L'équivalence de la protection des données personnelles en Union Européenne et aux Etats-Unis - l'affaire Schrems et ses conséquences

Auteur : Leclère, Astrid
Promoteur(s) : Van Cleynenbreugel, Pieter
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en mobilité interuniversitaire
Année académique : 2018-2019
URI/URL : http://hdl.handle.net/2268.2/6875

LIÈGE université
Droit, Science Politique & Criminologie
Département de Droit

L'équivalence de la protection des données personnelles en Union Européenne et aux Etats-Unis - l'affaire Schrems et ses conséquences

Astrid LECLERE

Travail de fin d'études
Master en droit à finalité spécialisée en mobilité internationale.

Année académique 2018-2019

Nombre de caractères: 69 431

Recherche menée sous la direction de :
Monsieur Pieter VAN CLEYNENBREUGEL
Professeur

RESUME

Récemment, différents scandales ont éclaté concernant un manque de sécurité et de protection de nos données personnelles. A la suite des affaires telles que *Cambridge Analytica*, l*'affaire Schrems* et bien d'autres, l'Union Européenne a décidé d'intervenir en légiférant et en adoptant le règlement général sur la protection des données personnelles. Ces données recueillies sur internet peuvent constituer une source très importante d'informations pour les sociétés commerciales. Or, cet échange d'informations peut s'avérer très dangereux quant à la protection de la vie privée et c'est dans ce contexte, que l'Union Européenne est intervenue afin d'offrir un cadre plus protecteur. La première partie de ce travail consistera à analyser ce nouveau système en vigueur. Quel est l'objectif poursuivi par ce règlement? Quelle est sa portée? Quels sont les droits qui y sont repris et comment peut-on les mettre en oeuvre concrètement (droit à l'effacement, à l'oubli etc)? Toutes ces questions feront l'objet d'un traitement approfondi à travers ce travail. Après avoir analysé le système en vigueur au sein de l'Union Européenne, dans une seconde partie, nous tenterons d'analyser l'impact éventuel du RGPD sur les Etats-Unis. Nous nous demanderons également comment fonctionne le système américain actuellement ainsi que les différences qui existent entre les deux systèmes (américain et européen).

REMERCIEMENTS

Fruit de plusieurs mois de recherches, certaines personnes ont également contribué à la réalisation de ce travail de fin d'étude.

D'abord, je souhaiterais remercier mon promoteur de TFE, le professeur PIETER VAN CLEYNENBREUGEL pour avoir suscité mon intérêt dans le domaine du droit européen, notamment à travers le cours de « Droit civil européen ». Plus particulièrement, je le remercie également pour sa disponibilité et pour ses précieux conseils tout au long de ce travail.

Je tiens également à témoigner ma reconnaissance à Maitre FISCHER, ainsi qu'à LOUIS LIBIN, étudiant à l'Université de Tilbourg avec lesquels j'ai pu échanger à propos de ce mémoire.

J'adresse mes plus sincères remerciements à mes parents ainsi qu'à mes frères pour leur soutien inconditionnel tout au long de ce parcours universitaire ainsi que pour les nombreuses relectures.

Enfin, un merci spécifique à MURIEL CAVACCIOCI pour ses conseils sur mon style d'écriture.

TABLE DES MATIÈRES

SECTION 1: INTRODUCTION

A l'ère de la révolution technologique et informatique, à l'aube du développement de l'intelligence artificielle, les données personnelles constituent une mine d'or, notamment pour les GAFAM[1].
Dans une société de plus en plus connectée où les mégadonnées (autrement dit les « *Big Data* ») sont exploitées, parfois à notre insu, l'intérêt de protéger nos données personnelles constitue actuellement un enjeu majeur.

Les données GPS récoltées sur notre téléphone, l'indication du nombre d'heures de sommeil, les calories perdues sur une journée, les données de carte de crédit, les achats effectués en ligne et bien d'autres données dont nous n'avons même pas connaissance, constituent un paradis d'informations.
Ces données peuvent être détournées et utilisées à mauvais escient, notamment pour constituer des « *profils-type* » ou encore pour manipuler des utilisateurs comme dans le cas du scandale de *Cambridge Analytica*.

