018, en France, 11 000 plaintes ont été enregistrées et la plupart visent des PME, des associations ou des institutions publiques et non les GAFA.[369] Le droit des données personnelles n'étant pas assez efficace pour satisfaire les ambitions communautaires, c'est donc logiquement que le Privacy Shield échoue également ; en effet, la tendance est que les géants de la Tech américains quand il s'agit de transférer des données se certifient au titre du Privacy Shield.[370] Les filiales européennes possédant déjà des politiques de protection des données personnelles respectant les standards de la législation européenne, il est donc aisé de se soumettre aux exigences du Privacy Shield.

Pour l'Union européenne et le développement de sa stratégie de développement de l'économie numérique, les solutions afin de contrer les GAFA semblent plutôt se trouver sur le terrain du droit de la concurrence.[371] Cependant, il a été observé que les comportements anticoncurrentiels sont difficilement sanctionnables en matière de données personnelles.[372] Par conséquent, il s'agira plus généralement de concilier les approches en matière de données personnelles, en matière de concurrence et en matière fiscale.

L'autre volet auquel il faut s'intéresser est celui du Big Data ainsi que le Cloud Computing, véritables moteurs de ces géants du numérique que l'on peut qualifier d'opérateurs systémiques en dominant les réseaux d'information.[373]

---

[369] LAZARÈGUE (A.), « Là où le RGPD a échoué, le droit de la concurrence peut encore gagner. », www.lemonde.fr, publié le 14 Juin 2019. https://www.lemonde.fr/idees/article/2019/06/14/la-ou-le-rgpd-a-echoue-le-droit-de-la-concurrence-peut-encore-gagner_5476263_3232.html

[370] Voir à ce titre la liste du Privacy Shield dans laquelle apparaissent beaucoup de GAFA.

[371] LAZARÈGUE (A.), « « Là où le RGPD a échoué, le droit de la concurrence peut encore gagner. » », www.lemonde.fr, publié le 14 Juin 2019. https://www.lemonde.fr/idees/article/2019/06/14/la-ou-le-rgpd-a-echoue-le-droit-de-la-concurrence-peut-encore-gagner_5476263_3232.html

[372] MONNERIE (N.), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, n°2018/4, volume 32, p. 440

[373] *Ibid.*

Section 2 : Le Privacy Shield dans le cadre du Big data et du Cloud Computing

Avant tout, il convient d'étudier les notions et enjeux du Big Data et du Cloud Computing (I) afin de bien comprendre la contribution et l'utilité du Privacy Shield sur ces aspects du marché de la donnée (II)).

I) Notions et enjeux du Big Data et du Cloud Computing

Ces deux concepts sont les pierres angulaires du fonctionnement des géants numériques américains comme les GAFA ou les NATU. En effet, ils leur ont permis de créer et maintenant de conserver l'hégémonie qu'ils détiennent sur le marché de la donnée. Il s'agit donc dans un premier temps d'étudier synthétiquement les notions techniques de Big Data et de Cloud Computing (A), avant de démontrer la dominance des GAFA sur ces concepts fondamentaux du marché de la donnée (B).

A) Notions techniques de Big Data et de Cloud Computing

Ces notions renvoient à des situations et des réalités différentes bien qu'elles se recoupent dans leur utilisation. En premier lieu, il faut définir le Big Data qui est la notion clé et dans un second temps il convient de s'intéresser au Cloud Computing.

1) Le Big Data

Pour différencier les systèmes traditionnels du Big Data, Gilles Babinet, ancien président du Conseil national du numérique et champion du numérique de la France auprès de l'Union européenne, utilise une métaphore assez pertinente pour comprendre le Big Data :

> « Dans un modèle classique, si les données étaient une photographie, on déconstruirait celles-ci pixel par pixel et on rangerait ces pixels en fonction de leur couleur : les rouges dans le silo rouge, les bleus dans le silo bleu, et ainsi de suite. Dans le modèle du Big Data, rien de tel. L'on prendra simultanément plusieurs jumelles afin de zoomer sur la photo aux différents endroits auxquels l'on s'intéresse, pour observer à loisir des variations entre différents points de la photo. Dans un cas, les données sont prétraitées (et structurées […]) : il s'agit du modèle classique ; dans l'autre, les données sont utilisées en mode non structuré. Le premier cas permet de faire de façon remarquablement efficace des opérations simples : compter le nombre de pixels, connaître le nombre de fois où ils se trouvent à côté d'un pixel rouge, la moyenne à

laquelle les bleus apparaissent, etc. L'autre système permet d'observer que les pixels dessinent un visage et que ce visage regarde un autre visage ; ce que l'on n'aurait sûrement jamais vu avec un système d'analyse de type structuré. »[374]

C'est d'ailleurs du constat que les modèles traditionnels ne suffiraient plus à suivre l'accroissement du trafic des réseaux, qu'est né le Big Data. En effet, il était impératif de faire évoluer les technologies et plus précisément les algorithmes.[375] Devant cette confrontation à une masse importante de données, Google crée une base de données compressée nommée *Big Table* en 2001, grâce à l'algorithme *Map Reduce* publié en 2004. Un ingénieur de chez Yahoo, Doug Cutting réalise le potentiel de cette technologie et lance *Hadoop*, un outil en open source capable de gérer d'énormes quantités de données qui fait désormais référence en matière de Big data.[376]

Étant un terme relativement nouveau, le « Big Data » a plusieurs acceptions. Si certains lui prêtent une définition vaste, le faisant corréler à « une quantité de données au-delà des capacités technologiques de stockage, de gestion, de traitement efficaces »[377], d'autres l'ont défini par la formule des trois V : Volume, Variété, Vélocité[378] ; les trois V ayant à la base été dégagés par Gartner afin de définir les grands enjeux du big Data.[379] Cependant, c'est bien la formule optimisée des quatre V qui fait consensus ; le quatrième V signifiant Valeur.[380] La définition retenue ici est la suivante : « Le Big Data est un ensemble de techniques et de technologies qui requièrent de nouvelles formes d'intégration pour découvrir une large valeur cachée à partir d'ensembles de données qui sont diverses, complexes et à une échelle gigantesque ».[381]

---

[374] BABINET (G.), *Big Data, penser l'homme et le monde autrement*, éditions Le Passeur, 19 février 2015.
[375] *Ibid.*
[376] BRASSEUR (C.), « Usages visuels des données et Big data », *I2D – Information, données et documents*, 2015/2, volume 52, 2015 p. 44.
[377] MANYIKA (J.), CHUI (M.), BROWN (B), BUGHIN(J.), DOBBS (R.), ROXBURGH (C.), BYERS (A.H.), « Big Data: The next frontier for innovation, competition, and productivity », www.mckinsey.com, mai 2011, p. 1.
https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation
[378] BERMAN (J.J.), *Principles of Big Data*, Morgan Kaufmann, Boston, 2013, introduction.
[379] HASHEM A. T. (I.), YAQOOB (I.), ANUAR B. (N.), MOKHTAR (S.), GANI (A.), KHAN U. (S.), « The rise of "big data" on cloud computing: Review and open research issues », *Information Systems*, volume 47, Janvier 2015, pp. 98 à 115, p. 100.
[380] GANTZ (J), REINSEL (D.), « Extracting Value from Chaos », *IDC iView*, juin 2011, pp. 1 à 12.
[381] HASHEM A. T. (I.), YAQOOB (I.), ANUAR B. (N.), MOKHTAR (S.), GANI (A.), KHAN U. (S.), « The rise of "big data" on cloud computing: Review and open research issues », *Information Systems*, volume 47, Janvier 2015, pp. 98 à 115. p. 100.

Ainsi, le volume est la quantité de données, de toutes natures provenant de différentes sources ; la variété c'est justement toutes les sortes de données collectées ; la vélocité s'apparente à la vitesse de transfert de la donnée ; et la valeur c'est le résultat après la transformation du grand nombre de données traitées.[382]
On peut donc classer le big data en plusieurs catégories ; les sources de la collecte de données ; le format, à savoir si l'ensemble est structuré ou non ; la manière de stocker les données, de manière graphique ou en colonnes par exemple ; la préparation des données, à savoir si elles sont transformées ou standardisées ; et le traitement des données, avec par exemple le traitement par lot ou le traitement en temps réel.[383]

Les technologies du Big Data permettent donc de collecter une quantité gigantesque de données et de les affiner pour une multitude de finalités grâce à de puissants algorithmes. Il est très utile dans l'utilisation du Cloud Computing.

2) Le Cloud Computing

De manière très simple, le Cloud Computing pourrait être défini comme une technologie permettant l'accès à des fichiers, à des données, à des programmes et à des services par le biais d'un navigateur internet.[384] Le Cloud Computing offre donc une solution à tout individu ou à toute entité d'accéder à des données.

Le problème est que les définitions fleurissent et il est difficile de ne pas se noyer dans la masse de significations qui lui sont prêtées. En 2008, quand le Cloud Computing est la nouvelle technologie en vogue, de nombreuses voix s'élèvent pour dénoncer une expression fourre-tout, dont celles de responsables de grandes entreprises comme Oracle ou Hewlett-Packard.[385]

En 2011, le « National Institute of Standards and Technology », agence fédérale sous la tutelle du Ministère américain du Commerce, dont la mission est notamment de promouvoir

[382] *Ibid.*
[383] *Ibid.*
[384] KIM (W.), « Cloud Computing: Today and Tomorrow », *Journal of object technology*, Volume 8, n°1, janvier/février 2009, pp. 66 à 72, p. 66.
[385] ARMBRUST (M.), FOX (A.), GRIFFITH (R.), JOSEPH D. (A.), KATZ H. (R.), KONWINSKI (A.), LEE (G.), PATTERSON A. (D.), RABKIN (A.), STOICA (I.), ZAHARIA (M.), « Above the Clouds: A Berkeley View of Cloud Computing », *Technical Report n° UCB/EECS-2009-28*, publié le 10 février 2009, p. 3.

l'économie américaine par le développement de technologies, publie dans une recommandation, sa définition technique du Cloud Computing. C'est donc :

> « Un modèle permettant un accès omniprésent, pratique et à la demande, à un ensemble partagé de ressources informatiques paramétrables (ex. : réseaux, serveurs, conservation, applications, et services) qui peuvent être rapidement fournies et émises avec le minimum d'effort de gestion ou d'intervention du fournisseur du service. »[386]

La publication détaille ensuite les cinq caractéristiques essentielles qui sont le self-service à la demande, l'accès au travers d'un large réseau ; le partage de ressources ; l'élasticité rapide des technologies, c'est-à-dire la possibilité pour l'utilisateur d'y accéder instantanément, de manière illimitée, partout et tout le temps ; et la mesure du service, c'est-à-dire le contrôle et l'optimisation des ressources.[387]

Les services de Cloud Computing permettent donc de bénéficier d'infrastructures complexes qui sont gérées par des tiers, mais qui évitent de se doter de matériel informatique coûteux pour du stockage par exemple, ou simplement de fournir un service de communication en ligne à des utilisateurs.[388] Cette technologie permet entre autres de manière schématique l'accès à des matériels informatiques à distance tel que des serveurs ou des Data Centers.

Le Cloud Computing sublime les technologies du Big data car l'allocation de gigantesques ressources communes permettent de collecter, de stocker et de traiter des quantités incroyables de données. Force est de constater que les GAFA dominent ces technologies fondamentales ce qui accroît leur mainmise sur le marché de la donnée.

B) La dominance des GAFA sur ces technologies fondamentales du marché de la donnée

Selon des auteurs américains, le marché de la donnée est structuré en trois niveaux. En premier lieu, il y a la collecte massive de données avec les fameux data brokers qui créent par la suite des bases de données. C'est une sorte de minage de la matière première. C'est également ce qui correspond à la phase du Big Data. Par la suite, cette masse d'informations est transformée en données économiquement exploitables. En pratique, il s'agit d'analyser les

[386] MELL (P.), GRANCE (T.), « The NSIT Definition of Cloud Computing », *recommendations of the National Institute of Standards and Technology*, special publication 800-145, septembre 2011, p. 2.
[387] *Ibid.*
[388] HASHEM A. T. (I.), YAQOOB (I.), ANUAR B. (N.), MOKHTAR (S.), GANI (A.), KHAN U. (S.), « The rise of "big data" on cloud computing: Review and open research issues », *Information Systems*, volume 47, Janvier 2015, pp. 98 à 115, p. 101.

données afin de dégager des données de qualité. Il s'agit donc métaphoriquement du polissage de la donnée brute. Enfin, une fois que ces données sont exploitables il s'agit de les utiliser ou de les vendre.[389]

Force est de constater que les géants américains du numérique dominent toutes ces étapes du marché ou ont pour le moins une présence significative leur permettant une situation de quasi-monopole.[390] Cela s'explique par le nombre d'utilisateurs de leurs services, par la variété et le volume des données collectées. En 2016, Facebook révélait une liste de 98 types de données personnelles utilisées à des fins de profilage aux États-Unis. Ainsi l'entreprise collecte les opinions politiques puisqu'il classe ses utilisateurs entre conservateurs ou libéraux, mais s'intéresse également au statut relationnel de ses utilisateurs, à savoir s'ils sont dans une nouvelle relation, ou bien une relation longue distance. Facebook affirme également connaître sur une personne, la taille de sa maison, si elle est propriétaire ou locataire, la composition de la construction de la maison, la valeur de la maison.[391] En termes de Big Data donc, force est de constater que Facebook collecte énormément d'informations sur ces utilisateurs en utilisant ces technologies. Par la suite, la firme basée à Menlo Park, CA, ne se cache pas de revendre les données à des annonceurs afin de faire de la publicité ciblée sur le réseau social. Pour cela, encore faut-il que l'information soit exploitable. On se doute dès lors que l'armée d'analystes de données travaillant pour Facebook a également pour mission de polir la masse de données collectées afin de fournir aux annonceurs le meilleur ciblage possible. En effet, l'onglet confidentialité qui annonce la politique en matière de données personnelles explique que les annonces sont personnalisées, sélectionnées, mais que les données servent également à fournir des mesures ou des analyses à des annonceurs ou des partenaires.[392] Cela signifie donc bien que les données ne sont pas simplement collectées en masse, mais qu'elles sont bien analysées et polies.

---

[389] HAGEL (J.) et SINGER (M.), « Net Worth: Shaping Markets when Customers Make the Rules », *Harvard Business School Press*, 8 janvier 1999 ; PATTERSON (M.), « On the Impossibility of Information Intermediaries », *Fordham Law and Economics Research Paper*, n° 13, juillet 2001 ; EVANS (P.) et WURSTER (T.), « Blown to bits: how the new Economics of Information Transforms Strategy », *Harvard Business School Press*, 2000, pp. 64-65 ; VOLOKH (E.), « Cheap Speech and What it Will do », *The Yale Law Journal*, volume 104, 1994-1995, p. 1805 ; SEN (S.), JOE-WONG (C.), HA (S.) et CHIANG (M.), « Smart Data Pricing: Economic Solution to Network Congestion », *Princeton University, Working Paper*, 11 avril 2013 ; PORTER (M.) et HEPPELMAN (J.), « How Smart Connected Products are Transforming Competition », *Harvard Business Review*, novembre 2014.

[390] MONNERIE (N.), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, n°2018/4, volume 32, p. 433.

[391] DEWEY (C.), « 98 personal data points that Facebook uses to target ads to you », www.washingtonpost.com, publié le 19 août 2016.

[392] Voir la politique de confidentialité de Facebook.

Reposant sur la même économie, tous les géants américains du numérique ont les mêmes pratiques et utilisent bien souvent les mêmes techniques et les mêmes stratégies sur le marché de la donnée, contribuant ainsi à ce règne sans partage. On peut par exemple citer Google qui concentre 90 % des recherches sur internet avec 40 000 requêtes par seconde.[393] Le fondement de ce règne sur le trafic massif de données est évidemment l'utilisation des technologies du Big Data.

Mais l'utilisation du Cloud Computing a également un impact fondamental sur l'optimisation des modes de fonctionnement des GAFA. Il ne sera pas fait ici de distinction entre les « Software as a service », « Infrastructure as a service » et « Plateform as a service ». Cependant, il faut garder à l'idée que les GAFA ne pourraient pas être aussi performants sans le recours aux technologies de Cloud. En effet, l'architecture en Cloud permet aux fournisseurs de service de centraliser et donc de simplifier l'installation de leurs logiciels, la maintenance et le contrôle.[394] En contrepartie, les utilisateurs peuvent accéder au service sans limites. La facilité d'utilisation et la praticité pour l'utilisateur ont notamment pour conséquence l'accroissement de l'utilisation du service qualitativement et quantitativement. Cela signifie qu'un utilisateur utilisera de plus en plus le service et que de plus en plus de personnes vont utiliser ce service. La collecte de données via un système informatique centralisé permet d'empêcher la dissémination de ces dernières puisque par définition elles seront stockées à un seul endroit ou bien à des endroits géographiquement stratégiques. En 2017, il y avait environ 4000 data centers répartis dans 18 pays.[395] Par exemple, la majorité des requêtes des utilisateurs de Facebook en Europe sont traitées dans son Data Center en Suède. Cela permet également de réguler le trafic mondial des données par souci d'efficacité.[396]

La technologie du Cloud Computing a donc réellement permis l'optimisation des ressources de ces entreprises et contribue à l'hégémonie des GAFA sur le marché mondial de la donnée et du numérique.

---

[393] BUCHY (F.), « Les GAFA sont-ils trop puissants ? », www.grandes-ecoles.studyrama.com, publié le 19 novembre 2018.
https://grandes-ecoles.studyrama.com/espace-prepas/concours/ecrits/hggmc/esh/economie/les-gafa-sont-ils-trop-puissants-7301.html

[394] ARMBRUST (M.), FOX (A.), GRIFFITH (R.), JOSEPH D. (A.), KATZ H. (R.), KONWINSKI (A.), LEE (G.), PATTERSON A. (D.), RABKIN (A.), STOICA (I.), ZAHARIA (M.), « Above the Clouds: A Berkeley View of Cloud Computing », *Technical Report n° UCB/EECS-2009-28*, publié le 10 février 2009, p. 4.

[395] DE KERAUTEM (V.), « Data centers : mais où se trouvent vos données ? », www.leparisien.fr, publié le 20 février 2017.