A l'heure actuelle, qui n'utilise pas l'un ou l'autre réseau social, que ce soit Facebook, Instagram, Twitter ou d'autres? Dans ce contexte, l'adage « *dis moi qui tu fréquentes, je te dirai qui tu e*s » y trouve tout son sens. En effet, les pages « *aimées*», les amis, les centres d'intérêt, les données de localisation constituent des données amassées, stockées et parfois utilisées dans un but bien précis par des entreprises commerciales.
De plus, à l'heure des algorithmes, certaines informations « *cachées* » peuvent être trouvées grâce à un regroupement d'informations. Tout ceci est aux antipodes de la protection de la vie privée, qui est pourtant garantie par l'article 8 de la CEDH.

C'est dans ce contexte, et à la suite d'une prise de conscience collective consécutive aux différents scandales qui ont éclaté, tels que l'*affaire Schrems*, *Cambridge Analytica* ou encore les *révélations d'Edward Snowden*, que l'Union Européenne est intervenue, « *soucieuse de garantir une meilleure protection de la vie privée des Européens, face aux modèles américain ou chinois qui donnent beaucoup plus de latitude pour recueillir et utiliser des données personnelles* »[2].

Cette nécessité de protéger les données personnelles récoltées sur internet n'est pas une nouveauté car il existait auparavant, une directive Européenne n° 95/46 du 24 octobre 1995 qui allait dans ce sens. Cependant, le besoin d'une amélioration de la protection de la vie privée des Européens n'a fait que croitre ces dernières années à la lumière des récents scandales. « *Une réforme de la législation européenne apparaissait nécessaire au regard de sa vétusté, révélée par l'explosion du numérique, l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques* »[3]. Il était en effet souhaitable que l'Union Européenne s'adapte aux évolutions technologiques, ce qui a été fait à la suite de l'adoption

---

[1] Google, Apple, Facebook, Amazon, Microscoft.

[2] A. GUIMOLLES, « L'Europe va mieux protéger la vie privée », 2018, disponible sur https://www.la-croix.com/Economie/Monde/LEurope-mieux-proteger-vie-privee-2018-05-24-1200941278

[3] J. LAUSSON, « RGPD: 15 questions pour comprendre le règlement sur la protection des données personnelles », 2019, disponible sur https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-internaute.html

du règlement Européen n° 2016/670, entré en vigueur le 24 mai 2018, sous le nom de Règlement général sur la protection des données, le RGPD.

A travers ce travail, nous tenterons de déterminer en quoi les différents scandales en la matière ont permis une prise de conscience de la société quant à la nécessité d'une meilleure protection des données récoltées sur internet (section 2).

Ensuite, nous essaierons de déterminer, dans une section réservée à l'Union Européenne (section 3), comment ce Règlement général de la protection des données sera appliqué, d'un point de vue matériel et territorial, tout en examinant également les droits qui en découlent.
Nous terminerons cette section, par une analyse critique de ce nouvel instrument européen et de son efficacité pour les citoyens européens.

Cependant, après l'analyse du système européen, il sera utile de se pencher sur les conséquences de la très médiatique *affaire Schrems*, ainsi que sur l'adoption du *Privacy Shield* et de la décision d'adéquation prise par la Commission Européenne le 12 juillet 2016 (section 4). Par cette décision, la Commission a conclu que les Etats-Unis offraient une protection essentiellement équivalente à celle de l'Union Européenne, ce qui semble néanmoins contesté par différentes critiques émises et par une différence culturelle de taille.

Nous conclurons en tentant de répondre à la question suivante: « *existe-t-il une équivalence de protection des données personnelles en Union Européenne et aux Etats-Unis?* »

« Ce qu'on appelle notre vie privée, c'est ce dont nous avons le droit de priver les autres. »

Gilles Martin-Chauffier

SECTION 2: RÉCENTS SCANDALES

Avant les récents scandales concernant l'utilisation abusive de nos données personnelles, qui parmi nous, prenait le temps de lire les conditions générales du célèbre réseau social, Facebook? Certainement une très faible minorité[4]…
Or, c'est notamment, grâce à ces conditions générales que Facebook « *obtenait le consentement de ses utilisateurs quant à la collecte et à l'analyse de leurs données personnelles* »[5].
Naïveté? Méconnaissance du danger? Désintérêt? Quoiqu'il en soit, les utilisateurs d'internet ont pris conscience du danger et du risque potentiel de violation de leur vie privée.