[396] EUDES (Y.), « Visite exceptionnelle dans le data center de Facebook, en Suède », www.lemonde.fr, publié le 19 mai 2016.
https://www.lemonde.fr/pixels/article/2016/06/03/les-datas-du-grand-froid_4932566_4408996.html

En ce qui concerne notre étude, qui dit masse de données immense et Cloud Computing, dit nécessairement transfert de données. Il n'y a pas nécessairement de flux transfrontières quand les données sont conservées en Europe, mais comme les data centers dans un système de cloud sont interconnectés, le transfert de données peut avoir lieu entre l'Europe et un pays tiers. En l'occurrence, de nombreux transferts de données sont effectués vers les États-Unis.
Dès lors, le Privacy Shield contribue à légaliser ces transferts et il démontre son utilité politique et économique.

II) Contribution et utilité du Privacy Shield sur ces aspects du marché de la donnée

Le marché de la donnée est devenu très complexe à contrôler. Ainsi il a fallu notamment contrôler les transferts. Entre l'UE et les États-Unis, ces transferts impliquent la potentielle utilisation du Privacy Shield (A). L'idée sous-jacente est que le contrôle des transferts doit se faire par un encadrement et non par un ciblage (B).

A) Le transfert de données EU/U.S, synonyme d'utilisation du Privacy Shield

À l'ère du Big Data et du Cloud Computing, les données se multiplient de manière exponentielle. En effet, les nouveaux modes de consommation numérique stimulent le marché de la donnée. À titre indicatif, en 2015, l'humanité postait 350 000 tweets toutes les minutes et de manière générale, 1 740 000 giga-octets d'informations étaient créés dans le monde.[397] Le droit doit nécessairement répondre aux problématiques posées par la démocratisation de ces nouvelles technologies dans l'économie et l'accès à de nouveaux services pour toute la population. Force est de constater que malgré ses nombreuses défaillances, le Privacy Shield constitue une partie de cette réponse juridique afin de préserver la libre circulation des données conditionnant la liberté d'accès à ces services. En effet dans l'exploitation de la donnée personnelle, son transport, son acheminement sont par exemple, des étapes très importantes du commerce de la donnée, carburant des activités des GAFA. De la même façon, la donnée est très volatile et ubiquitaire dans le sens où elle peut être traitée dans plusieurs endroits différents. Le processus consiste donc en la duplication de la donnée puis en son transport vers le futur lieu de traitement. La donnée pouvant de manière générale être assimilée à un bien incorporel,

[397] Rapport du CIGREF d'octobre 2015 sur l'« économie des données personnelles : les enjeux d'un business éthique », p. 1.

elle est susceptible de faire l'objet d'échange de toute nature.[398] Dès lors, le droit régule ces flux de données personnelles. Le RGPD comme la directive avant son adoption prévoit un chapitre entier sur le transfert de données personnelles vers des pays tiers ou à des organisations internationales. Pour rappel, le transfert fondé sur la décision d'adéquation de la Commission n'est qu'une des possibilités offertes par les textes pour opérer un transfert. Le transfert peut en effet être effectué si des garanties appropriées telles que des BCR, des clauses contractuelles types, ou un mécanisme de certification, sont mises en place.[399] Le constat est que le Privacy Shield est un mécanisme à base légale hybride. En effet, le mécanisme en soi est prévu sur la base des garanties appropriées, mais il existe bien une décision d'adéquation de la Commission entérinant ce mécanisme. Le bouclier de protection intervient car la Commission n'a pas reconnu que les États-Unis en tant qu'État apportaient une protection des données à caractère personnel suffisante. En effet, la liste blanche des pays justifiants d'une protection adéquate est mince. Figure sur cette liste, Andorre, l'Argentine, le Canada (seulement pour ce qui concerne les transferts entre organisations commerciales), les îles Féroé, Guernesey, Israël, l'île de Man, le Japon, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay.[400] Il est difficile dès lors d'imaginer, vu le nombre de transferts effectués par les GAFA à l'ère du Big Data, qu'il n'existe pas de solution légale globale afin de transférer des données personnelles du territoire de l'Union européenne jusqu'aux États-Unis. Mais il est peut-être encore plus difficile d'imaginer une protection adéquate de la part des États-Unis, de nature à justifier une décision d'adéquation. C'est donc encore une fois le compromis qui a été choisi et ici le droit n'est qu'un moyen et non une finalité. Comme il a déjà été souligné, le Privacy Shield permet par essence de transférer de grandes quantités de données. Les transferts devenant toujours plus nombreux et plus rapides, du fait du Big Data,[401] un accord de ce type est économiquement indispensable pour les entreprises, mais aussi indispensable pour l'Union européenne et pour ces citoyens bénéficiant de services de ces acteurs économiques. Dans ce sens, l'accord est politique puisqu'un volume élevé de données transférées implique quasi systématiquement l'utilisation du Privacy Shield faisant de lui un accord nécessaire. De la même façon, le système du Cloud Computing permettant notamment l'optimisation des ressources informatiques par un centre d'opération massif, dont les data centers sont un bon exemple, incite à l'envoi de données vers

[398] BENSOUSSAN (A.), « La propriété des données », www.blog.lefigaro.fr, publié le 18 mai 2010. http://blog.lefigaro.fr/bensoussan/2010/05/la-propriete-des-donnees.html
[399] Art. 45 et 46 du RGPD.
[400] Voir les décisions d'adéquations de la Commission sur les pays autorisés à transférer des données personnelles depuis le territoire européen, www. ec.europa.eu.
[401] *Voir supra relatif aux 4 V et plus spécifiquement le volume et la vélocité.*

ces derniers ; quand bien même ces centres existent également en Europe, et qu'il est fortement conseillé d'héberger des données sur le territoire européen dans la mesure où chaque organisation doit permettre un contrôle par une autorité européenne indépendante,[402] il a déjà été mentionné que pour des raisons tenant aux trafics d'informations mondiaux, les données peuvent transiter par les États-Unis.[403] Dès lors, il est impossible d'apporter une garantie par transfert, d'autant plus que ces derniers sont automatisés. La meilleure solution encore une fois est une autorisation de transfert globale. Le constat est donc le suivant : les évolutions technologiques qui permettent de traiter toujours plus de données obligent le législateur à orienter le droit vers un encadrement sous la forme d'obligations générales à la charge de l'entreprise sous peine de sanctions et le Privacy Shield n'échappe pas à cette règle. De cette manière, les transferts transatlantiques de données personnelles, intensifiés par le développement de ces nouvelles technologies informatiques, sont légalisés et l'encadrement aussi faillible soit-il, existe à la charge des opérateurs américains. Ces derniers peuvent dès lors transférer des données après validation de la certification, tandis que dans une économie fondée sur la donnée personnelle, les utilisateurs européens peuvent continuer à bénéficier de services numériques sans contrepartie pécuniaire. En ce sens, le Privacy Shield est une pièce juridique contribuant au bon fonctionnement de la machine de l'économie du numérique basée entre autres sur le Big Data et le Cloud Computing.

B) Le contrôle par l'encadrement plutôt que par le ciblage

Il est clair que des choix politiques ont été faits quant au contenu du Privacy Shield et plus spécifiquement sur son régime juridique. Comme il a déjà été mentionné, l'accord entre les États-Unis et l'Union européenne a été le fruit de négociations intenses. Au-delà de la conciliation de deux conceptions différentes du statut des données personnelles, les différentes évolutions technologiques ont certainement impacté le contenu de l'accord. En effet, le Safe Harbour ne prenait pas en considération les problématiques liées au Big Data puisque bien antérieur à l'émergence de ce phénomène et ne prévoyait logiquement donc pas de règles adaptées aux gros volumes de transferts transatlantiques de données. L'approche choisie dans le Bouclier de protection par les négociateurs a pris en compte les réalités informatiques modernes, dans la tendance actuelle du droit des données personnelles. Plutôt que de prôner un contrôle ciblé sur toutes les entreprises et sur tous les transferts, c'est un mécanisme

[402] Déclaration commune adoptée par le G29 du 25 novembre 2014 dans le cadre de « The European Data Governance Forum » du 8 décembre 2014.
[403] *Voir supra sur le Cloud et le trafic internet mondial.*

d'« accountability » qui est mis en place. En effet, face à de tels volumes de données, c'est bien l'approche pragmatique américaine qui a été préférée, comme dans la rédaction du RGPD.[404] N'en déplaise aux partisans d'une approche basée sur un contrôle absolu et des règles ultra-complexes et détaillées, la solution privilégiée bien qu'imparfaite impliquant directement les acteurs, semble la plus réaliste. En effet, malgré les critiques justifiées, formulées à l'égard de l'accord sur son manque de rigueur juridique,[405] il faut garder les pieds sur terre et accepter que dans le monde du numérique, tout ne peut pas être contrôlé. À partir du moment où l'on perd cette réalité tangible pour basculer dans une réalité immatérielle, la conception de la règle juridique change. En ajoutant à cela l'automatisation des tâches, le développement de l'intelligence artificielle et le volume toujours plus grand de données, il est plus simple d'appréhender juridiquement les problématiques en cadrant plutôt qu'en ciblant.

C'est d'ailleurs un constat plus généraliste que l'on peut faire en droit du numérique et plus spécialement sur des textes entrés en vigueur dans les années 2000 et n'ayant pas suivi les évolutions technologiques ayant révolutionné les pratiques. À titre d'exemple, on peut citer la directive commerce électronique ayant exonéré de responsabilité les opérateurs de prestataires intermédiaires de services, afin de ne pas freiner le développement de l'économie numérique.[406] L'émergence et le développement du commerce électronique par l'intermédiaire de plateformes e-commerce et du concept de marketplace sont venus bouleverser les schémas et prédictions qui avaient été établis en 2000. Étant confrontée à une irresponsabilité prévue par le droit européen, la France s'est dotée de la loi « pour une république numérique » du 7 octobre 2016, afin de mettre des obligations à la charge de ces opérateurs de plateforme.[407] De plus, un règlement « Platform To business » est en préparation au niveau européen afin de compléter une législation imparfaite n'ayant pas pris la mesure des évolutions technologiques qui ont changé les pratiques commerciales. Ce nouveau règlement vient notamment fixer des exigences communautaires aux opérateurs de plateforme.[408]

---

[404] MAXWELL (W), TAIEB (S), « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT 2016* p.123.
[405] CASTETS-RENARD (C), « L'adoption du Privacy Shield sur le transfert de données personnelles », *Recueil Dalloz* n°28, Août 2016, p. 1696.
[406] GRYNBAUM (L.), « La directive « Commerce électronique » ou l'inquiétant retour de l'individualisme juridique », *La Semaine Juridique – Edition Générale,* n°12, 21 mars 2001.
[407] BOUGUETTAYA (F), « Loi « pour une république numérique » : quel impact pour l'e-commerce », *Revue Lamy droit de l'immatériel,* n°133, 1er janvier 2017, p. 2.
[408] ANONYME, « Un accord en trilogue sur le règlement « platform to business » a été trouvé », *Contrats Concurrence Consommation* n°4, Avril 2019, alerte 16 sur le communiqué de la commission européenne du 14 février 2019.

Le but est de mettre en place une corégulation avec les opérateurs de plateforme voire même une autorégulation fondée sur des principes[409] avec comme finalité la responsabilisation de ces derniers.[410]

Dès lors, il faut se rendre compte que c'est exactement le même raisonnement qui est appliqué dans le cadre du Bouclier de protection entre les États-Unis et l'Union européenne ; il s'agit de cadrer plutôt que de cibler.

En matière de droit des données personnelles comme en matière de droit de la concurrence, le raisonnement juridique moderne est qu'il faut impliquer les acteurs économiques à défaut de pouvoir les contraindre. En effet, dans le cas des GAFA, forts de leur hégémonie, et du soutien du gouvernement américain, les menaces pèsent si des mesures trop restrictives à leur encontre sont prises. À titre d'exemple, lors des discussions sur la taxe GAFA en 2018, un groupe de sénateurs républicains avaient évoqué des sanctions financières à l'encontre de l'Union européenne si le texte était adopté.[411] De la même manière, la position de force des géants américains permet d'exercer des pressions non négligeables ayant de réelles conséquences sur les textes adoptés.[412] On comprend donc que la négociation reste le meilleur moyen d'arriver à des solutions en droit favorisant la responsabilisation par l'autorégulation et la corégulation et surtout ne pénalisant pas l'Europe et son économie. Cependant, dans le cadre du Privacy Shield, mais plus généralement dans les propositions et négociations de la Commission, cette vision à court terme risque de poser des problèmes par la suite. En effet, il y a fort à parier que ces grandes entreprises que l'on responsabilise en leur déléguant une partie du pouvoir normatif, bien qu'encadré, ne voient leur pouvoir s'accroître encore plus. Peut-être devrions-nous, être acteur plutôt que spectateur, dans la manière de légiférer. En effet, le développement des technologies de l'information est entre les mains de ces très puissantes entreprises. Comme il est démontré que ces technologies influencent les conceptions légales, il serait de bon ton de rééquilibrer ladite influence qu'un pôle a sur un autre. L'éternelle question subsiste : qui du droit ou de l'évolution influence l'autre ?

---

[409] La Commission européenne a publié des principes en matière de meilleures pratiques à l'adresse https://ec.europa.eu/digital-singlemarket/en/news/principles-better-self-and-co-regulation-and-establishment-community-practice.

[410] Communication COM(2016)288 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 25 mai 2016 sur « les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe », p. 6.

[411] MARCHAIS (I.), « Comment Washington fait pression contre la taxe GAFA à Bruxelles », www.lopinion.fr, publié le 11 mars 2019.
https://www.lopinion.fr/edition/international/comment-washington-fait-pression-contre-taxe-gafa-a-bruxelles-180382

[412] Voir à ce titre la campagne de lobbying dans le cadre de la directive droit d'auteur dans le marché numérique.

Toujours est-il qu'en pratique, on pourrait qualifier le Privacy Shield d'outil d'encadrement juridique de transferts de données personnelles entre les États-Unis et l'Union européenne à visée politique et économique, dont l'une des finalités est l'appréhension du développement des technologies informatiques,[413] propres à s'appliquer à de tels transferts.

De plus, cet accord a également contribué à ouvrir de nouveaux horizons politiques aux États-Unis en matière de protection des données personnelles.

[413] Notamment les technologies du Big Data et de Cloud Computing.

CHAPITRE II : Privacy Shield et évolution de la protection des données aux États-Unis.

Aux États-Unis, le vent tourne en matière de protection des données personnelles et le Privacy Shield s'inscrit dans cette mouvance protectrice. Ainsi, on constate un changement de position radical des acteurs américains sur les données personnelles (Section 1), mais également une amélioration de la protection légale des personnes aux États-Unis (Section 2).

Section 1 : Le changement de position des acteurs américains sur les données personnelles

Il est certain que cette mouvance et notamment, le changement de position des acteurs américains provient en partie des standards de protections européens qui sont véhiculés par le Privacy Shield (I), mais également parce que l'éthique des données personnelles est de plus en plus perçue comme un avantage pour les compagnies de la Tech. (II).

I) Des standards de protection véhiculés par le Privacy Shield

Le Privacy Shield a permis de véhiculer certains standards de protection issus des politiques européennes. Bien que l'on puisse de prime abord le qualifier de protection sectorielle, le Bouclier de protection revêt bien une logique de protection globale propre à l'Europe (A). De plus, les principes qu'il prévoit sont empreints d'une rigueur européenne (B).

A) Une protection sectorielle de prime abord masquant une logique de protection globale

On pourrait bel et bien considérer le Privacy Shield comme la continuité de l'approche sectorielle américaine. En effet, il n'y a *a priori* pas lieu de penser que l'accord proclame des principes qui revêtent une portée générale. En effet, ce texte n'existe que parce qu'il y a des transferts de données entre l'Union européenne et les États-Unis. Cela signifie qu'en dehors de ce champ, il n'a pas vocation à s'appliquer. Cependant, il faut d'abord définir le terme de sectoriel ou du moins savoir à quelle réalité il s'attache en droit. Ce qui est sectoriel est relatif à un secteur d'activité déterminé. Or un « secteur » connaît plusieurs acceptions. Ainsi il peut être défini comme un domaine déterminé d'activité économique, sociale dans un État, une

organisation ou une institution.[414] Mais il peut également renvoyer à la division d'un espace par rapport à une activité quelconque.[415] Il est donc essentiel de ne pas opposer les termes global et sectoriel puisque la globalité ou l'exhaustivité existe également dans une approche sectorielle, l'une n'empêchant pas l'autre. Cela explique d'ailleurs pourquoi au sein de la doctrine américaine, des voix se sont élevées afin de défendre la conception américaine sectorielle en arguant du fait que cela ne signifie pas qu'elle est moins stricte que la position européenne globale.[416]

Pour en revenir aux transferts de données personnelles, il faut tout d'abord comprendre que selon la définition que l'on choisit, ils peuvent être considérés ou non comme sectoriels. En effet, s'ils se rattachent à la division d'un espace par rapport à une activité, il y a bien lieu de considérer le caractère sectoriel des transferts puisqu'étant bien distincts du reste des activités du traitement de la donnée personnelle. En revanche si l'on prend la première acception, les transferts de données sont simplement une action réalisée par une organisation dépendante d'un secteur déterminé qui peut par exemple être économique, mais qui pourrait tout aussi bien être social.

Pour expliquer la protection des données personnelles aux États-Unis, Shawn Boyne, Professeur de droit à l'université de l'Indiana, considère que les Américains suivent une approche sectorielle du droit des données personnelles, car il n'y a pas de législation fédérale globale assurant la protection de la vie privée et des données personnelles, mais qu'il s'agit d'une combinaison de législations fédérales et étatiques, de règlementations administratives et de lignes directrices d'autorégulation émanant de certaines industries.[417] Les secteurs peuvent être par exemple la santé, l'éducation, les communications et les services financiers.[418] Ainsi, ce qui est sectoriel est nécessairement disséminé.

Cependant, il existe une législation fédérale spécifique sur la collecte en ligne des données personnelles des enfants. En effet, le texte impose des obligations à la charge des opérateurs de sites internet ou de services en ligne destinés à des enfants de moins de 13 ans ; et à tout autre site ou service en ligne qui a connaissance de collecter des données personnelles

[414] Définition du mot « secteur », www.larousse.fr.
[415] *Ibid.*
[416] SWIRE (P.), KENNEDY-MAYO (D.), « How both EU and the U.S. are "stricter" than each other for the privacy of government requests for information » *Emory Law Journal*, volume 66, 2016, p. 629.
[417] BOYNE M. (S.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343, p.299.
[418] *Ibid.*

d'enfants de moins de 13 ans.[419] Il est dans le cas de ce texte, difficile de parler d'approche sectorielle à moins de considérer les enfants de moins de 13 ans comme un secteur. Or, les autres domaines concernés par une législation spécifique en matière de données personnelles, étant plutôt d'ordre économique ou social, il y a lieu de considérer que le « COPPA » est plutôt un texte empruntant une approche globale.

La différence entre l'approche sectorielle et globale résiderait donc dans le cloisonnement et l'absence de cloisonnement. Tandis que certains secteurs sont cloisonnés, rien n'empêche que l'on retrouve des problématiques impliquant des enfants de moins de 13 ans, dans un environnement en ligne et pour des motifs commerciaux, qui sortent de ces cloisonnements. Par exemple, la collecte de données en ligne par un organisme d'assurance santé, qui relève du secteur de la santé régulé par le « Health Insurance Portability and Accountability Act » pourrait également se voir imposer le COPPA, si cet organisme remplit ces critères en collectant des données. Donc, bien que les secteurs soient traités distinctement au regard du droit des données personnelles américain, il existe tout de même des obligations concernant les enfants de moins de 13 ans s'appliquant potentiellement à plusieurs secteurs. Il en est de même pour le « Controlling the Assault of Non-solicited Pornography and Marketing Act » (CAN-SPAM Act). Ce dernier vise la régulation de la collecte et de l'usage d'e-mail et couvre tout type de messages à caractère publicitaire.[420] On ne peut légitimement considérer qu'il soit attaché à un secteur économique ou social déterminé. Il est donc parfois erroné de parler d'approche sectorielle de la protection des données personnelles puisque le secteur n'est lui-même pas correctement défini et des incohérences peuvent être soulevées.

Ainsi, et même si les transferts de données personnelles entre les États-Unis et l'Union européenne semblent alors être un champ délimité, ils ne sauraient être considérés valablement comme faisant l'objet d'une approche sectorielle, dès lors qu'il s'agit en réalité d'une approche transversale, bien qu'extrêmement ciblée. En effet, le Privacy Shield a vocation à s'appliquer à tous ces transferts indépendamment du secteur concerné de la même façon que le COPPA protège les données personnelles des enfants de moins de 13 ans indépendamment du reste de la législation américaine, ce qui caractérise également cette approche transversale. Donc la logique est bien celle d'une protection globale, si tant est qu'on lui applique un caractère de transversalité. C'est bien le cas du Privacy Shield puisque toutes les organisations qui veulent

[419] Art. 312.2 Children's Online Privacy Protection Rule ("COPPA").
[420] BOYNE M. (S.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343, p.303.

transférer des données depuis l'Union européenne peuvent utiliser cet outil, peu importe le secteur, du moment qu'elles transfèrent de telles données.

C'est d'ailleurs bien l'absence d'une transversalité suffisante de la loi américaine qui va entre autres empêcher la Commission européenne d'ajouter les États-Unis à la liste blanche des pays fournissant une protection adéquate. En effet, l'article 45 du RGPD dispose que l'évaluation de la Commission se fait notamment sur la pertinence de la législation tant générale que sectorielle.[421] La qualité protective de la législation est quant à elle longuement détaillée par la suite.

Force est de constater que le Privacy Shield véhicule ce caractère global de la législation qui n'est pas assez développé aux États-Unis par l'imposition d'obligations sur le traitement général des données transférées, aux organisations qui se certifient. Le Bouclier de protection doit à ce titre être vu comme une autre pierre à l'édifice de protection des données américaines en ce qu'il impose des règles transversales s'appliquant à tous les transferts de données.

La grande différence est qu'il porte sur les traitements de données directement et non sur des situations amenant au traitement ; c'est en effet un point qu'il s'agit également de distinguer. Le transfert de la donnée, comme mentionné plus haut, est une composante du traitement au même titre que la collecte, le stockage ou la modification par exemple.[422] Il apparaît alors plus aisé de construire une législation globale en se basant directement sur les traitements plutôt que sur les situations qui se rattacheront plus facilement à des secteurs donnés. On peut alors considérer que l'approche globale est également celle qui consiste à se focaliser sur les traitements, indépendamment de leur déclencheur tandis que l'approche sectorielle viserait à appréhender des comportements, des situations, des spécificités dans un secteur donné. En ce sens, on peut donc parler d'une logique de protection globale véhiculée par le Privacy Shield.

Cette même conception tend de plus en plus à être défendue par les acteurs américains du fait que l'accord conditionne le transfert de données au respect des règles qu'il édicte. En effet, si la législation européenne ne prévoyait pas de dispositions encadrant le transfert de données, et était de facto cantonnée au seul territoire de l'Union européenne, l'accord

[421] Art. 45 du RGPD.
[422] Définition du traitement de données à caractère personnel, www.cnil.fr. https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles

n'existerait pas et il n'est pas sûr que les acteurs américains revendiqueraient une quelconque conscience protectrice des données personnelles aux États-Unis.

Quoi qu'il en soit, si l'accord contribue à véhiculer cette conception de protection globale des données, il contribue également à ancrer une certaine rigueur européenne.

B) Des principes empreints d'une rigueur européenne

S'il est d'ores et déjà convenu qu'il ne s'agit pas de trouver cette rigueur européenne dans le degré de protection apporté par le Privacy Shield qui bien qu'elle soit améliorée, reste largement insuffisante au regard des standards européens, on peut toutefois la retrouver dans l'architecture des principes de l'accord. En effet, ce qui frappe à la première lecture de l'accord c'est non seulement la volonté d'avoir voulu faire un texte conciliant deux approches très différentes, mais de conserver tout de même des principes proches dans leurs structures de ceux qui sont énoncés dans la législation européenne.

Ainsi, le principe de notification, comme il a été souligné en première partie reprend des caractéristiques du devoir d'information qui est imposé à un responsable de traitement. Il s'agit notamment d'informer du type de données collectées, des finalités et il faut que cette notification soit faite en des termes clairs et précis. Ces notions de clarté et de précision sont plutôt d'influence européenne. Si le droit européen des données personnelles les a érigés de manière générale, il n'en est pas de même aux États-Unis. Le seul texte en droit américain requérant un devoir d'information équivalent est le COPPA qui régule les traitements de données des mineurs de moins de treize ans. Ce dernier prévoit en effet, que la notification, donc l'information, doit être faite de manière claire et compréhensible et que l'opérateur doit s'assurer par des efforts raisonnables que cette information est communiquée aux parents.[423] Il y a d'ailleurs lieu de s'interroger sur l'influence du droit européen sur le COPPA puisque ce texte a été adopté après l'adoption de la directive européenne de 95 et avant celle du Safe Harbor.[424] D'autres éléments abondent d'ailleurs dans ce sens puisque le même texte prévoit des dispositions explicites relatives aux différents programmes « Safe Harbor ».[425] Ainsi, dans ce texte, on ressent une influence européenne assez forte que ce soit sur les obligations des responsables de traitement, mais également sur les droits des personnes concernées.

[423] Art. 312.4 Electronic Code of Federal Regulations, Titre 16.
[424] *Voir supra P1, Ch.1, Sec.1, §1.*
[425] Art. 312.11 Electronic Code of Federal Regulations, Titre 16.

Ce qui est dès lors certain, c'est que le droit européen accepte bien plus volontiers que le droit américain, la dualité de notions accentuant les obligations à la charge des responsables de traitements, mais accordant également des droits positifs aux personnes concernées. En effet, excepté le texte du COPPA, les autres législations américaines qui incluent une protection des données personnelles sont très hétérogènes aussi bien sur le degré de protection que sur l'angle choisi pour traiter de telles problématiques et bien souvent les droits des personnes sur leurs données sont négligés.

Par exemple, le HIPPA se focalise surtout sur les exigences minimales en matière de confidentialité, d'intégrité et de disponibilité des données de santé que ce soit sur le plan organisationnel que technique notamment.[426] Tandis que le CAN-SPAM Act s'attache plutôt à prévoir des sanctions pénales en cas de collecte massive d'adresses e-mails à des fins de prospection commerciale.[427]

Dès lors, le droit américain en matière de données personnelles semble répondre à des besoins spécifiques dans différents secteurs. Si par exemple, il est reconnu l'importance d'une protection accrue des données de santé, le texte prévoit de facto un encadrement assez strict de la divulgation de ces dernières.[428] C'est donc assez logiquement que le volet de la sécurité organisationnelle et technique protégeant ces données soit abordé dans le texte, le contraire aurait été étonnant. De la même façon, le texte régulant les communications commerciales en se fondant notamment sur les règles encadrant les pratiques déloyales et frauduleuses se devait de résoudre la problématique de la collecte d'adresses mails à des fins de prospection. Il doit donc être dégagé un caractère très hétérogène de ce droit aux États-Unis. Cela explique que certains auteurs américains découpent le « Privacy Law » en trois catégories de lois : la première est la « modality-focused law » et cette dernière a pour but de réguler un seul type de technologie ou d'équipement. C'est donc une réponse directe à une invention ou à une pratique se développant et la régulation porte généralement sur les conditions d'utilisation des données. La deuxième est la « Content-Focused Law », et va plutôt prendre comme paradigme un type de donnée ou un secteur industriel. La dernière est bien sûr la loi protégeant les enfants.[429]

[426] BOYNE M. (S.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343, p.303.
[427] *Ibid.*
[428] Voir à ce titre la section 2713 du « Health Insurance Portability and Accountability Act of 1996 ».
[429] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114.

Il faut donc constater que le droit fédéral américain en matière de données personnelles est chirurgical, se contentant de remplir des cavités juridiques laissées vides par les autres branches du droit. En effet, les problématiques liées aux données personnelles sont le plus souvent réglées sur le terrain du droit de la concurrence, comme en témoigne la forte compétence de la FTC en la matière. Dernièrement, c'est bien l'agence chargée du respect du droit de la consommation et des pratiques commerciales anticoncurrentielles qui, sur le fondement du COPPA, a condamné le réseau social TikTok à une amende de 5,7 millions de dollars, pour défaut de consentement des représentants légaux des enfants, pour la collecte des données et pour refus de supprimer les vidéos et autres données à la demande de certains parents.[430]

Dès lors, cette absence de structure et d'homogénéité qui caractérise le droit américain sur les données démontre que le droit européen a bien contribué à apporter un peu de rigueur juridique au Privacy Shield. En effet, ce dernier reprend dans une version édulcorée les grands principes européens et fournit à l'accord une structure cohérente de la collecte de la donnée jusqu'à son potentiel transfert ultérieur, ce que le droit américain fédéral échoue majoritairement à faire se contentant de combler les vides juridiques existant en matière de données personnelles. C'est d'ailleurs la thèse défendue par une partie de la doctrine américaine qui considère que ce type d'accord contribue à l'apport d'un régime de protection des données aux États-Unis même si, dans les faits, il instaure un régime à deux vitesses.[431]

En ce sens, on peut donc affirmer que le Privacy Shield contribue, à son échelle, à véhiculer une rigueur juridique en matière de données personnelles propre à l'Europe. Cette rigueur est issue d'une éthique en matière des données personnelles plus réfléchie, que les géants américains détournent à leur avantage puisque le transfert de données impose des obligations à leur charge, dans le cadre de l'accord.

II) Les nouvelles éthiques de données personnelles prônées par les GAFA

Il semble qu'un virage à 180 degrés ait été pris par les géants américains du numérique sur la protection des données personnelles. En effet ces derniers qui prônaient jadis la

[430] KANG (C.), « FTC Hits Musical.ly With Record Fine for Child Privacy Violation », www.nytimes.com, publié le 27 février 2019.
https://www.nytimes.com/2019/02/27/technology/ftc-tiktok-child-privacy-fine.html
[431] BERGELSON (V.), « It's Personal but Is It Mine – Toward Property Rights in Personal Information », *University of California Davis Law Review*, volume 37, n°2, Décembre 2003, pp. 379-452.

circulation libre et sans contraintes, se retrouvent à défendre des standards de protection européanistes par nécessité (A) ou par stratégie (B).

A) La défense d'une protection globale et rigoureuse par nécessité : Le cas Facebook

Facebook est sûrement l'entreprise qui a opéré le plus de volte-face médiatiques sur la question de la protection des données. La firme basée à Menlo Park en Californie avait, bien avant les scandales qui l'ont ébranlée, une position sur les données personnelles très éloignée des principes prônés par l'Union européenne, comme en témoignent les déclarations de son PDG pour qui le concept de « Privacy » ne devait plus être considéré comme une norme sociale.[432] En effet, avant le vote du RGPD au Parlement, la directrice des opérations de Facebook qualifiait la future législation de menace critique pour les intérêts de l'entreprise.[433] En 2019, des révélations avaient fait éclater au grand jour, l'intense campagne de lobbying du réseau social aux 2 milliards d'utilisateurs contre les tentatives législatives de protection des données personnelles à travers le monde.[434] Plus important, les révélations démontraient la proximité entre certains cadres de Facebook et l'ancienne première ministre irlandaise Enda Kenny qui aurait proposé l'aide irlandaise afin d'influer en faveur de la firme lors des négociations du RGPD.[435] De plus, à partir de 2015 jusqu'en 2018, des documents internes issus de la Commission européenne ont montré que de nombreuses réunions ont été organisées entre Facebook et des membres de la Commission, afin de communiquer leurs préoccupations sur les lois en préparation les concernant directement et notamment[436] la nouvelle législation européenne sur les données personnelles. Force est de constater que la firme n'était pas favorable à une loi protégeant de manière plus efficace les personnes dont les données sont collectées.

---

[432] DARCY (S.), « Battling for the Rights to Privacy and Data Protection in the Irish Courts », *Utrecht Journal of International and European Law*, volume 31, n°80, 2015, DOI, pp. 131 à 136, p. 131.
[433] CADWALLADR (C.), CAMPBELL (D.), « Revealed : Facebook's global lobbying against data privacy laws », www.theguardian.com, publié le 2 mars 2019.
https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment
[434] *Ibid.*
[435] ANONYME, « De nouveaux documents détaillant le lobbying de Facebook », www.lemonde.fr, publié le 4 mars 2019.
https://www.lemonde.fr/pixels/article/2019/03/04/de-nouveaux-documents-detaillent-le-lobbying-de-facebook_5431071_4408996.html
[436] ANONYME, « Advocates publish European Commission records of Facebook lobbying », www.iapp.org, publié le 24 janvier 2019.
https://iapp.org/news/a/ec-documents-reveal-facebook-pushed-back-against-eu-regulations/

Cependant, l'année 2018 a été cruciale en termes de changement de position de la firme californienne en matière de protection des données et de protection de la vie privée. Il faut dire que cette même année a été éprouvante pour le PDG de Facebook, Mark Zuckerberg. Depuis mars 2018 et le fameux scandale Cambridge Analytica qui s'est d'ailleurs soldé par une amende record de 5 milliards de dollars infligée à l'entreprise par la FTC, pour fuite de données,[437] Facebook a connu d'autres déboires en matière de données personnelles. En septembre 2018, c'est un bug ayant permis à des pirates de subtiliser les données de 29 millions d'utilisateurs,[438] qui touchait le réseau social, et deux mois plus tard, une faille de sécurité avait entrainé l'exposition des photos de 6,8 millions d'utilisateurs.[439] Pour ne rien arranger, le New York Times publiait une enquête le 18 décembre 2018, révélant des partenariats entre Facebook et d'autres grandes entreprises du numérique. Ces derniers avaient pour but de permettre un accès à ces entreprises, dont Netflix, Amazon, Microsoft et Apple, aux données d'utilisateurs.[440]
C'est donc dans sous la pression des médias et dans l'urgence que Facebook a annoncé lors de sa *Keynote* 2019, une approche désormais plus privée du réseau social. À titre introductif comme pour justifier ce qui suivait, Mark Zuckerberg tenait les propos suivants : « *Nous n'avons pas la meilleure réputation sur le sujet en ce moment, pour le dire gentiment* ».[441] De plus, dans un long texte publié le 6 mars 2019, le PDG de Facebook annonçait les grands principes sur lesquels la protection des données et de la vie privée allait s'amorcer. C'est donc avec une volonté en apparence résolument protectrice que le réseau social veut s'afficher auprès de ces quelques 2 milliards d'utilisateurs actifs.

Les six principes énoncés à la manière du Privacy Shield sont : les interactions privées, le chiffrement des communications, la réduction de conservation des communications, la

[437] PIQUARD (A.), « Amende record mais indolore pour Facebook », www.lemonde.fr, publié le 13 juillet 2019. https://www.lemonde.fr/economie/article/2019/07/13/amende-record-mais-indolore-pour-facebook_5488977_3234.html
[438] SZADKOWSKI (M.), « Affaires, failles de sécurité et scandales… 2018 année terrible pour Facebook », www.lemonde.fr, publié le 4 janvier 2019. https://www.lemonde.fr/pixels/article/2019/01/04/2018-annee-terrible-pour-facebook_5404946_4408996.html
[439] SZADKOWSKI (M.), « Facebook : une faille de sécurité a pu exposer les photos de 6.8 millions d'utilisateurs », www.lemonde.fr, publié le 17 décembre 2018. https://www.lemonde.fr/pixels/article/2018/12/17/facebook-une-faille-de-securite-a-pu-exposer-les-photos-de-6-8-millions-d-utilisateurs_5398948_4408996.html
[440] ANONYME, « Facebook : des accès « partenaires » aux données utilisateurs ont été accordés à Apple, Netflix, Spotify, Amazon, Yahoo ! », www.lemonde.fr, publié le 19 décembre 2018. https://www.lemonde.fr/pixels/article/2018/12/19/facebook-des-acces-partenaires-aux-donnees-utilisateurs-ont-ete-accordes-a-apple-netflix-spotify-amazon-yahoo_5399904_4408996.html
[441] LELOUP (D.), « Mark Zuckerberg annonce un virage vers un Facebook plus privée », www.lemonde.fr, publié le 30 avril 2019. https://www.lemonde.fr/pixels/article/2019/04/30/mark-zuckerberg-annonce-un-virage-vers-un-facebook-plus-prive-mais-toujours-plus-integre_5456886_4408996.html

sécurité, l'interopérabilité des services Facebook, et la sécurité de la conservation des données.[442]

Le premier constat est que l'approche de la protection des données retenue est principalement d'ordre technique. En effet, beaucoup de ces principes sont dictés par la volonté de mettre en place des technologies, à l'image du chiffrement bout-en-bout pour garantir le caractère privé des communications, assurant que les données soient sécurisées et détruites au bout d'un certain temps. Même s'il existe implicitement une prise en compte de l'expérience et des intérêts des utilisateurs au travers de la durée de conservation de ce qui est publié, elle semble insuffisante. Facebook doit aller plus loin dans sa volonté de protéger la vie privée et les données des personnes, en instaurant par exemple des interfaces plus explicites et plus transparentes sur la propagation d'une information comme une étude publiée dans le « Ohio State Law Journal » le préconisait.[443] De fait, il serait possible d'informer la personne du caractère sensible de la donnée, qu'elle est sur le point de partager et le cas échéant l'en empêcher.