« *Doit-on craindre pour la protection de notre vie privée?* » [6] est une question qui n'a cessé d'alimenter les débats à la suite des scandales, ceux-ci qui ont permis aux autorités de réagir et d'ouvrir les yeux sur l'ampleur de ce phénomène.
Par conséquent, il semblait essentiel, dans un travail comme celui-ci, de commencer par le commencement, c'est-à-dire, par la prise de conscience de l'intérêt de sauvegarder notre vie privée. Bien que ces affaires ne soient pas des faits isolés, nos propos seront limités à l'analyse de trois scandales à dimension mondiale: les révélations d'Edward Snowden, le scandale *Cambridge Analytica* ainsi que les conséquences de l'affaire Schrems.

1. Les révélations d'Edward Snowden

« *Les révélations de Edward Snowden au sujet de la National Security Agency (NSA) et des moyens employés à un niveau mondial aux fins d'une surveillance illicite de toutes formes de nos communications électroniques, ou via téléphone mobile ou encore Internet ont contribué à sensibiliser un très large public à la question de la protection des données à caractère personnel.*»[7].

En 2013, Edward Snowden a été l'un des précurseurs de cette lutte contre l'utilisation abusive et illégale de nos données personnelles. Il a mis en lumière la surveillance massive des données contenues sur Internet et d'autres plateformes, par les services de renseignements. Ces déclarations ont été les premières en la matière et ont donc eu un impact considérable sur les esprits. Cependant, il serait illusoire de croire que la situation a changé du tout au tout à la suite de cette affaire[8].

En effet, au sein de l'Union Européenne, et 3 ans après le scandale Snowden, le Royaume-Uni a adopté une loi, le 17 novembre 2016, qui a pour objectif d'étendre les pouvoirs de

---

[4] A. EPINEY, D. SANGSUE, « L'ère numérique et la protection de la sphère privée », Schulthess, 2018, p.82.

[5] A. EPINEY, D. SANGSUE, « L'ère numérique et la protection de la sphère privée », Schulthess, 2018, p.82.

[6] L. WESSBECHER, « Netflix et les données personnelles: doit-on craindre pour la protection de notre vie privée? », 2018, disponible sur https://www.france24.com/fr/20180428-netflix-donnees-personnelles-doit-on-craindre-protection-notre-vie-privee

[7] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, p.15.

[8] M. UNTERSINGER « Surveillance: quel bilan tirer, cinq ans après le début des révélations d'Edward Snowden », 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/06/05/surveillance-quel-bilan-tirer-cinq-ans-apres-le-debut-des-revelations-d-edward-snowden_5310017_4408996.html

surveillance des services de renseignements et de police[9,10]. Selon Edward Snowden, « *le Royaume-Uni a légalisé la surveillance la plus extrême des démocraties occidentales. Elle va plus loin que certaines autocraties* »[11]. A ce propos, la CEDH a eu l'occasion de se pencher sur cette loi à travers un arrêt rendu le 13 septembre 2018, par lequel elle a validé le principe de surveillance de masse mais a sanctionné ses modalités qui pour certains aspects, méconnaissent les articles 8 et 10 de la CEDH[12]. Cet arrêt est important car même si ce n'est pas la première fois que la Cour examine les systèmes de surveillance de masse, il s'agit ici de la première affaire « *dans laquelle la Cour étudie spécifiquement la portée de l'atteinte à la vie privée d'une personne qui est susceptible de résulter de l'interception et de l'examen des données de communication* »[13].
Quant à la France, elle a adopté une loi en 2015 créant un « *dispositif qui implique l'analyse des données de navigation de tous les Français, dans le but de repérer quelques individus* »[14].