Par conséquent, on peut regretter qu'il ne soit pas plus question d'un changement dans les politiques de Facebook. En effet, en la matière, on peut simplement noter que l'entreprise s'engage à ne pas conserver de données sensibles dans des pays qui ne respectent pas les droits fondamentaux des personnes.

Cependant, dans la même période, Mark Zuckerberg plaide pour la création d'un RGPD américain dans une tribune au Washington Post.[444] Invoquant la nécessité d'un rôle plus proactif des États, le message paraît donc assez clair puisque si Facebook veut bien assurer la sécurité de son réseau, il se déresponsabilise complètement des problématiques politiques préférant renvoyer ces dernières aux gouvernements et aux législateurs des États tout en proposant cependant son aide et son expertise.

---

[442] ZUCKERBERG (M.), « A Privacy-Focused Vision for Social Networking », www.facebook.com, publié le 6 mars 2019.
https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

[443] WANG (Y.), GIOVANNI (L.), CHEN (X.), SARANGA (K.), NORCIE (G.), SCOTT (K.), ACQUISTI (A.), CRANNOR FAITH (L.), SADEH (N.), « From Facebook Regrets to Facebook Privacy Nudges », *Ohio State Law Journal*, volume 74, n°6, 2013, pp. 1307 à 1334, p. 1334.

[444] ZUCKERBERG (M.), « Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas. », www.washingtonpost.com, publié le 30 mars 2019.
https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html

C'est par nécessité donc que Facebook plaide pour une protection des données plus globale et plus rigoureuse puisqu'il s'agit pour la firme de sauvegarder ses intérêts économiques en suivant la tendance protectrice des données personnelles qui émerge depuis les scandales à son encontre, qui ont ébranlé le monde entier, mais cet intérêt est également insufflé par la création de législations plus protectrices comme le RGPD, et d'outils permettant de garantir un certain niveau de protection dans les transferts de données internationaux dont le Privacy Shield fait partie. En effet, comme il a été étudié, ce dernier permet de véhiculer aux États-Unis des standards de protection européanisés. Indirectement, l'accord transatlantique a donc contribué à un changement de mœurs en matière de protection des données personnelles par les géants américains. Il est cependant à noter que les améliorations, bien qu'existantes, sont limitées à ce qui est nécessaire à Facebook pour redorer son image tandis que la société Apple mène une véritable campagne de protection des données personnelles.

B) La défense stratégique d'une protection globale et rigoureuse : Le cas Apple

Généralement, les géants du numérique ne sont pas par nature enclins à supporter une meilleure protection des données personnelles et de la vie privée ou bien quand ils le font, c'est pour des raisons bien précises qui tiennent au caractère nécessiteux comme il a été démontré pour Facebook. Dans cet écosystème, force est de constater qu'Apple fait figure d'exception. En effet la firme de Cupertino, Californie a développé depuis longtemps une fibre protectrice des données personnelles de ces utilisateurs. En 2014, l'actuel PDG, Tim Cook, se disait outré par le modèle économique de beaucoup de géants du numérique, basé sur la collecte et la vente des données de leurs utilisateurs jugeant que les personnes ont un droit à la vie privée.[445]

À la suite des révélations d'Edward Snowden, Apple par le biais de Tim Cook avait réitéré sa volonté de protéger les données de ses utilisateurs en justifiant le fait que leur modèle économique n'était pas basé sur les données collectées et que de facto le client n'était pas le produit. Un extrait de la lettre publiée annonçait que :

> « Notre modèle économique est très simple : nous vendons d'excellents produits. Nous ne construisons pas un profil basé sur le contenu de vos emails ou sur vos habitudes de recherches sur internet afin de les vendre à des annonceurs. Nous ne "monétisons" pas

[445] EDWARDS (J.), « Tim Cook Basically Just Said He Was 'Offended' By The Way Google And Amazon Do Business », www.businessinsider.fr, publié le 16 septembre 2014. https://www.businessinsider.com/tim-cook-is-offended-by-how-google-and-amazon-do-business-2014-9

> les informations que vous stockez sur votre iPhone ou sur l'iCloud. Et nous ne lisons pas vos emails ou messages pour obtenir des informations pour vous démarcher. Nos logiciels et services sont conçus afin d'améliorer nos appareils. […] Enfin, je veux être absolument clair sur le fait que nous n'avons jamais travaillé avec aucune agence gouvernementale de quelque pays que ce soit afin de créer un accès caché sur aucun de nos produits ou services. De la même façon, nous n'avons jamais autorisé d'accès à nos serveurs. Et nous ne le ferons jamais. »[446]

Si cette citation de la lettre ouverte du PDG d'Apple illustre la politique de protection des données personnelles de la firme, la deuxième partie de la citation est une réponse directe aux griefs faits aux géants américains sur les accès à leurs serveurs par les agences de renseignements américaines et notamment la NSA, mis en lumière en 2013 par Edward Snowden.

C'est d'ailleurs dans la continuité de préservation de son image de défenseur de la vie privée de ses utilisateurs que le géant américain s'est déjà opposé à des mandats visant l'accès à des appareils de la marque dans le cadre du « All Writs Act ». En Octobre 2015, le gouvernement américain avait déjà saisi l'« U.S. District Court for the Eastern District of New York », afin d'obtenir un accès au téléphone d'un suspect dans le cadre d'un trafic de drogue. Apple avait refusé de s'y soumettre, plaidant alors notamment le dommage commercial et réputationnel ainsi que l'impossibilité d'obtenir les informations. La cour rejette alors les prétentions du gouvernement au motif que la demande d'assistance prévue dans le « All Write Acts » ne trouve pas à s'appliquer dans ce cas.[447] C'est la première victoire judiciaire d'Apple en matière de protection des données de ses utilisateurs.

La deuxième affaire à quelques mois d'intervalle a été bien plus médiatisée. En effet à la suite de la fusillade de San Bernardino survenue le 2 décembre 2015, une cour fédérale de Californie ordonne à la firme d'assister le FBI, en permettant l'accès à l'iPhone d'un des tireurs.[448] Apple, par la voix de son PDG, publie un communiqué sur le refus de l'entreprise de

---

[446] Traduction de la lettre de Tim Cook disponible sur l'article suivant : COLT (S.), « Tim Cook Has An Open Letter To All Customers That Explains How Apple's Privacy Features Work », www.businessinsider.fr publié le 18 septembre 2014.
https://www.businessinsider.com.au/tim-cook-published-a-letter-on-apple-privacy-policies-2014-9
[447] United States District Court, Eastern District of New York, *Affaire 1:15-mc-01902-JO (E.D.N.Y.)* du 17 février 2016, Apple c/ The U.S Government.
[448] POLLACK C. (M.), « Taking Data », *University of Chicago Law Review*, volume 86, n°1, January 2019, pp. 77 à 141, p. 78.

se conformer à l'ordonnance de la Cour.[449] Selon Tim Cook, le risque d'atteinte à la vie privée et la sécurité de millions d'Américains est trop grand, puisque se conformer à cette ordonnance est synonyme d'utilisation systématique par le gouvernement américain. Mais le risque est potentiellement plus global puisque Apple fournissant un service international, cela signifierait un accès territorialement illimité.[450] Finalement, le FBI notifie à la Cour qu'il a réussi à accéder aux données sur le téléphone et que par conséquent l'aide d'Apple n'est plus nécessaire.[451]

Évidemment, il s'agit pour la firme à la pomme de conserver sa posture de défenseur de la vie privée de ses utilisateurs afin de préserver sa réputation et de facto, d'éviter des retombées économiques et financières négatives.[452] Mais il s'agit également de se démarquer sur le marché et de pouvoir distancer ses concurrents directs. En effet, si les utilisateurs des services en ligne prennent de plus en plus au sérieux l'utilisation faite de leurs données, ils ne croient pas que les entreprises puissent garder leurs données en sécurité. C'est ce qu'a révélé une étude américaine dans laquelle 93 % des sondés accordent de l'importance à qui possède leurs données et au contrôle qu'ils peuvent exercer. Cependant, seulement 9 % d'entre eux sont confiants envers les entreprises concernant l'utilisation de leurs données.[453] Cet aspect du marché n'est donc pas à négliger et Apple l'a bien compris. Cela est également une des raisons pour lesquelles Apple défend une protection plus forte des données personnelles, étant donné que la firme dépend moins de ces dernières que ses concurrents directs. En effet, Apple vend avant tout des appareils et des services et ne fonde pas son modèle économique sur l'exploitation commerciale de données de ses utilisateurs qui est une activité secondaire.

C'est donc logiquement qu'à la suite du scandale de Cambridge Analytica, Tim Cook a réitéré à la fin de 2018, à la 40e conférence des commissaires à la protection des données et de la vie privée, à Bruxelles, sa volonté de protéger les données. Il s'est notamment dit favorable à la création d'une législation américaine similaire au RGPD.[454] Quelques mois plus tard, il

---

[449] COOK (T.), « A Message to Our Customer », https://perma.cc/68X7-SDLL (archivage), publié le 16 février 2016.
[450] BAUER L. (J.), « Playing Off-Key: Trans-Atlantic Data Regulation in a discordant World », *West Virginia Law Review*, volume 119, n°2, Hiver 2016, pp. 793 à 828, p. 794.
[451] United States Court for the Central District of California, *Affaire 5:16-cm-00010-SP (C.D. Cal.)* du 28 mars 2016, Apple c/ The U.S Government.
[452] ASTA A. (T.), « Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions », *Florida State University Law Review*, volume 45, n°1, automne 2017, pp. 261. à 312., p. 301.
[453] *Ibid.*
[454] AFP, « Le patron d'Apple défend à Bruxelles l'idée d'une loi américaine sur les données personnelles », www.lemonde.fr, publié le 24 octobre 2018. https://www.lemonde.fr/pixels/article/2018/10/24/le-patron-d-apple-defend-a-bruxelles-l-idee-d-une-loi-americaine-sur-les-donnees-personnelles_5373982_4408996.html

signait une tribune dans le *Time Magazine* appelant le Congrès américain à agir en faveur d'une telle législation. Ainsi il défend un idéal législatif selon lequel les entreprises doivent s'enregistrer auprès de la FTC. Le but étant de permettre à tout utilisateur un droit d'accès et le cas échéant de rectification ou de suppression.[455]

Cet idéal rappelle quelque peu le système de déclaration préalable prévu par la directive de 95 et qui avait été un échec partiel par manque de moyens de contrôle notamment. Mais cette idée rappelle aussi et surtout le mécanisme d'autocertification prévu par le Privacy Shield et le Safe Harbor avant lui. En effet, il s'agit ici pour les entreprises de s'engager à respecter des obligations, notamment dans l'accès aux droits des personnes dont les données sont collectées. À défaut, on peut imaginer que le traitement serait illégal, comme le transfert de données depuis l'Europe à destination des États-Unis est réputé illégal s'il a lieu en dehors des mécanismes prévus, dont le Privacy Shield. Preuve en est donc que cet accord si imparfait soit-il, est source d'inspiration pour les acteurs américains désireux de s'inspirer d'un modèle législatif européaniste, pour mettre en place une législation en la matière, propre aux États-Unis.

Cette inspiration des principes véhiculés par la législation européenne incluant le Privacy Shield a contribué à une amélioration de la protection légale des données aux États-Unis.

[455] ANONYME, « Le patron d'Apple s'attaque aux revendeurs de données personnelles », www.lemonde.fr, publié le 17 janvier 2019.
https://www.lemonde.fr/pixels/article/2019/01/17/le-patron-d-apple-s-attaque-aux-revendeurs-de-donnees-personnelles_5410687_4408996.html

Section 2 : Une amélioration de la protection légale sur les données personnelles aux États-Unis

Cette amélioration se traduit par l'apparition de nouvelles pousses législatives américaines (I), mais également par la direction prise d'une convergence de définition de la donnée personnelle entre les États-Unis et l'UE (II).

I) Les nouvelles pousses législatives américaines

Ensemble, les différents scandales en matière de données personnelles, la règlementation européenne et le Privacy Shield auront contribué sans aucun doute au développement législatif américain en matière de protection des données. Ainsi, la Californie s'est dotée en 2018 d'une législation influencée par la conception européenne (A), mais on évoque de plus en plus un « RGPD » à l'américaine en cours de préparation (B).

A) La législation californienne : symbole de l'influence de la conception européenne

À titre liminaire, il faut souligner qu'aux États-Unis, la Californie a toujours été pionnière voire avant-gardiste en matière de protection des données personnelles. En effet, la première règlementation en matière de vie privée en Californie date de 2003 et est entrée en vigueur début 2004. Cette loi est le « California Online Privacy Protection Act » (CalOPPA)[456] qui influencera ensuite d'autres lois en la matière dans plusieurs États.[457] Ce texte précurseur impose à toute personne physique ou morale collectant des données de résidents californiens, via un site internet ou un service en ligne, pour des finalités commerciales, d'identifier les différentes catégories de données collectées sur les utilisateurs, d'identifier les tiers avec qui les données sont susceptibles d'être partagées, et de publier une politique de confidentialité compréhensible et accessible sur le site internet ou dans le cadre du service en ligne.[458] Mais la Californie ne s'est pas arrêtée en si bon chemin dans sa quête de protection de la vie privée et des données de ses résidents. Le 1er janvier, le « California Electronic Communications Privacy Act » (CalECPA) entre en vigueur. Ce texte constitue un volet important de la protection des

[456] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 89.
[457] BOYNE M. (S.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343, p. 309.
[458] Art. 22575 à 22578 California Business & Professions Code.

données des Américains puisqu'il concerne un champ plutôt inhabituel aux États-Unis qui est celui de l'accès aux communications privées par des entités gouvernementales.[459] Ce texte vient renforcer en Californie la protection des communications privées, régie à l'échelle fédérale par l'« Electronic Communications Privacy Act » de 1986, en ajoutant des obligations d'information à la personne ciblée et désormais, c'est l'appareil électronique en lui-même qui est protégé par la condition du mandat et plus seulement la communication en cause.[460]

De plus, l'État ouest-américain s'est doté d'un texte interdisant aux opérateurs collectant des données d'écoliers K-12,[461] d'utiliser, de vendre, de diffuser ou de faire du profilage à partir de ces données.[462] Ce texte cible spécifiquement les opérateurs en ligne dont les sites, services ou applications sont utilisés à des fins scolaires.[463]

Dans la continuité de cette volonté de protection des données, la Californie s'est récemment dotée d'un texte qui sous les projecteurs médiatiques a beaucoup été comparé au RGPD. En 2018, le gouverneur de Californie Jerry Brown a signé le « California Consumer Privacy Act ». Ce texte a une double portée juridique et sociale puisqu'en premier lieu il s'agit du texte le plus transversal en matière de données personnelles qui existe aux États-Unis à l'heure actuelle. En second lieu, il s'agit aussi d'une émanation de la prise de conscience des Américains sur la nécessité de protéger leurs données, mais également de contrôler l'utilisation qui en est faite. En effet, le texte intervient juste après l'affaire Cambridge Analytica et les auditions du PDG de Facebook devant le Congrès américain.[464]

Le texte qui a vocation à protéger les consommateurs californiens va concerner toute entité faisant du profit et remplissant au moins l'une des trois conditions suivantes : il faut que les revenus annuels bruts soient d'au moins 25 millions de dollars ; ou qu'elle achète, vende, reçoive, ou partage pour des finalités commerciales, des données personnelles d'au moins 50 000 consommateurs, familles, ou appareils électroniques ; ou dégage au moins 50 % de ces revenus annuels de la vente des données personnelles des consommateurs.[465] Il est à noter que

[459] FREIWALD (S.), « At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA) », *Berkeley Technology Law Journal*, volume 33, n°1, 2018, pp. 131 à 176.
[460] *Ibid.*
[461] Signification : les écoliers de Kindergarten à partir du 1er grade jusqu'au 12e grade.
[462] Art. 22584 et 22585 California Business & Professions Code.
[463] MCGRATH P. (K.), « Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act », *University of California Davis Law Review*, volume 49, n°3, février 2016, pp. 1149 à 1181, p. 1152.
[464] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 71.
[465] Art. 1798.140 California Civil Code.

le texte prévoit également un élargissement du champ d'application aux entités contrôlant ou étant contrôlées par une autre[466], ce qui signifie l'exclusion de stratégies de cloisonnement de l'activité par de grosses structures afin d'échapper à la règlementation. Le consommateur lui est défini comme une personne physique résidant en Californie.[467] Mais ce qui est intéressant dans ce texte, c'est la définition de « l'information personnelle ». Ainsi, c'est : « une information qui identifie, qui se rapporte à, qui décrit, qui est susceptible d'être associé à, ou qui peut raisonnablement être liée, directement ou indirectement à une personne ou une famille. »[468] Cependant sont exclues les informations personnelles dites « publiquement disponibles », c'est-à-dire les informations détenues et disponibles depuis des registres fédéraux, d'État ou locaux.[469] La section suivante exclut du champ d'application du texte les types de données qui rentrent dans le champ d'un texte fédéral ; c'est le cas par exemple du HIPPA.[470]

Le texte prévoit des droits actifs pour les consommateurs désireux de contrôler l'usage qui est fait de leurs données. Ainsi, le consommateur bénéficie d'un droit de connaître les données collectées à son sujet. Il peut s'opposer à la vente de ses informations personnelles puisque le texte impose à toutes les entités concernées d'obtenir le consentement du sujet pour procéder à la vente de ses données. Le résident californien dispose également d'un droit d'effacement.[471]

Plus classiquement, on retrouve un droit à l'information du consommateur qui peut être qualifié de passif puisqu'il s'agit d'obligations mises à la charge de l'entité concernée sous la forme de publication d'une politique de confidentialité.[472] Afin de satisfaire aux droits d'information du consommateur, elle doit contenir les catégories de données collectées afin que la personne soit informée avant ladite collecte, les catégories de tiers avec lesquels les données personnelles sont partagées, les catégories de sources d'information via lesquelles les données personnelles ont été obtenues et l'objet commercial de la collecte. De plus, une personne a le droit d'intenter une action en justice si toutefois il était prouvé que l'entité ne respecte pas ses

[466] *Ibid*.
[467] *Ibid*.
[468] *Ibid*.
[469] *Ibid*.
[470] Art. 1798.145 California Civil Code.
[471] GERRISH (C.), APTEL (P.), « Le « California Consumer Privacy Act » : un timide RGPD américain ? », www.village-justice.com, publié le 10 juillet 2018.
https://www.village-justice.com/articles/california-consumer-privacy-act-timide-rgpd-americain,28977.html
[472] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 89

obligations.[473] Cependant, le texte ne vise que les violations résultant de mesures de sécurité.[474] La nouvelle loi californienne reprend donc certaines dispositions du devoir d'information prévues par le CalOPPA, mais en crée majoritairement de nouvelles. En ce sens, le texte va plus loin dans la protection des données des Californiens.

Concernant, le consentement à la vente des données personnelles, ce dernier doit faire l'objet d'une procédure d'opt-out à partir d'un lien internet intitulé « Do Not Sell My Personal information »[475] et cette procédure doit être accompagnée d'une description des droits du consommateur.[476] Il semblerait cependant que ce mécanisme soit facilement contournable par les entreprises, puisque si la vente de données est soumise au consentement, il n'en est pas de même pour le partage de données avec un tiers.[477] De plus, les entreprises peuvent vendre des biens ou des services à des prix plus élevés, aux consommateurs qui auraient refusé la vente de leurs données, sur le fondement des répercussions de ce refus sur la valeur du bien ou du service.[478] Reste alors une interrogation à laquelle devront répondre les juges quant à savoir dans quels cas la valeur du bien ou du service peut se trouver altérée par le refus du traitement des données.

Dans sa structure et ses dispositions, on peut aisément constater que cette loi se distingue du droit américain en ce qu'elle donne le contrôle à l'individu sur les données personnelles le concernant, plutôt que d'imposer simplement une plus grande transparence aux acteurs les collectant, ou en se bornant à imposer de simples obligations sécuritaires.[479]

En ce sens, les observateurs ont souvent rapproché ce texte de la législation européenne. Cependant, il serait erroné d'affirmer que ce texte reprend des dispositions similaires au RGPD même à des fins de vulgarisation.[480] S'il faut reconnaître que ce texte est d'influence

---

[473] GERRISH (C.), APTEL (P.), « Le « California Consumer Privacy Act » : un timide RGPD américain ? », www.village-justice.com, publié le 10 juillet 2018.
https://www.village-justice.com/articles/california-consumer-privacy-act-timide-rgpd-americain,28977.html
[474] DE LA TORRE (L.), « GDPR matchup : The California Consumer Privacy Act 2018 », www.iapp.org, publié le 31 juillet 2018.
https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/
[475] *Ne vendez pas mes données personnelles.
[476] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 99
[477] GERRISH (C.), APTEL (P.), « Le « California Consumer Privacy Act » : un timide RGPD américain ? », www.village-justice.com, publié le 10 juillet 2018.
https://www.village-justice.com/articles/california-consumer-privacy-act-timide-rgpd-americain,28977.html
[478] *Ibid.*
[479] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 89.
[480] Dans cet article l'auteur parle de règles similaires ce qui est à éviter : MARIN (J.), « La Californie vote une loi sur la protection des données », www.lemonde.fr, publié le 29 juin 2018.

européenne, le paradigme sur lequel il est basé n'est pas le même puisque l'on est toujours dans une optique de plébisciter la libre circulation des données, au détriment de la reconnaissance d'un droit fondamental à la protection des données personnelles comme il peut exister en droit européen.[481] Cette différence de paradigme qui était déjà établie au moment de l'entrée en vigueur de la directive de 95,[482] persiste encore aujourd'hui. De facto, l'esprit de la loi étant différent, on ne peut dès lors pas parler de dispositions similaires. D'ailleurs, les dispositions prévues sont tout de même assez éloignées de la rigueur du RGPD que ce soit sur les droits conférés à la personne concernée, les obligations à la charge de l'entité ou encore leur champ d'application.

Ainsi, l'esprit de la loi californienne serait plutôt à rechercher du côté du Privacy Shield. En effet, c'est le seul texte juridique qui combine réellement les deux conceptions européenne et américaine. Et, à y regarder de plus près, ce sont plutôt des principes de notification, de choix et d'accès prévus au titre de l'accord transatlantique, que le texte semble se rapprocher. À titre d'exemple, la procédure d'opt-out du consentement prévue par le texte américain sur la vente de données reprend les mêmes conditions de clarté, de précision et de facilité d'accès que le Privacy Shield en ce qui concerne la transmission de données à un tiers, sans s'encombrer de la lourdeur de la législation européenne en matière de consentement.[483] Il y a donc évidemment une influence européenne tout en gardant un esprit américain marqué, comme c'est d'ailleurs le cas pour le Privacy Shield.

Il est à noter tout de même que le texte qui doit enter en vigueur début 2020 est encore susceptible d'être amendé, et les géants du numérique américains basés pour la majeure partie d'entre eux en Californie risquent bien d'exercer des pressions afin d'obtenir un texte final à leur avantage.[484]

Bien que l'État doré soit pionnier en matière de protection des données personnelles, une législation fédérale serait en préparation.

---

https://www.lemonde.fr/pixels/article/2018/06/29/la-californie-vote-une-loi-sur-la-protection-des-donnees_5322856_4408996.html

[481] Art. 8 de la Charte des droits fondamentaux de l'Union européenne.

[482] MONAHAN A (P.), « Deconstructing information Walls: The impact of the European Data Directive on U.S Businesses » *Law & Policy in International Business*, volume 29, 1998, pp. 275 à 277.

[483] Art. 7 du RGPD.

[484] PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114, p. 102.

B) Un RGPD américain en préparation ?

Bien que le sujet soit revenu en force ces derniers mois du fait de l'adoption et de l'entrée en vigueur du RGPD ainsi que des scandales concernant les données de millions de personnes, l'idée d'une législation américaine globale sur la protection des données n'est pas nouvelle. En effet, on retrouve dans la doctrine américaine plusieurs auteurs soutenant la mise en place d'une telle législation autour de 2010 avant même les révélations d'Edward Snowden. Si certains plaident pour un texte n'imposant qu'une obligation de notification et plus particulièrement en cas de failles ou de violations des données,[485] d'autres arguent en faveur de règles globales d'influence européenne afin de satisfaire aux exigences de la Commission en matière d'adéquation et de pouvoir accéder à la liste blanche des transferts de données hors de l'Union européenne.[486] Cela montre d'ailleurs à quel point la légalité du transfert de données depuis l'Union européenne vers les États-Unis est importante. D'autres soulèvent le fait que la législation américaine en la matière est devenue indigeste par le chevauchement de différentes lois fédérales et d'États, mais également que la protection des données est devenue trop dépendante du droit de la concurrence et de la consommation utilisés pour réguler l'économie alors que c'est avant tout la protection de l'individu qui doit primer.[487]

De plus, l'administration Obama avait déjà tenté de préparer le terrain pour une législation globale américaine en publiant le « Privacy Bill of Rights » en 2012 qui appelait les entreprises à plus de transparence et à redonner le contrôle de leurs données aux personnes concernées.[488] Mais du fait du lobbying de la part des grandes entreprises du numérique, un tel texte n'a jamais été à l'étude devant le Congrès américain.[489]

Du fait du scandale de Cambridge Analytica notamment, l'idée d'un RGPD à l'américaine est revenue sur le devant de la scène. En effet, le congrès a même soulevé la question pendant l'audition du PDG de Facebook, Mark Zuckerberg quand le sénateur de la

[485] JOERLING (J.), « Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data. » *Washington University Journal of Law and Policy*, volume 32, n°1, 2010, pp. 467-488.
[486] BORDER C. (A.), « Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States », *Suffolk Transnational Law Review*, volume 35, n° 2, été 2012, pp. 363-392.
[487] BALABAN L. (T.), « Comprehensive Data Privacy Legislation: Why Now is the Time? », *Case Western Reserve Journal of Law, Technology & the Internet*, volume 1, n°1, automne 2009, pp. 1-35.
[488] Communiqué de presse de la Maison Blanche du 23 février 2012, « We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online ».
[489] ROMM (T.), « The Trump Administration is talking to Facebook and Google about potential rules for online privacy », www.washingtonpost.com, publié le 27 juillet 2018.
https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/

Caroline du Sud, Lindsey Graham lui avait demandé si les Européens avaient eu raison, en référence au règlement européen sur la protection des données.[490] Cette idée a d'ailleurs été confirmée puisque des réunions entre le ministère du Commerce américain et les géants du numérique ont été organisées afin de publier une première esquisse d'une protection globale des données.[491] Cette initiative trouve notamment son origine dans le sillage du texte qui a été adopté par la Californie à l'été 2018 et devrait par conséquent être influencée par la législation européenne tout en gardant la libre circulation des données intacte.

Cependant, rien n'a encore filtré quant au contenu d'une telle loi et il est de mise de rester prudent sur le sujet puisqu'il n'y aucune certitude sur les dispositions qui vont garnir le texte aussi bien sur l'effectivité du contrôle des citoyens américains sur les données collectées les concernant que sur l'existence de droits effectifs ou bien d'obligations à la charge des entreprises. On ne sait pas non plus quel sera son champ d'application. En l'espèce, celui qui nous intéresse est plutôt le champ d'application matériel puisqu'il sera crucial d'inclure les entités publiques collectant des données. En effet, aucune disposition aux États-Unis ne vise à protéger effectivement les personnes dont les données sont traitées par une entité gouvernementale. Cela sera d'ailleurs la clé de la décision de la Commission européenne concernant la protection adéquate des données personnelles aux États-Unis. Il semblerait cependant que comme pour la loi californienne, une protection dans le cadre d'une relation « Business To Consumer » soit plutôt privilégiée.[492]

Beaucoup de points restent alors à définir. Qu'ils s'agissent du champ d'application matériel jusqu'à la compétence de la FTC comme autorité de régulation, il faudra tout de même rester cohérent. En effet, il serait difficilement justifiable d'étendre le champ d'application à toutes les organisations publiques ou privées et de déléguer toute la compétence à la FTC dont on sait que son champ de compétence est limité principalement aux problèmes de concurrence et de protection du consommateur. D'autres inconnues doivent être résolues telles que le droit d'action privée, les modalités de son ouverture, ainsi que les sanctions attenantes. Enfin, il

[490] NOACK (R.), « One key question for Zuckerberg: Will Americans become second class citizens? », www.washingtonpost.com, publié le 10 avril 2018.
https://www.washingtonpost.com/news/worldviews/wp/2018/04/10/could-european-privacy-rules-save-facebooks-zuckerberg-from-a-senate-grilling/
[491] ROMM (T.), « The Trump Administration is talking to Facebook and Google about potential rules for online privacy », www.washingtonpost.com, publié le 27 juillet 2018.
https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/
[492] *Ibid.*

faudra définir la donnée personnelle, puisque la définition est très hétérogène, selon le texte auquel on se réfère.[493]

Il est également à noter que plusieurs propositions de loi ont déjà été déposées devant le Congrès ou bien seulement dévoilées.[494] Si leurs auteurs visent majoritairement les opérateurs de service en ligne ou parfois plus globalement toutes les organisations, dont l'activité, se trouve sous la compétence de la FTC, aucune de ces propositions n'aborde le traitement des données personnelles par des personnes morales de droit public, ce qui est regrettable dans la quête d'un « RGPD à l'américaine ». Certaines de ces propositions vont plus loin dans les exigences mises à la charge des organisations, et des missions conférées à l'autorité de régulation. En effet, certaines prônent un triptyque classique réunissant les obligations de transparence, les droits des consommateurs et les obligations en matière de sécurité dont le contrôle serait assuré par la FTC[495], tandis que d'autres qui font la distinction entre les données sensibles et les autres données plaident pour un consentement par une procédure d'opt-in pour tout ce qui concerne le traitement de données sensibles.[496] Ces propositions prévoient cependant toutes des dispositions différentes qu'il ne convient pas d'étudier en détail, mais qu'il convient tout de même de mentionner, puisqu'elles ont commun la volonté d'une législation globale sur la protection des données personnelles aux États-Unis. Un autre point commun qu'elles partagent est l'influence européenne dont elles sont empreintes. Une chose est certaine, l'influence européenne est bien présente aux États-Unis dans cette branche du droit. Toutes ces pousses législatives américaines abondent dans le sens du caractère politique du Privacy Shield. On retrouve en effet les mêmes clivages dont il a été question lors des négociations entre l'Union européenne et les États-Unis, mais cette fois à la seule échelle américaine. En effet, on ne peut pas nier que la bataille se situe politiquement encore une fois quelque part entre la protection des personnes concernées et la volonté très forte de ne pas entraver l'économie. C'est d'autant plus vrai que le statut de la donnée est lentement en train de changer outre-Atlantique.

---

[493] CEDARBAUM G. (J.), FREEMAN JR (R.), LICHLYTER (L.), « United States: Congress Begins Consideration of Comprehensive Federal Privacy Legislation », www.mondaq.com, publié le 21 février 2019. http://www.mondaq.com/unitedstates/x/783634/Data+Protection+Privacy/Congress+Begins+Consideration+of+Comprehensive+Federal+Privacy+Legislation

[494] *Ibid.*

[495] Consumer Data Protection Act, SIL18B29, proposé par le sénateur de l'Oregon, R. Wyden.

[496] Consumer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT Act), S. 2639/H.R. 5815, proposé par le sénateur du Massachussets E. Markey.

II) Vers une convergence de définition de la donnée personnelle entre les États-Unis et l'UE

Bien qu'il existe une différence conceptuelle originelle de la donnée personnelle entre les États-Unis et l'Europe (A), on assiste à un changement de définition outre-Atlantique ce qui aurait une influence sur l'application du Privacy Shield (B).

A) La différence de conception originelle de la donnée personnelle aux États-Unis et en Europe

Au-delà de la différence de philosophies européenne et américaine dans la manière de légiférer pour faire face à des problématiques de données personnelles, il s'agit également d'étudier les différences qui tiennent à la définition même de la donnée personnelle. Ces différences peuvent poser des problèmes en matière de transfert de données transatlantiques puisque dès lors la lecture que l'on fait du Privacy Shield est biaisée. En effet, bien que contenant sa définition de la donnée personnelle, l'accord semble tout de même souffrir du manque d'homogénéité juridique transatlantique sur le sujet. Cela contribue à accentuer le caractère politique de l'accord puisqu'il ne s'agit pas de concilier des définitions juridiques, mais plutôt de défendre des intérêts, quels qu'ils soient, en procédant à des compromis de part et d'autre. En effet, si la définition de la donnée prévue par le Privacy Shield renvoie fortement à la législation européenne, beaucoup d'incertitudes planent sur la véritable valeur juridique de l'accord et donc sur la légitimité de cette définition en droit américain.

Le RGPD définit la donnée à caractère personnel comme :

> « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; »[497]

[497] Art. 4 du RGPD.

La première différence réside dans la référence concrète à une personne physique identifiable en droit européen, qui n'est jamais mentionnée en droit fédéral américain.[498] Ainsi, l'approche généraliste du droit américain se borne dans le meilleur des cas à définir l'information personnelle comme l'information qui identifie une personne[499], mais la personne en soi n'est jamais définie. Ce problème a d'ailleurs déjà été mentionné par des auteurs américains qui considéraient que cette approche revenait à définir l'information personnelle identifiable comme l'information personnelle identifiable sans savoir à quoi elle renvoyait concrètement.[500]

Cela nous amène à la deuxième différence cruciale de la définition de la donnée personnelle. Le vieux continent s'est doté d'une seule définition de la donnée personnelle, ce qui permet de clarifier la législation. Outre-Atlantique, ce sont bien une multitude de définitions de l'information qui ont été adoptées et toutes ces définitions sont très disparates selon la loi dans laquelle elles sont incluses. Dans un souci de clarté, nous reprendrons dans ce développement la catégorisation des définitions de la donnée personnelles, telle qu'elle a été théorisée par les auteurs américains, Paul Schwartz et Daniel Solove dans un article de 2012 paru dans la revue « New York Law Review ».[501] Cette classification se divise en trois catégories :

La première est l'approche tautologique de la donnée personnelle. C'est celle qui a été donnée plus haut et qui est tirée du « Video Privacy Protection Act » de 1988. Cette approche de la donnée personnelle n'est pas une définition acceptable dans le sens où elle est très incomplète, mais elle a le mérite d'être ouverte et d'accueillir des évolutions sémantiques.[502]

La deuxième est l'approche dite non publique. Il s'agit ici de raisonner a contrario. On considère que toutes les données qui ne sont pas publiques sont personnelles. C'est l'approche retenue dans le « Gramm-Leach-Bliley Act » du 12 novembre 1999 qui a instauré les services de banque universelle permettant d'assurer les services de banque de dépôt, d'investissement et de compagnie d'assurance. Cette définition est également très imparfaite, car le concept

[498] BOYNE S. (M.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343.
[499] Art. 2710 Video Privacy Protection Act of 1988, U.S.C. titre 18 (2006).
[500] SCHWARTZ M. (P.), SOLOVE J. (D.), « PII 2.0: Privacy and a New Approach to Personal Information », *Privacy & Security Law Report*, volume 11, novembre 2012 p. 142.
[501] SCHWARTZ M. (P.), SOLOVE J. (D.), « The PII Problem: Privacy and a New Concept of Personally Identifiable Information », *New York University Law Review*, volume 86, n°6, décembre 2011, pp. 1814-1894.
[502] *Ibid*.

d'identification n'est pas retenu. Donc une donnée permettant clairement d'identifier une personne ne serait pas personnelle, si elle est publique.[503]

La troisième approche des données personnelles par le droit américain est l'approche des types spécifiques de données. Ici, il s'agit d'énumérer des catégories de données qui seront considérées comme personnelles au sens de la loi.[504] Par exemple, le COPPA prévoit que les données personnelles au sens du texte sont les noms, les adresses, les numéros de sécurité sociale, les numéros de téléphone et les adresses e-mails.[505] On se retrouve donc avec une définition très restreinte et cantonnée à certains types de données alors que le responsable de traitement peut potentiellement collecter d'autres données qui ne seront pas considérées comme personnelles puisqu'elles ne sont pas mentionnées par le texte.

Il y a donc un double problème auquel le droit américain peine à répondre. Le premier est que la multitude de définitions, toutes façonnées pour les besoins spécifiques de tel ou tel secteur, ce qui par ailleurs semble logique au regard de l'approche sectorielle retenue, entraine un manque de clarté du droit sur ce qu'est concrètement une donnée personnelle. Il faut par définition d'abord identifier quel texte de loi s'applique à une situation pour savoir ce qui sera susceptible d'être considéré comme étant personnel. Le deuxième problème est que ces définitions sont tantôt larges et tantôt restreintes, ce qui semble très inégalitaire dans la protection des citoyens américains. En effet, ce qui sera considéré comme étant une donnée personnelle par un texte, ne le sera pas par un autre ce qui ferme potentiellement les droits d'action ou ce qui supprime les obligations à la charge des organisations traitant des données qui sont par essence personnelles, mais simplement pas reconnues comme telles.