Cette surveillance massive des services de renseignements s'explique notamment par le contexte terroriste auquel nous devons faire face actuellement, ce qui complique d'avantage la situation. Nous faisons face à deux grandes problématiques: d'une part, protéger la vie privée des individus et d'autre part, protéger la sécurité des citoyens. De la sorte, trouver une solution qui serait à mi-chemin entre ces deux préoccupations essentielles, n'est pas chose aisée et nous n'avons pas la prétention de pouvoir remettre ceci en question dans un tel travail. La surveillance de masse dans le but de protéger les citoyens est un débat qui relève des autorités même s'il faut néanmoins prendre en compte certaines valeurs que la démocratie n'est pas prête à abandonner. Trouver le juste équilibre ne s'avère malheureusement pas simple…

2. **Cambridge Analytica**

La surveillance de masse effectuée par les services de renseignements dans le but de déjouer des attentats ou d'éventuelles attaques de nos démocraties, est une chose bien différente de l'utilisation illicite de nos données personnelles, révélée notamment à la suite du scandale de *Cambridge Analytica* impliquant le géant des réseaux sociaux: Facebook.

Dérober nos données à caractère personnel afin de constituer des profils de consommateur ou encore en vue de manipuler des élections politiques constitue une violation de notre vie privée sans que cela ne puisse faire l'objet d'une quelconque justification.

---

[9] Investigatory Powers Act 2016

[10] « Surveillance: ce que contient la nouvelle loi sur le renseignement britannique », 2016, disponible sur https://www.lemonde.fr/pixels/article/2016/11/21/surveillance-ce-que-contient-la-nouvelle-loi-sur-le-renseignement-britannique_5035373_4408996.html

[11] Propos d'Edward Snowden.

[12] C.E.D.H., 13 septembre 2018, Big Brother Watch et autres c. Royaume-Uni, 58170/13.

[13] FAQ sur l'arrêt Big Brother Watch et autres c. Royaume-Uni.

[14] M. TUAL« Trois ans après les révélations Snowden, la surveillance de masse se porte bien », 2016, disponible sur https://www.lemonde.fr/pixels/article/2016/11/24/trois-ans-apres-les-revelations-snowden-la-surveillance-de-masse-se-porte-bien_5037022_4408996.html

En l'espèce, le scandale *Cambridge Analytica* a éclaté en 2018 à la suite d'une enquête notamment menée par les médias américains « *The New-York Times* » et « *The Observer* »[15]. A la suite d'un test de personnalité réalisé sur Facebook par certains utilisateurs, ces derniers se sont vu dérober, à leur insu leurs données à caractère personnel, entrainant dans leur sillage l'ensemble de leurs amis Facebook. Tout ceci, dans un seul et unique but: constituer un profil politique afin de les influencer, notamment dans les élections présidentielles américaines de 2016[16].

Facebook est ensuite tombé dans la tourmente médiatique et politique engendrée par ce scandale, car le fameux réseau social n'avait pris aucune mesure de sécurité afin d'éviter un tel problème. Cependant, « *aussi choquante soit-elle, l'affaire Cambridge Analytica, n'est qu'un exemple - d'ailleurs relativement mineur - des pratiques en matière de collecte de données et de violation de confidentialité, effectuées de manière systématique et quotidienne par différents acteurs, et notamment les plateformes numériques* »[17].

Nous sommes cependant en droit de nous demander si cette manipulation de données a réellement joué un rôle clef dans la victoire de Donald Trump aux élections présidentielles; mais cette question est un autre sujet de préoccupation même s'il est certain que « *faire passer l'opinion publique entre les mains de ceux qui sont en mesure de payer semblerait saper le fondement même de la démocratie* »[18].

Cet événement a provoqué une onde de choc à dimension mondiale, dans une thématique qui faisait déjà l'objet de vives critiques notamment en raison des lois inadaptées. C'est dès lors dans un contexte très sensible, que le Règlement général de protection des données est entré en vigueur en 2018, afin d'éviter que de tels événements ne se reproduisent dans le futur…

Cependant, il ne faut pas être naïf et penser que seule la société *Cambridge Analytica* dérobait des données à caractère personnel, car il ne s'agissait en réalité que de la partie émergée de l'iceberg, là où d'autres entreprises telles que Google et Facebook « *collectent, analysent et monétisent de manière constante des données sur les individus sans qu'ils en aient réellement conscience*»[19]. Nous tenterons donc par la suite, d'examiner si le RGPD est réellement apte à répondre à cette problématique…

Les révélations d*'Edward Snowden* ainsi que le scandale *Cambridge Analytica* montrent clairement que l'Union Européenne avait besoin d'un nouveau cadre juridique, plus moderne. Auparavant, une autre affaire, tout aussi retentissante avait déjà éclaté et permis une première prise de conscience des autorités: l*'affaire Schrems*. Nous verrons dans la section réservée aux

---

[15] M. GEELKENS, « *Données volées, données protégées… L'année du scandale Cambridge Analytica* », 2019, disponible sur https://www.levif.be/actualite/international/donnees-volees-donnees-protegees-l-annee-du-scandale-cambridge-analytica/article-normal-1069869.html

[16] M. GEELKENS, « Données volées, données protégées… L'année du scandale Cambridge Analytica », 2019, disponible sur https://www.levif.be/actualite/international/donnees-volees-donnees-protegees-l-annee-du-scandale-cambridge-analytica/article-normal-1069869.html

[17] I. MANOKHA, « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » disponible sur https://www.cairn.info/revue-cultures-et-conflits-2018-1-page-39.htm

[18] « Why the Cambridge Analytica scandal matters », disponible sur https://thespinoff.co.nz/politics/21-03-2018/why-the-cambridge-analytica-scandal-matters/

[19] I. MANOKHA, « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » disponible sur https://www.cairn.info/revue-cultures-et-conflits-2018-1-page-39.htm

Etats-Unis l'impact de cette affaire sur la protection des données personnelles ainsi que la réaction de la commission européenne.

SECTION 3: UNION EUROPÉENNE

La protection des données personnelles est un sujet qui a été à la fois fortement influencé par le droit, et ce depuis l'adoption d'une directive européenne le 24 octobre 1995, la directive n°95/46, mais s'est également développée à la suite de plusieurs arrêts rendus par la Cour de Justice de l'Union Européenne[20].

Nous pouvons notamment citer l'arrêt rendu le 8 avril 2014, « *Digital Rights Ireland* »[21] par lequel la CJUE a invalidé une directive sur la conservation des données[22] au motif que « *la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* »[23].

De plus, l'arrêt « *Google Spain »* a également joué un rôle essentiel dans l'évolution de la protection des données personnelles en Europe car il a permis d'une part, d'étendre la notion d'établissement contenue dans la directive via une interprétation extensive, et d'autre part, a consacré le droit à l'oubli[24]. Comme l'illustrent ces différents arrêts, le modèle juridique européen consacré par un nouvel instrument entré en vigueur en 2018, le RGPD, a donc été fortement influencé par la jurisprudence de la Cour de Justice de l'Union Européenne.

Cependant, avant de s'intéresser au Règlement sur la protection des données, il semble également utile d'examiner les raisons pour lesquelles la directive européenne n°95/46 était à bout de souffle et ne correspondait plus aux besoins de cette époque.

1. Directive 95/46

L'Union Européenne est notamment caractérisée par les différentes libertés de circulation, telles que la liberté d'établissement, la liberté de circulation des capitaux, des personnes et des biens, ce qui nécessite automatiquement une certaine liberté de circulation des données. C'est donc dans ce contexte, que très tôt, les Etats-membres de l'Union ont adopté des lois

---

[20] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, p.19.

[21] C.J.U.E. (gde Ch.), 8 avril 2014, *Digital Rights Ireland Ltd*, aff. C-293/12, (ECLI:EU:C:2014:238)

[22] 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 fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

[23] C.J.U.E. (gde Ch.), 8 avril 2014, *Digital Rights Ireland Ltd,* aff. C-293/12, §65.

[24] C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain*, aff. C-131/12,

nationales sur la protection des données personnelles[25]. Cependant, l'utilité d'une harmonisation de ces lois s'est fait sentir très rapidement d'où l'adoption de la directive n° 95/46 entrée en vigueur le 24 octobre 1995.

Cette directive adoptée il y a plus de 20 ans, n'est cependant pas aux antipodes du RGPD, comme nous pourrions le croire à première vue. En effet, la directive et le règlement partagent en réalité le même objectif tendant à harmoniser la protection de la vie privée au sein des Etats-membres tout en permettant également une certaine liberté de circulation des données.