Finalement, cette difficulté américaine à définir la donnée peut grandement s'expliquer par le tiraillement entre la protection des données et la libre circulation des données. Certains auteurs considèrent même que trop de protection mènerait à une loi inconstitutionnelle[506] ; en effet, ils considèrent que la circulation de l'information doit être attachée à la liberté d'expression, garantie dans le premier amendement de la constitution américaine et que par conséquent, protéger les données reviendrait à porter atteinte à cette liberté ce qui entrainerait l'inconstitutionnalité de la loi.[507] Il en résulte donc que la protection de la donnée personnelle

[503] *Ibid*.
[504] *Ibid*.
[505] Art. 6501.8 Children's Online Privacy Protection Act of 1998.
[506] VOLOKH (E.), « Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You », *Stanford. Law Review*, volume 52, 2000, pp. 1049 à 1122.
[507] BERGELSON (V.), « It's Personal but Is It Mine – Toward Property Rights in Personal Information », *University of California Davis Law Review*, volume 37, n°2, décembre 2003, pp. 379-452.

est limitée par ce qui est considéré ou non comme personnel et qu'une définition trop large par la loi entrainerait des batailles politiques et juridiques importantes.

Dès lors, le Privacy Shield se situe dans une zone grise entre l'Union européenne et les États-Unis en ce qui concerne la définition même de la donnée, puisque si cette définition respecte les standards européens, elle se heurte aux pratiques juridiques américaines en la matière. Il y a donc lieu de considérer que cette différence conceptuelle de la notion de donnée personnelle a pour conséquence que le Privacy Shield ne peut pas être un outil juridique efficace et qu'il existe simplement pour répondre à des attentes d'ordre politique et économique. On lui reproche d'ailleurs souvent outre-Atlantique sa trop grande différence avec le droit américain.[508]

Cependant, la définition de donnée personnelle aux États-Unis est en train de changer, ce qui pourrait contribuer à rendre le Privacy Shield juridiquement plus efficace.

B) Privacy Shield et changement de définition de la donnée aux États-Unis

On assiste aux États-Unis à un réveil collectif sur la nécessité de protéger la vie privée et de reprendre le contrôle sur ses données. Une partie de la doctrine avait déjà cerné l'importance de redessiner les bases du droit des données personnelles américain. Sans surprise, c'est la définition de donnée personnelle qui a été revue. Ainsi, plusieurs auteurs ont proposé des pistes de redéfinition, mais la plus aboutie est bien celle du passage de la « Personally identifiable information » à la « Personally identifiable information 2.0 » dans l'article commun de 2012 de Paul Schwartz et Daniel Solove. Ainsi, la préconisation qui est faite par les auteurs américains est de scinder les informations personnelles en trois subdivisions. La première concerne les informations personnelles à propos d'un individu identifié. L'identification est réputée exister si l'information distingue spécifiquement une personne et que son identité est de fait révélée. La deuxième est relative aux informations personnelles concernant des personnes identifiables. Dans cette définition, le caractère identifiable se déduit si par l'information, il existe des possibilités d'identification future. La troisième catégorie traite des informations personnelles sur des personnes non identifiables. Ici, on pourrait penser qu'il s'agit de données non personnelles, mais il n'en est rien. En réalité, la différence entre identifiable et non identifiable réside dans le risque d'identification future. Dans ce cas, l'information personnelle est considérée comme non identifiable s'il existe un risque minime

[508] *Ibid.*

d'identification.[509] Selon les auteurs, le régime juridique applicable à ces trois catégories serait différent, en partant du postulat selon lequel les données identifiées nécessitent un degré de protection plus élevé que les données dont le risque qu'elles aboutissent à l'identification d'une personne physique est faible.[510]

Cette proposition de définition de la donnée personnelle est intéressante en ce qu'elle base son régime juridique sur un paradigme complètement différent de celui utilisé en droit européen. En effet, La PII 2.0 fonde le degré de protection sur le risque d'identification indépendamment du type de donnée, tandis qu'en droit européen c'est bien le type de donnée qui conditionne le degré de protection. Le RGPD prévoit en effet un régime de protection spécial pour les données dites sensibles qui renvoient entre autres à l'opinion politique, l'orientation sexuelle ou les données de santé.[511] Retenir cette conception en droit américain reviendrait donc à éloigner encore davantage les deux modèles de part et d'autre de l'Atlantique. En conséquence, le Privacy Shield perdrait encore plus de sens juridique puisque la manière de légiférer dans le domaine et les règles adoptées seraient complètement différentes et la probabilité de voir les entreprises adhérentes au Privacy Shield, respecter les principes sur le fondement de la définition européenne de la donnée personnelle serait a priori assez faible. De plus, les institutions américaines auraient plutôt tendance à favoriser leur conception, que ce soit dans les recours ou bien même dans les contrôles des entreprises certifiées. Dès lors, si une future loi fédérale retenait cette théorie de la PII 2.0, cela déboucherait par souci de cohérence juridique sur une renégociation de l'accord, si tant est que l'on considère ce dernier comme un cadre juridique. Cependant, rien n'est moins certain et cette situation étaye un peu plus la thèse d'un accord politique.

Cependant, la tendance ne semble pas suivre cette théorie. Si l'on prend comme référence actuelle le CCPA, il semblerait que la définition européenne de la donnée personnelle ait le vent en poupe puisque celle du CCPA en est proche. Comme il déjà été mentionné, il définit l'information personnelle comme :

[509] SCHWARTZ M. (P.), SOLOVE J. (D.), « The PII Problem: Privacy and a New Concept of Personally Identifiable Information », *New York University Law Review*, volume 86, n°6, décembre 2011, pp. 1814-1894.
[510] *Ibid.*
[511] Art. 9 du RGPD.

> « Une information qui identifie, qui se rapporte à, qui décrit, qui est susceptible d'être associé à, ou qui peut raisonnablement être liée, directement ou indirectement à une personne ou une famille. »[512]

On retrouve bien ici un équivalent de la définition de l'article 4 du RGPD sur le fait que la donnée doit être liée à une personne identifiée ou identifiable. À la suite de la définition, le CCPA fournit une liste non exhaustive d'informations personnelles. Ainsi, on y retrouve en autres, les données commerciales, les données biométriques, les données issues d'un système informatique et les données de géolocalisation[513]. Cela rappelle également l'article 4 du RGPD qui fournit une liste de catégories de données personnelles. Même s'il existe des différences dans la loi californienne, comme l'exclusion des informations publiquement disponibles ou bien l'absence de définition des données sensibles, ce qui les soumet donc au même régime que les autres catégories de données, il y a des similitudes sémantiques dans la définition de donnée personnelle proposée.

Si cette direction est confirmée au niveau fédéral, c'est une bonne nouvelle pour le Privacy Shield. En effet, cela devrait permettre aux entreprises adhérentes de fusionner davantage les pratiques de traitement de données états-uniennes avec celles issues des transferts de données depuis l'Europe. De ce fait, cela aurait pour conséquence que l'accord soit plus efficace juridiquement.

Si et seulement si cette direction est prise, alors on pourra commencer à entrevoir le Privacy Shield comme un accord ayant une valeur juridique puisque cette dernière dépend du rapprochement des conceptions européenne et américaine de la donnée personnelle. En attendant, il demeure un accord juridiquement très limité qui remplit bien sa fonction politique. Mais si la conception américaine venait à évoluer dans le sens d'une protection plus forte, alors c'est vraisemblablement une décision d'adéquation globale qui serait prise par la Commission, auquel cas le Privacy Shield disparaitrait.

[512] Art. 1798.140 California Consumer Privacy Act of 2018.
[513] *Ibid.*

CONCLUSION

Juridiquement, le Privacy Shield souffre de trop de lacunes pour être considéré comme un cadre juridique efficace. C'est notamment le cas à cause de mécanismes d'exceptions trop larges en ce qui concerne l'accès aux données par les autorités américaines ou bien par un manque de volonté d'application de ce cadre du côté américain. Il n'est d'ailleurs pas exclu qu'il subisse le même sort que son prédécesseur si une action à son encontre aboutit.

Économiquement, il remplit sa mission en conservant la libre circulation des données personnelles pour les organisations certifiées et en permettant les transferts de gros volumes de données vers les États-Unis. À l'ère du Big Data et du Cloud Computing, il semble indispensable que cette libre circulation soit rendue possible entre les États-Unis et l'Union européenne puisque ce sont deux partenaires économiques puissants et privilégiés. De plus, beaucoup de grosses entreprises américaines de services numériques doivent pouvoir continuer à exercer leurs activités basées en autres sur l'exploitation de données personnelles afin de satisfaire une clientèle nombreuse en Europe. Enfin, il s'agit plus généralement d'ouvrir le marché à des primo arrivants et de développer le marché numérique global en fournissant un moyen efficace de transférer de gros volumes de données.

Politiquement, les conclusions de l'étude sont les plus intéressantes. En effet, l'accord transatlantique a éclos dans un contexte de scandales impliquant des organisations américaines, mais également le gouvernement américain. Cela a rebattu les cartes dans les négociations et notamment durant les examens conjoints. Ainsi il semblerait que les acteurs états-uniens se sentent plus concernés par la protection des données personnelles et que des revendications éclatent parmi les citoyens pour réclamer plus de protection. Il est évident que le Privacy Shield n'a pas joué un rôle fondamental, mais il a apporté chaque jour sa pierre à l'édifice en étant une contrainte juridique, aussi maigre soit-elle dans l'économie et la politique américaine. Ainsi le Privacy Shield représente ce que le droit a de plus politique puisque l'outil juridique est utilisé à des fins de négociations et de convergences des intérêts des deux parties.

BIBLIOGRAPHIE

I. OUVRAGES GÉNÉRAUX ET SPÉCIALISÉS

- BERMAN (J.J.), *Principles of Big Data*, Morgan Kaufmann, Boston, 2013.

- BABINET (G.), *Big Data, penser l'homme et le monde autrement*, édition Le Passeur, le 19 février 2015.

- CATE H. (F.), DEMPSEY X. (J.), *Bulk Collection: Systematic Government Access To Private-Sector Data*, Oxford Scholarship Online, Octobre 2017.

- CHERRY (D), *The Basics of Digital Privacy: Simple Tools to Protect Your Personal Information and Your Identity Online*, The Basics, Syngress, 2014.

- DESGENS-PASANAU (G.), *La protection des données personnelles*, édition n° 3, LexisNexis, juin 2018.

- FÉRAL-SCHUHL (C.), *Cyberdroit 2018/19*, édition n° 7, Praxis Dalloz juillet 2018.

- GRAY (D.), HENDERSON E. (S.), *The Cambridge Handbook of Surveillance Law*, Cambridge University Press, Octobre 2017.

- GOLA V (R.), *Droit du E-commerce et du marketing digital*, Gualino, juin 2019.

- LEROY (F), *Surveillance : Le risque totalitaire*, Éditions actes sud, juin 2018.

- VOSS (G.), WOODCOCK H. (C.), *Navigating EU Privacy and Data Protection Laws*, American Bar Association, 1 décembre 2016.

II. THÈSES ET MÉMOIRES

- SALOLATVA (L), « Privacy Shield Redress Mechanisms Assessment in the Light of the Schrems Case », Master's Thesis in European Law, faculty of Law, University of Helsinki.

- BOULLIER (V.), « L'influence des États-Unis sur le droit du réseau internet », Mémoire pour l'obtention du Master « Droit des médias et des télécommunications », Faculté de droit et de sciences politiques, Aix Marseille Université.

III. ARTICLES, CONTRIBUTIONS, INTERVENTION

- ANONYME, « Lutte contre le terrorisme : Qu'est ce que le PNR, le fichier sur les passagers aériens ? », www.lemonde.fr, publié le 19 novembre 2015.

- ANONYME, « PNR-UE ; un bilan préoccupant », http://www.aedh.eu, publié le 6 mars 2017.

- ANONYME, « Are they allowed to do that? A breakdown of selected government surveillance programs », www.brennancenter.org.

- ANONYME, « Atos, 1ère société informatique à obtenir la certification BCR pour sa capacité à garantir la protection des données personnelles de ses clients », www.atos.net, publié le 20 novembre 2014.
- ANONYME, « Données personnelles des passagers aériens : accord entre les États-Unis et l'Europe », www.vie-publique.fr, publié le 9 mai 2012.

- ANONYME, « Global 500 companies to spend $7.8B on GDPR compliance », www.iapp.org, publié le 20 novembre 2017.

- ANONYME, « Marché unique numérique : un état des lieux », www.touteleurope.eu, publié le 15 mars 2018.

- ANONYME, « Un accord en trilogue sur le règlement "platform To business" a été trouvé », *Contrats Concurrence Consommation* n° 4, Avril 2019, alerte 16 sur le communiqué de la commission européenne du 14 février 2019

- ANONYME, « De nouveaux documents détaillant le lobbying de Facebook », www.lemonde.fr, publié le 4 mars 2019.

- ANONYME, « Advocates publish European Commission records of Facebook lobbying », www.iapp.org, publié le 24 janvier 2019.

- ANONYME, « Facebook : des accès "partenaires" aux données utilisateurs ont été accordés à Apple, Netflix, Spotify, Amazon, Yahoo ! », www.lemonde.fr, publié le 19 décembre 2018.

- ANONYME, « Le patron d'Apple s'attaque aux revendeurs de données personnelles », www.lemonde.fr, publié le 17 janvier 2019.

- ANONYME, « PNR UE-USA : un bilan préoccupant », www.aedh.eu, publié le 6 mars 2017.

- AFP, « Après le scandale Facebook, Cambridge Analytica met la clé sous la porte », www.lemonde.fr, publié le 2 mai 2018.

- AFP, « Le patron d'Apple défend à Bruxelles l'idée d'une loi américaine sur les données personnelles », www.lemonde.fr, publié le 24 octobre 2018.

- ASSEY M (J.jr), DEMETRIOS A (E), « The EU-U.S privacy Safe harbour : smooth sailing in trouble waters? », *CommLaw Conspectus* n°9, 2001.

- ALVAREZ (D.), « Safe Harbor is dead; Long live the Privacy shield », www.americanbar.org, publié le 20 mai 2016.

- ANGELA, « La sécurisation des données personnelles aux États-Unis : la FTC s'immisce dans le débat », www.avocat-transatlantique.com, publié le 29 Novembre 2015.

- AUDUREAU (W.), « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », www.lemonde.fr, publié le 22 mars 2018.

- AUVRET-FINCK (J.), « L'échange d'information dans les accords PNR conclus par l'UE avec des États tiers », Colloque « l'échange des données dans l'espace de liberté, de sécurité et de justice de l'Union européenne », Grenoble, 17-18 novembre 2016.

- ANONYME, « Antitrust Compliance: Perspectives and Resources for Corporate Counselors », *ABA Publishing*, Chicago, 2005, pp. 25-27.

- AFALO (A.), « Apple, Amazon, Alphabet… les 10 entreprises les plus valorisées en bourse », www.leparisien.fr, publié le 3 août 2018.

- ASTA A. (T.), « Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions », *Florida State University Law Review*, volume 45, n°1, automne 2017, pp. 261. à 312.

- ARMBRUST (M.), FOX (A.), GRIFFITH (R.), JOSEPH D. (A.), KATZ H. (R.), KONWINSKI (A.), LEE (G.), PATTERSON A. (D.), RABKIN (A.), STOICA (I.), ZAHARIA (M.), « Above the Clouds: A Berkeley View of Cloud Computing », *Technical Report n° UCB/EECS-2009-28*, publié le 10 février 2009.

- BLANKE M (J), « Safe Harbor and the European Union's Directive on Data Protection », *Albany Law Journal of Science & Technology* n°11, 2000.

- BARRAT (O), « Informatique en nuage : mettez de côté le PATRIOT Act, penchez-vous sur le FISAA », *Sécurité et stratégie* 2013/3 (14).

- BRACY (J.), « Senate confirms PCLOB members ahead of Privacy Shield second-annual review », www.iapp.org, publié le 12 octobre 2018.

- BALDWIN (C.), « Hackers release files indicating NSA monitored global bank transfers », www.reuters.com, publié le 14 Avril 2017.

- BARRAUD (B.), « Se souvenir de Cambridge Analytica », *la REM*, n° 48, Automne 2018

- BONIS (P.), « L'internet européen : intérêts communs et acquis communautaires », *Annales des Mines – réalités industrielles*, n° 2016/3, Août 2016, pp. 19 à 23.

- BARRAUD (B.), « Aux États-Unis, les données personnelles sont des biens commerciaux comme les autres », *La REM*, n° 42-43, Printemps — Été 2017.

- BRILL (J.), « Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation, Keynote Address at Ghostery », Hogan Lovells Data Privacy Day n°9, le 21 Janvier 2016.

- BRASSEUR (C.), « Usages visuels des données et Big data », *I2D – Information, données et documents*, 2015/2, volume 52, 2015.

- BUCHY (F.), « Les GAFA sont-ils trop puissants ? », www.grandes-ecoles.studyrama.com, publié le 19 novembre 2018.

- BENSOUSSAN (A.), « La propriété des données », www.blog.lefigaro.fr, publié le 18 mai 2010.

- BOUGUETTAYA (F), « Loi "pour une république numérique" : quel impact pour l'e-commerce », *Revue Lamy droit de l'immatériel*, n° 133, 1er janvier 2017.

- BOYNE M. (S.), « Data Protection in the United States », *American Journal of Comparative Law*, volume 66, 2018, pp. 299 à 343.
- BERGELSON (V.), « It's Personal but Is It Mine – Toward Property Rights in Personal Information », University of California Davis Law Review, volume 37, n°2, Décembre 2003, pp. 379-452.

- BAUER L. (J.), « Playing Off-Key: Trans-Atlantic Data Regulation in a discordant World », *West Virginia Law Review*, volume 119, n° 2, Hiver 2016, pp. 793 à 828.

- BORDER C. (A.), « Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States », *Suffolk Transnational Law Review*, volume 35, n° 2, été 2012, pp. 363-392.

- BALABAN L. (T.), « Comprehensive Data Privacy Legislation: Why Now is the Time? », *Case Western Reserve Journal of Law, Technology & the Internet*, volume 1, n°1, automne 2009, pp. 1-35.

- BERGELSON (V.), « It's Personal but Is It Mine – Toward Property Rights in Personal Information », University of California Davis Law Review, volume 37, n°2, décembre 2003, pp. 379-452.

- BECKER (M.), « GDPR Compliance: How it's Affecting U.S Companies », www.emarsys.com.

- BOWMAN M. (C), « US-EU Safe Harbor invalidated: What now? », www.privacylaw.proskauer.com, publié le octobre 2015.

- BOTCHORICHVILI (N.), « Transferts de données personnelles hors de l'Union européenne — Quelles nouveautés avec le RGPD », *Legicom* 2017/2, n ° 59.