Néanmoins, il est indéniable que d'une certaine manière, la directive était devenue obsolète et qu'il était nécessaire d'adopter un nouvel instrument mieux adapté aux réalités actuelles[26]. En effet, lors de l'adoption de la directive en 1995, l'évolution d'internet ainsi que des nouvelles technologies étaient totalement imprévisibles car nous étions à l'aube de leur développement. C'est notamment pour répondre à ce progrès technique, que le RGPD est né.

« *Consciente du délicat défi du numérique, tout en maintenant le principe de la libre circulation des données* »[27], l'Union Européenne a décidé d'adopter un règlement et non plus une directive qui avait échoué dans l'objectif d'harmonisation des législations des différents Etats-membres. Dans ce contexte, il semble que l'adoption d'un règlement ait été une bonne solution car cet outil permet une intégration et une sécurité juridique beaucoup plus intéressante et dès lors une stabilité permettant un meilleur développement du numérique[28].

Par ailleurs, le règlement apporte sur le fond, des avancées non négligeables. En effet, l'article 4 de la directive prévoyait un champ d'application territorial relativement restreint car la directive ne s'appliquait « *qu'aux traitements de données à caractère personnel lorsque le responsable de traitement est établi sur le territoire de l'Etat membre ou s'il recourt, à des fins de traitement de données à caractère personnel, à des moyens situés sur le territoire d'un Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la communauté*»[29]. Cette disposition avait notamment pour effet que les GAFAM, principalement installés aux Etats-Unis, échappaient au droit de l'Union. C'est donc pour pallier à cette lacune que l'Union a changé cette disposition dans le cadre de son règlement, pour prendre en compte ces différents acteurs.

De plus, là où l'article 7 de la directive prévoyait un consentement indubitable, ce qui était jugé insuffisant, le règlement instaure en son article 4, un consentement spécifique, ce qui constitue une véritable avancée dans la protection des données. Nous verrons cependant par la suite la difficulté qui réside dans la mise en place d'un tel système, face au principe de l'opt out développé par le droit américain[30]…

Même si la directive a eu le mérite d'exister pendant de nombreuses années, celle-ci n'a cependant pas réussi à répondre à certains objectifs: d'une part, elle n'a malheureusement pas

---

[25] PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, p. 29.

[26] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p. 35.

[27] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p. 35.

[28] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelle*s* », Larcier, 2015, p.21.

[29] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.36.

[30] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.36.

permis une harmonisation suffisante des différentes législations, et d'autre part, il était impossible à l'heure de son adoption, d'imaginer l'évolution exponentielle d'internet et du numérique. C'est notamment pour répondre à ces besoins, que l'Union Européenne a adopté le Règlement sur la protection des données personnelles.

2. Règlement général sur la protection des données (RGPD):

C'est dans un contexte de crise, notamment à la suite des différents scandales qui ont éclaboussé les géants d'Internet, que le RGPD a été adopté en 2016 et est entré en vigueur en 2018, abrogeant de la sorte l'ancienne directive n°95/46. Celui-ci a eu pour effet de moderniser le droit de l'Union Européenne en matière de protection des données personnelles en permettant de protéger les droits fondamentaux des citoyens européens face à l'apogée du numérique[31].

Comme l'indique le considérant 9 de ce règlement, l'existence de divergences dans l'application et l'interprétation de la directive de 1995 a mené à des différences de protection des données personnelles. Le Règlement sur la protection des données personnelles constitue donc une réponse à ce problème, car celui-ci doit être appliqué de manière identique au sein des Etats-membres, sans devoir être transposé en droit interne, offrant dès lors une protection cohérente et homogène aux citoyens européens[32].

Dès lors, à travers ce travail, un examen approfondi de ce règlement s'impose. Après avoir exposé les différents objectifs poursuivis par cet instrument juridique, nous nous intéresserons également aux champs d'application *ratione materiae* et *ratione loci*.

En outre, un intérêt tout particulier sera porté à l'étude des différents droits octroyés aux citoyens européens par ce règlement, afin de leur donner un certain contrôle de leurs données personnelles.

Nous terminerons cette partie, par une analyse critique de ce règlement et sur les éventuels obstacles à sa mise en oeuvre.

i. Les objectifs:

Le règlement ne s'éloigne pas totalement de ce qui a été établi il y a 20 ans par la directive mais permet de moderniser le droit en prenant en compte les évolutions du numérique ainsi que la jurisprudence en la matière[33]. Le règlement apporte également certaines nouveautés permettant une meilleure protection des droits fondamentaux garantis par la charte de l'Union Européenne.