- CLAVET (S), « Les conséquences de l'accord Passenger Name Record sur la protection des droits fondamentaux en Europe », *Droits Fondamentaux, Revue électronique du CRDH*, rubrique études, www. droits-fondamentaux.u-paris2.fr, 2010.

- CNIL, « Invalidation du "safe harbor" par la Cour de Justice de l'Union européenne : une décision clé pour la protection des données », www.cnil.fr, publié le 07 octobre 2015.

- CASTETS-RENARD (C), « Données personnelles : accord entre la Commission et les États-Unis », *Recueil Dalloz* n° 6/7675e, 11 février 2016.

- Conférence organisée par le Centre de recherche en droit public de l'Université de Montréal, V*ie privée : Europe vs. Amérique*, intervenants, CASTETS-RENARD (C.), REIDENBERG (J.), le 25 mai 2016, à Montréal.

- CASTETS-RENARD (C), « Adoption du Privacy Shield : Des raisons de douter de la solidité de cet accord », *Dalloz IP/IT* n° 10, Octobre 2016.

- CASTETS-RENARD (C), « L'adoption du Privacy Shield sur le transfert de données personnelles », Recueil Dalloz n° 28, Août 2016.

- CASTETS-RENARD (C.), « Le Privacy Shield », *DallozIP/IT*, n° 3, Mars 2016.

- CADWALLADR (C.), GRAHAM-HARRISON (E.), « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », www.theguardian.com, publié le 17 mars 2018.

- CHRISTAKIS (T.), « Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques Avis Juridique sur l'affaire Microsoft Ireland (Cour Suprême des États-Unis) », *livre blanc CEIS et The Chertoff Group*, décembre 2017.

- COLT (S.), « Tim Cook Has An Open Letter To All Customers That Explains How Apple's Privacy Features Work », www.businessinsider.fr publié le 18 septembre 2014.

- COOK (T.), « A Message To Our Customer », https://perma.cc/68X7-SDLL (archivage), publié le 16 février 2016.

- CNIL « Les clauses contractuelles types de la Commission européenne », www.cnil.fr, publié le 8 février 2016.

- CEDARBAUM G. (J.), FREEMAN JR (R.), LICHLYTER (L.), « United States: Congress Begins Consideration of Comprehensive Federal Privacy Legislation », www.mondaq.com, publié le 21 février 2019.

- CNIL « Le Privacy Shield », www.cnil.fr, publié le 24 mai 2017.

- DEIGHTON (A.), « The EU-US Privacy Shield - is it strong enough? », *Privacy & Data Protection*, volume n°16, issue n°4, Mars 2016.

- DONOHUE K (L.), « Section 702 and the collection of international telephone and internet content », *Harvard Journal of Law and Public Policy*, volume 38, issue 1, 2015, pp. 117 à 275.

- DEBET (A.), « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce électronique* n° 12, Décembre 2018, comm. 92.

- DELPECH (X.), « Un premier bilan décevant, mais pas désespéré », *Juris association*, n° 591, février 2019.

- DEBET (A.), « L'ICO, autorité de protection des données anglaise, prononce une sanction de 500 000 livres à l'encontre de Facebook dans l'affaire Cambridge Analytica », *Communication Commerce électronique* n° 12, Décembre 2018, comm. 92.

- DASKAL (J.), « Microsoft Ireland, The Cloud Act, and International Lawmaking 2.0 », Stanford Law Review Online, volume 71, Mai 2018, pp. 9 à 16.

- DEWEY (C.), « 98 personal data points that Facebook uses to target ads to you », www.washingtonpost.com, publié le 19 août 2016.
- DE KERAUTEM (V.), « Data centers : mais où se trouvent vos données ? », www.leparisien.fr, publié le 20 février 2017.

- DARCY (S.), « Battling for the Rights to Privacy and Data Protection in the Irish Courts », *Utrecht Journal of International and European Law*, volume 31, n°80, 2015, DOI, pp. 131 à 136.

- DEBET (A.), « Quelle législation pour la protection des données aux États-Unis », *communication commerce électronique*, n° 5, Mai 2019, comm. 36.

- DE LA TORRE (L.), « GDPR matchup : The California Consumer Privacy Act 2018 », www.iapp.org, publié le 31 juillet 2018.

- EVANS (P.) et WURSTER (T.), « Blown to bits: how the new Economics of Information Transforms Strategy », *Harvard Business School Press*, 2000, pp. 64-65.

- EUDES (Y.), « Visite exceptionnelle dans le data center de Facebook, en Suède », www.lemonde.fr, publié le 19 mai 2016.

- EDWARDS (J.), « Tim Cook Basically Just Said He Was 'Offended' By The Way Google And Amazon Do Business », www.businessinsider.fr, publié le 16 septembre 2014.

- FLIPO (O), « Après le "Safe Harbor", le "Privacy Shield" », Dossiers d'actualité *LexisNexis*, 27 mai 2016.

- FRAYSSINET (J), « Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les États-Unis : l'accord dit "sphère de sécurité" (ou safe harbour) », *Communication Commerce électronique* n° 3, Mars 2001, chron.7.

- FISCHER (P), « From the safe harbour to the privacy shield: selected aspects of the EU-US privacy shield », *Revue de droit des affaires internationales* n°2, 2018, pp. 143 à 153.

- FUNG (B.), « Trump has signed repeal of the FCC privacy rules. Here's what happen next », www.washingtonpost.com, publié le 4 avril 2017.

- FRISON-ROCHE (M.A), « Le droit de la compliance », *Recueil Dalloz* n° 32, 29 septembre 2016, chronique p. 1871.

- FRISON-ROCHE (M.A), « Le droit de la compliance au-delà du droit de la régulation », *Recueil Dalloz*, 2018, chronique. pp. 1561 et s.

- FREIWALD (S.), « At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA) », *Berkeley Technology Law Journal*, volume 33, n°1, 2018, pp. 131 à 176.

- GREENWALD (G), « NSA collecting phone records of millions of Verizon customers daily », www.theguardian.com, publié le 6 juin 2013.

- GREENWALD (G), MASCASKILL (E), « NSA Prism program taps in to user data of Apple, Google and others », www.theguardian.com, publié le 7 juin 2013.

- GASTAUD (F), « Quelles conséquences pratiques pour le transfert de données aux États-Unis suite à l'invalidation du "Safe Harbor" par la CJUE ? », www.village-justice.org, publié le 7 octobre 2015.

- GRIGUER (M), « Le Safe Harbor est mort, vive l'UE-US Privacy Shield Arrangement », *Cahiers de droit de l'entreprise* n° 2, Mars 2016, prat. 10.

- GRANT (G), « Tech companies like Privacy Shield but worry about legal challenges », www.cio.com, publié le 21 décembre 2016.

- GILLASPIE (A.), « Extraterritorial Application of the Stored Communications Act: Why Microsoft Corp. v. United States Signals That Technology Has Surpassed the Law », University of Kansas Law Review, volume 66, 2017, pp. 459 à 483.

- GRYNWAJC (S.), « GDPR : Surviving the likely demise of the Privacy Shield », www.transatlantic-lawyer.com, publié le 8 Juillet 2018.

- GRYNBAUM (L.), « La directive "Commerce électronique" ou l'inquiétant retour de l'individualisme juridique », *La Semaine Juridique — Edition Générale*, n° 12, 21 mars 2001.

- GERRISH (C.), APTEL (P.), « Le "California Consumer Privacy Act" : un timide RGPD américain ? », www.village-justice.com, publié le 10 juillet 2018.

- HASHEM A. T. (I.), YAQOOB (I.), ANUAR B. (N.), MOKHTAR (S.), GANI (A.), KHAN U. (S.), « The rise of "big data" on cloud computing: Review and open research issues », *Information Systems*, volume 47, Janvier 2015, pp. 98 à 115, p. 100.
- GANTZ (J), REINSEL (D.), « Extracting Value from Chaos », *IDC iView*, juin 2011, pp. 1 à 12.

- HAGEL (J.) et SINGER (M.), « Net Worth: Shaping Markets when Customers Make the Rules », *Harvard Business School Press*, 8 janvier 1999.

- HOUSER A. (K.), VOSS W. (G.), « The End of Google and Facebook Or a New Paradigm in Data Privacy », *Richmond Journal of Law & Technology*, volume 25, issue 1, 2018.

- ICO, « Data transfers to the U.S and Safe Harbor – interim guidance », www.ico.org.uk, publié le 10 février 2016.

- ICO, « ICO issues maximum £500000 fine to Facebook for failing to protect user's personal information », www.ico.org.uk, publié le 25 Octobre 2018.

- JACOBSON (R.), « 2.5 quintillion bytes of data created every day. How does CPG and Retail manage it? », www.ibm.com, publié le 24 avril 2013.

- JOERLING (J.), « Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data. » *Washington University Journal of Law and Policy*, volume 32, n°1, 2010, pp. 467-488.

- KIM (W.), « Cloud Computing: Today and Tomorrow », *Journal of object technology*, Volume 8, n°1, janvier/février 2009, pp. 66 à 72.

- KANG (C.), « FTC Hits Musical.ly With Record Fine for Child Privacy Violation », www.nytimes.com, publié le 27 février 2019.

- LINN (E.), « A Look into the Data Privacy Crystal Ball: A survey of possible Outcomes for the EU-U.S Privacy Shield Agreement », *Vanderbilt Journal of Transnational Law*, volume n°50, 2017, pp. 1311 à 1358.

- LE VOGUER (G.), « Donald Trump et les services de renseignement : une relation sous tension », *revue LISA*, volume 16, n° 2, 2018.

- LIPTAK (A.), « President Donald Trump has signed the FISA reauthorization bill », www.theverge.com, publié le 20 janvier 2018.

- LAUSSON (J.), « Privacy Shield : la Commission européenne met en garde les États-Unis », www.numerama.com, publié le 31 juillet 2018.

- LEQUEUX (V.), « Le commerce extérieur de l'Union européenne », www.touteleurope.eu, publié le 14 Avril 2019.

- LAUSSON (J.), « Les États-Unis planchent aussi sur leur RGPD, mais dans une version moins stricte », www.numerama.com, publié le 30 juillet 2018.

- LE NOAN (E.), « Non à un protectionnisme numérique européen », www.lesechos.fr, publié le 23 Octobre 2018.

- LÉVÊQUE (F.), « François Lévêque : « Face aux GAFA, l'Europe doit accélérer la numérisation de ces entreprises », www. alternatives-economiques.fr, publié le 31 Décembre 2018.

- LELOUP (D.), UNTERSINGER (M.), « "Le pouvoir de Mark Zuckerberg est sans précédent" : un de ses cofondateurs appelle à démanteler Facebook », www.lemonde.fr, publié le 9 Mai 2019.

- LAZARÈGUE (A.), « "Là où le RGPD a échoué, le droit de la concurrence peut encore gagner." », www.lemonde.fr, publié le 14 Juin 2019.

- LELOUP (D.), « Mark Zuckerberg annonce un virage vers un Facebook plus privée », www.lemonde.fr, publié le 30 avril 2019.

- MCGOOGAN (C), « What does the end of Safe Harbor mean for you? », www.wired.co.uk, publié le 6 octobre 2015.

- METALLINOS (N), « Adoption du Privacy Shield : un constat à durée déterminée ? », *Communication Commerce électronique* n° 10, Octobre 2016, comm. 85.

- MAXWELL (W), TAIEB (S), « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT* n° 3, Mars 2016.

- MONELEONE (S), PUCCIO (L) (Service de recherche du Parlement européen, EPRS), « Du Safe Harbour au Privacy Shield : Avancées et insuffisances des nouvelles règles de transfert des données UE-États-Unis », PE 595 892, Janvier 2017.

- MARGULIES (P.), « Reauthorizing the FISA Amendments Act: A Blueprint for enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities », Journal of Business & Technology Law, volume 12, issue 1, 2016 pp. 23 à 52.

- MOURON (P.), « Pour ou contre la patrimonialité des données personnelles », *la REM*, n° 46-47 Printemps — été 2018.

- MATSAKIS (L.), « Microsoft Supreme Court case has big implications for data », www.wired.com, publié le 27 février 2018.

- MISTRAL (J.P.), « Le Cloud Act, des questions et des réponses », www.village-justice.com, publié le 5 Février 2019.

- MAKSO (B.), « Exporting the Policy – International Data Transfer and the Role of Binding Corporate Rules for Ensuring Adequate Safeguards », *Pecs Journal of International & European Law*, volume 2016, 2016.

- MCALLISTER (C.), « What about small businesses? The GDPR and its consequences for small U.S.-based companies? », *Brooklyn Journal of Corporate, Financial & Commercial Law*, volume 12, 1er septembre 2017, pp. 187 à 211.

- MERRITT (C.), « What Size Company Is Considered a Mid-Size Company », www.chron.com, mis à jour le 8 mars 2019.

- MONNERIE (N.), « Les défis de la commercialisation des données après le RGPD : aspects concurrentiels d'un marché en développement », *Revue internationale de droit économique*, n° 2018/4, volume 32.

- MANYIKA (J.), CHUI (M.), BROWN (B), BUGHIN(J.), DOBBS (R.), ROXBURGH (C.), BYERS (A.H.), « Big Data: The next frontier for innovation, competition, and productivity », www.mckinsey.com, mai 2011.

- MELL (P.), GRANCE (T.), « The NSIT Definition of Cloud Computing », *recommendations of the National Institute of Standards and Technology*, special publication 800-145, septembre 2011.

- MARCHAIS (I.), « Comment Washington fait pression contre la taxe GAFA à Bruxelles », www.lopinion.fr, publié le 11 mars 2019.

- MCGRATH P. (K.), « Developing a First Amendment Framework for the Regulation of Online Educational Data: Examining California's Student Online Personal Information Protection Act », *University of California Davis Law Review*, volume 49, n°3, février 2016, pp. 1149 à 1181.

- MONAHAN A (P.), « Deconstructing information Walls: The impact of the European Data Directive on U.S Businesses » *Law & Policy in International Business*, volume 29, 1998, pp. 275 à 277.

- NOACK (R.), « One key question for Zuckerberg: Will Americans become second class citizens? », www.washingtonpost.com, publié le 10 avril 2018.

- POULLET (Y), « Les Safe Harbor Principles : une protection adéquate ? », www.droit-technologie.org.

- PIXELS, « Max Schrems, le "gardien" des données personnelles qui fait trembler les géants du Web », www.lemonde.fr, publié le 05 octobre 2015.

- PERRAY (R), UZAN-NAULIN (J), « Transfert de données — Arrêt Schrems : Cour(s) magistral(e) de droit à la protection des données personnelles » *Communication Commerce électronique* n° 12, Décembre 2015, étude 21.

- PAHL (T.), « Your cop on the privacy beat », www.ftc.gov, publié le 20 Avril 2017.

- PÉPIN (G.), « Privacy Shield : un an plus tard, l'efficacité du bouclier européen reste difficile à mesurer », www.nextinpact.com, publié le 18 octobre 2017.

- PÉPIN (G.), « Retour sur le scandale Cambridge Analytica et la (molle) réponse de Facebook », www.nextinpact.com, publié le 23 mars 2018.

- PETIT (N.), « New Challenges for 21st Century Competition Authorities », *Working Paper*, 28 janvier 2013.

- PATTERSON (M.), « On the Impossibility of Information Intermediaries », *Fordham Law and Economics Research Paper*, n° 13, juillet 2001.

- PHILOUZE (A.L.), « The EU-US Privacy Shield: Has Trust Been restored », *The European Data Protection Law Review*, volume n°3, 2017, pp. 463 à 472.

- PORTER (M.) et HEPPELMAN (J.), « How Smart Connected Products are Transforming Competition », *Harvard Business Review*, novembre 2014.
- PARDAU L. (S.), « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », *Journal of Technology Law & Policy*, volume 23, n°1, 2018-2019, pp. 68 à 114.

- PIQUARD (A.), « Amende record, mais indolore pour Facebook », www.lemonde.fr, publié le 13 juillet 2019.

- POLLACK C. (M.), « Taking Data », *University of Chicago Law Review*, volume 86, n°1, January 2019, pp. 77 à 141.

- REES (M), « La CJUE invalide le Safe Harbor américain : quelles conséquences ? », www.nextincpact.com, publié le 6 octobre 2015.

- REES (M.), « Privacy Shield : le sombre bilan des CNIL européennes, la menace d'un recours », www.nextinpact.com, publié le 6 décembre 2017.

- REES (M.), « Au Parlement européen, la commission Libe demande la suspension du Privacy Shield », www.nextinpact.com, publié le 12 juin 2018.

- REES (M.), « Une étude dresse les enjeux, problèmes et dommages collatéraux de l'affaire Microsoft Ireland », www.nextinpact.com, publié le 07 décembre 2017.

- ROMM (T.), « The Trump Administration is talking to Facebook and Google about potential rules for online privacy », www.washingtonpost.com, publié le 27 juillet 2018.

- SCHWARTZ M. (P), PEIFER (K.N), « Transatlantic Data Privacy Law », *The George Town Law Journal*, volume 106, 2017, pp. 115 à 179.

- SCHWARTZ M. (P.), « The EU-US Privacy collision: a turn to institutions and procedures », *Harvard Law Review*, volume n°126, 2013.

- SANGARE (M.), « La NSA a aussi surveillé les transactions financières mondiales », www.mediapart.fr, publié le 17 septembre 2013.

- SALINAS (S.), « Facebook Stock Slides After FTC Launches Probe of Data Scandal », www.cnbc.com, publié le 26 mars 2018.

- SEGALIS (B.), LINKSY (K.), « FTC Commissioner Julie Brill Comments on EUUS Privacy Shield », www.dataprotectionreport.com, publié le 4 Février 2016.

- SEGOND (V.), « Des données personnelles très convoitées », www.lemonde.fr, publié le 29 mai 2017.

- SFADJ (R.), GOMBAUD-SAINTONGE (H.), « Le RGPD est une mine de valeurs », www.lesechos.fr, publié le 4 Juin 2019.

- SEN (S.), JOE-WONG (C.), HA (S.) et CHIANG (M.), « Smart Data Pricing: Economic Solution to Network Congestion », *Princeton University, Working Paper*, 11 avril 2013.

- SWIRE (P.), KENNEDY-MAYO (D.), « How both EU and the U.S. are "stricter" than each other for the privacy of government requests for information » *Emory Law Journal,* volume 66, 2016.

- SZADKOWSKI (M.), « Affaires, failles de sécurité et scandales… 2018 année terrible pour Facebook », www.lemonde.fr, publié le 4 janvier 2019.

- SZADKOWSKI (M.), « Facebook : une faille de sécurité a pu exposer les photos de 6,8 millions d'utilisateurs », www.lemonde.fr, publié le 17 décembre 2018.

- SCHWARTZ M. (P.), SOLOVE J. (D.), « PII 2.0: Privacy and a New Approach to Personal Information », *Privacy & Security Law Report*, volume 11, novembre 2012.

- SCHWARTZ M. (P.), SOLOVE J. (D.), « The PII Problem: Privacy and a New Concept of Personally Identifiable Information », *New York University Law Review*, volume 86, n°6, décembre 2011, pp. 1814-1894.

- VALÉRIE (M), « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, 2006.

- VOSS W. (G.), « The future of transatlantic data flows: Privacy Shield or bust », Journal of internet Law vol.19, n°11 May 2016, pp. 9 à 18.

- VALLAT (T.), « L'accord PNR prévu entre l'Union européenne et le Canada ne peut pas être conclu sous sa forme actuelle selon l'avis de la CJUE du 26 juillet 2017 », www.thierryvallatavocat.com, publié le 27 juillet 2017.

- VOLOKH (E.), « Cheap Speech and What it Will do », *The Yale Law Journal*, volume 104, 1994-1995.

- VOLOKH (E.), « Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You », Stanford. Law Review, volume 52, 2000, pp. 1049 à 1122.

- WILBUR (R.), « EU Data privacy laws are likely to create barriers to trade », www.ft.com, publié le 30 mai 2018.
- WEN J. (C.), « Secrecy, Standing, and executive Order 12,33 », 89 Southern California Law Review, volume 89, 2016, pp. 1099 à 1138.

- WARRICK (P), « Brief for Amici Curiae computer and data science experts in support of appellant Microsoft Corporation », pour *l'affaire Microsoft corporation c/United States of America*, publié le 15 décembre 2014.

- WANG (Y.), GIOVANNI (L.), CHEN (X.), SARANGA (K.), NORCIE (G.), SCOTT (K.), ACQUISTI (A.), CRANNOR FAITH (L.), SADEH (N.), « From Facebook Regrets to Facebook Privacy Nudges », *Ohio State Law Journal*, volume 74, n° 6, 2013, pp. 1307 à 1334.
- ZUCKERBERG (M.), « Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas. », www.washingtonpost.com, publié le 30 mars 2019.

- ZUCKERBERG (M.), « A Privacy-Focused Vision for Social Networking », www.facebook.com, publié le 6 mars 2019.

IV. CONCLUSIONS DES COMMISSAIRES DU GOUVERNEMENT OU DES RAPPORTEURS PUBLICS/RAPPORTS DES AVOCATS GÉNÉRAUX

- Avis 1/15 « Conclusions de l'avocat général M. Paolo Mengozzi », 8 septembre 2016

- Rapport du Député Raphaël Gauvain à M. le Premier Ministre Édouard Philippe du 26 juin 2019 sur « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriales ».
- Rapport avec preuve de la Chambre des Lords du 5 juin 2007 sur le « EU/US Passenger Name Record (PNR) Agreement ».
- Rapport du PCLOB du 2 juillet 2014, sur le programme de surveillance mené conformément à la section 702 du FISA.

V. NOTES, OBSERVATIONS, COMMENTAIRES ET CHRONIQUES DE JURISPRUDENCE

- DEBET (A), « L'invalidation du Safe Harbor, un nouveau "grand arrêt", de la CJUE dans le domaine de la protection des données », Communication Commerce électronique n° 11, Novembre 2015, comm. 94.

- DEBET (A), « L'invalidation du Safe Harbor par la CJUE : tempête sur les transferts de données vers les États-Unis », La Semaine Juridique Edition Générale n° 46-47, 9 Novembre 2015, 1258, p.2109.

VI. DOCUMENTS SPÉCIALISÉS

- Avis WP32 du G29, du 16 mai 2000 sur le niveau de protection garanti par les principes du Safe Harbor.
- Avis 4/2016 du Contrôleur européen à la protection des données du 30 mai 2016 concernant le « bouclier vie privée UE-États-Unis » (Privacy Shield), Projet de décision d'adéquation.

- CJUE, affaire C-362/14 du 6 octobre 2015, Maximillian Schrems c/Data Protection Commissioner.

- Communiqué du G29 du 16 octobre 2015.

- Communiqué du G29 sur l'opinion sur le EU-U.S Privacy Shield du 13 Avril 2016.

- Communiqué du Conseil national du numérique sur le sujet « pourquoi le Privacy Shield doit être renégocié » du19 septembre 2017, www.cnnumérique.fr.

- Communiqué de presse de la Commission européenne du 6 novembre 2015, — la Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire Schrems.

- Communiqué de presse de la Commission européenne du 6 novembre 2015, — la Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire Schrems.

- Communiqué de presse de la Commission européenne du 2 février 2016, – La Commission européenne et les États-Unis s'accordent sur un nouveau cadre pour les transferts transatlantiques de données, le « bouclier vie privée UE-États-Unis ».

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

- Communication COM (2016) 117 de la Commission européenne au Parlement européen et au conseil du 29 février 2016 relative aux flux de données transatlantiques : rétablir la confiance grâce à des garanties solides.

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

- Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.

- Discours de la Commissaire V. Jourová du 26 octobre 2015 sur la décision de la CJUE sur le Safe Harbor devant la Commission des libertés civiles, de la justice et des affaires intérieures (Libe).

- Déclaration commune adoptée par le G29 du 25 novembre 2014 dans le cadre de « The European Data Governance Forum » du 8 décembre 2014.

- Liste du U.S-EU Safe Harbor list consultable sur le site www.export.gov.

- Lettre de John F. Kerry au Commissaire à la protection des données V. Jourová du 7 juillet 2016.

- Lettre du secrétaire d'État américain à la justice au Commissaire à la protection des données V. Jourová du 19 février 2016.

- Lettre du Secrétaire américain au commerce au Commissaire à la protection des données V. Jourová du 7 juillet 2016.

- Lettre de la FTC au Commissaire à la protection des données V. Jourová du 23 Février 2016.

- Opinion 01/2016, WP238 du G29 du 13 avril 2016 sur la décision d'adéquation de la version préliminaire du EU–U.S. Privacy Shield.

- Principes de l'accord U.S.-EU Safe Harbor, www. 2016.export.gov, dernière mise à jour le 30 janvier 2009.

- Principes de l'accord EU-U.S Privacy Shield publié par le Département du Commerce américain.

- Proposition de décision-cadre COM/2005/0475 du Conseil et de la Commission du 4 octobre 2005 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

- Proposition de résolution 2018/2645 (RSP) du Parlement européen, du 26 juin 2018, sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis.

- Rapport d'activité 2015 de la CNIL, www.cnil.fr.

- Rapport COM (2017) 611 de la Commission au Parlement européen et au Conseil, du 18 octobre 2017, sur le premier examen annuel relative au fonctionnement du EU–U.S. Privacy Shield.

- Rapport 17/EN, WP255 du G29 du 28 novembre 2017 sur le premier examen annuel conjoint du EU – U.S. Privacy Shield.

- Rapport du Comité européen de la protection des données du 22 janvier 2019 sur le deuxième examen annuel conjoint du EU – U.S. Privacy Shield.

- Rapport COM (2018) 860 de la Commission au Parlement européen et au Conseil, du 19 décembre 2018, sur le deuxième examen annuel relative au fonctionnement du EU–U.S. Privacy Shield.

- Remarques par la Secrétaire américaine au commerce Penny Pritzker à la conférence de presse du 12 juillet 2016 du Département du Commerce américain sur l'accord EU-U.S. Privacy Shield.

VII. SITES INTERNET

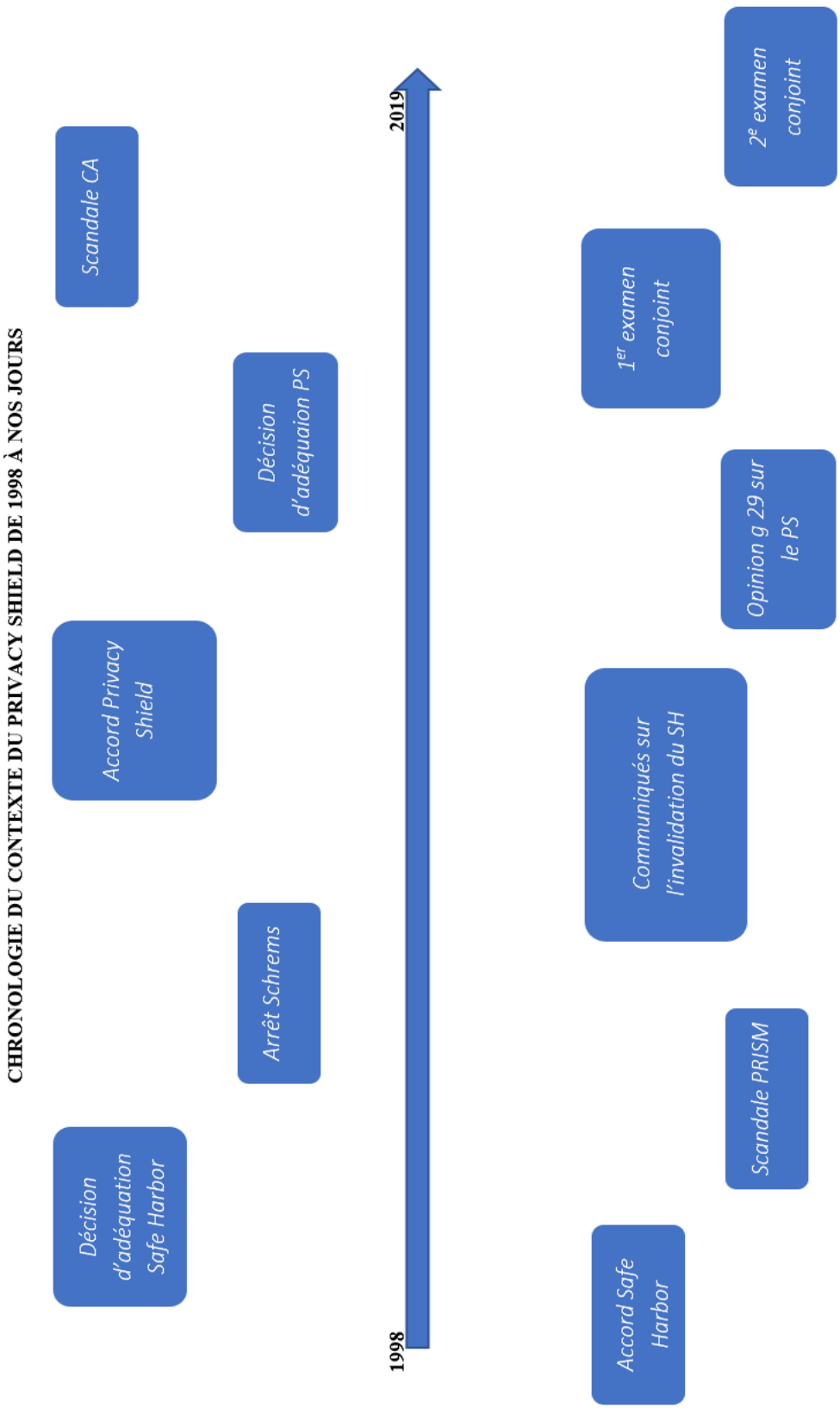
- www.build.export.gov
- www.cio.comwww.droit-technologie.org
- https://www.ecfr.gov
- www.lemonde.fr
- http://curia.europa.eu
- http://www.aedh.eu
- https://droits-fondamentaux.u-paris2.fr
- www.theguardian.com
- www.brennancenter.org

- www.cnil.fr
- www.wired.co.uk
- www.privacylaw.proskauer.com
- www.atos.net
- www.ico.org.uk
- www.cairn.info
- www.cio.com

VIII. RESSOURCES VIDÉOS

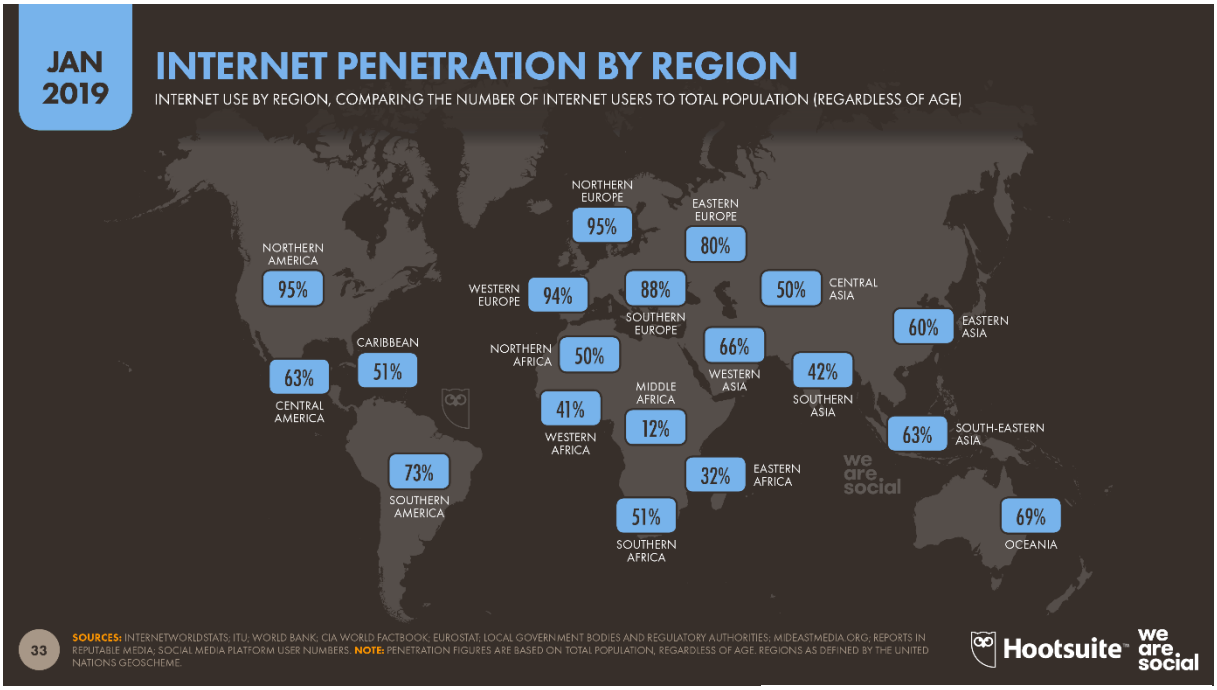
- Channel 4 News, « Cambridge Analytica Uncovered : Secret filming reveals election tricks », www.youtube.com, publié le 19 mars 2018. https://www.youtube.com/watch?v=mpbeOCKZFfQ

Annexe n° 1 : Chronologie du contexte du Privacy Shield de 1998 à nos jours



Annexe n° 2 : Statistiques du monde numérique par *Wearesocial*

Source : www.wearesocial.com



Source : www.wearesocial.com

Annexe n° 3 : Infographie : échanges commerciaux Europe/États-Unis, *le Data Lab*, www.alternatives-economiques.fr.

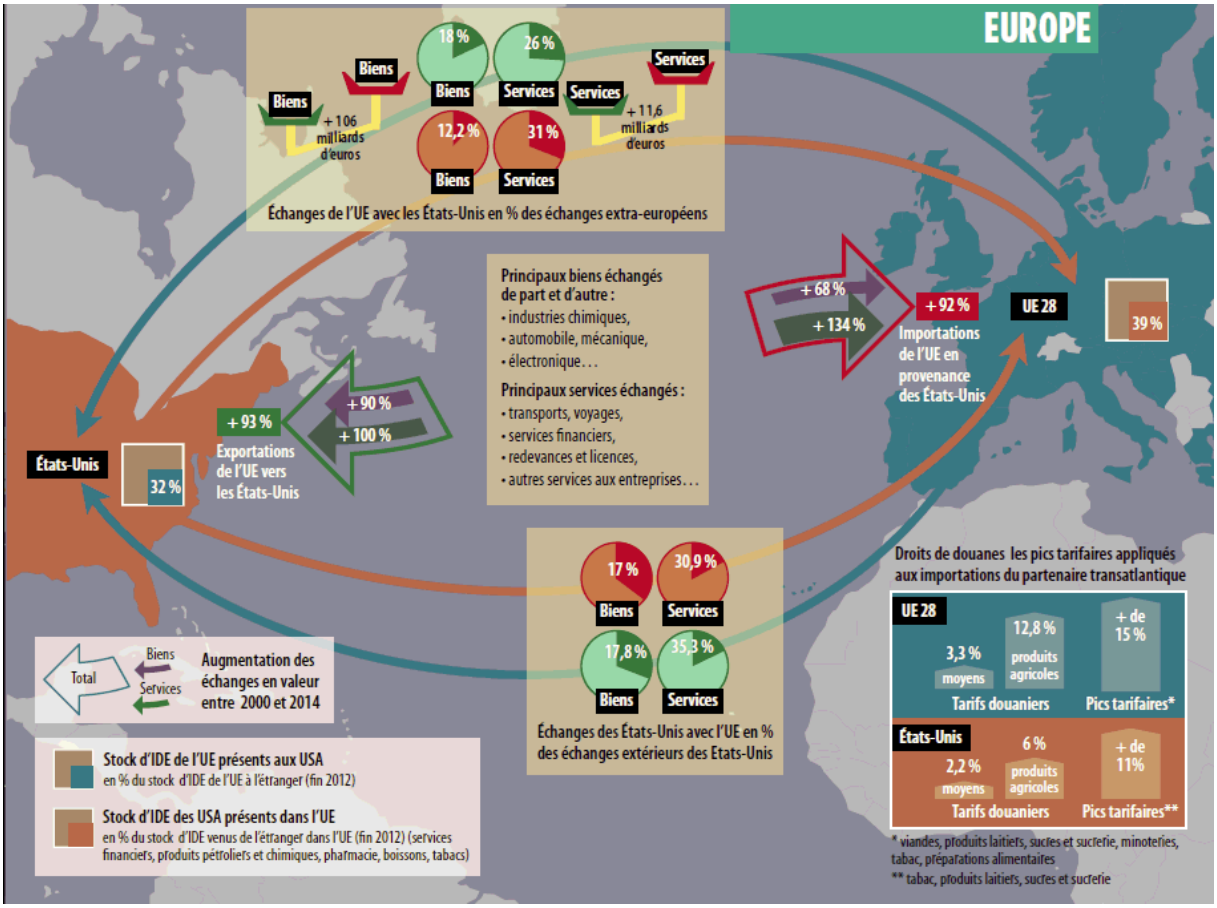


TABLE DES MATIÈRES