---

[31] PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, p.31.

[32] Considérant 10 du RGPD

[33] Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 ».

Premièrement, il offre « *un cadre juridique harmonisé aboutissant à une application uniforme des règles, au profit du marché unique numérique de l'UE* »[34].
Comme expliqué à plusieurs reprises, l'un des objectifs essentiels de la législation européenne est d'éviter une mise en oeuvre de la protection des données personnelles différente d'un état membre à un autre. Ici, il est certain, que chaque état membre et chaque citoyen européen sera protégé de la même manière…

Deuxièmement, l'application identique au sein de l'Union de ce règlement peut constituer une réelle opportunité pour les entreprises. En effet, contrairement à ce qui était applicable auparavant, grâce à l'adoption du RGPD, « *une entreprise qui exerce des activités dans différents pays ne doit plus se conformer à plusieurs réglementations, souvent divergentes, mais uniquement au RGPD si elle souhaite proposer ses services au sein de l'UE* »[35]. Ceci constitue également une opportunité pour les entreprises de retrouver la confiance des consommateurs, perdue à la suite des récents scandales.

Un autre avantage non-négligeable offert aux entreprises européennes consiste en des conditions de concurrence équitables pour l'ensemble des entreprises proposant des biens et services au sein de l'Union Européenne. Cela signifie que le « *règlement exige des entreprises établies en dehors de l'Union Européenne qu'elles appliquent les mêmes règles que celles qui sont installées dans l'Union Européenne dans le cas où elles offrent des biens et services dans le domaine des données à caractère personnel ou surveillent le comportement de personnes dans l'Union* »[36].

Cependant, il est certain que là où le règlement peut être perçu comme une opportunité pour les entreprises, certains inconvénients existent bel et bien. En effet, pour que l'application de ce règlement soit un succès, il faut d'une part que les entreprises soient correctement informées et d'autre part, qu'elles respectent les obligations - obligations spécifiques et potentiellement lourdes - qui leur incombent[37]. En cas de non respect de ces dernières, les entreprises risquent de très fortes amendes, ce qui constitue un réel danger pour les plus petites entreprises. Alors même si en pratique, les obligations ne seront pas identiques en fonction des données traitées et du volume, chaque entreprise qui traite, c'est-à-dire qui utilise, stocke ou transmet des données à caractère personnel, devra se conformer au RGPD, ce qui n'est pas chose aisée pour les petites entreprises[38].

Ensuite, concernant les obligations qui incombent aux sociétés établies en dehors de l'Union Européenne mais offrant des services aux clients établis au sein de l'Union Européenne, la situation s'avère beaucoup plus compliquée et constitue un véritable obstacle à la mise en

---

[34]Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 ».

[35] « Le RGPD, nouvelles opportunités, nouvelles obligations », Commission Européenne, p.2, disponible sur https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_fr.pdf

[36]Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 ».

[37]Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 », pp.13 à 14.

[38] J. GASSEND, « RGPD, GDPR…votre entreprise est-elle prête? », 2017, disponible sur https://www.digitalwallonia.be/fr/publications/gdpr

oeuvre de ce règlement, comme nous tenterons de le comprendre lors de l'analyse critique. En effet, le principe de l'*opt out* est applicable, notamment aux Etats-Unis, où les GAFAM sont implantés, ce qui entraine un souci majeur dans l'application de ce règlement.

En tout cas, il est certain qu'un des objectifs essentiels de ce règlement est de responsabiliser les entreprises sur la problématique du traitement des données personnelles[39].

Troisièmement, le règlement renforce les droits individuels des citoyens européens[40]. En effet, le RGPD offre aux citoyens européens différents droits:

- le « *droit d'accès au données* »[41] ainsi que le « *droit de rectification* »[42] si la personne estime qu'elles sont incorrectes, inexactes ou incomplètes.
- le « *droit à la portabilité* », qui est une nouveauté instaurée par l'article 20 du règlement qui permet de renforcer le contrôle exercé sur nos propres données[43].
- le droit à un « *consentement libre, spécifique, éclairé et équivoque* »[44] car le « *silence ou l'absence de réaction n'auront plus valeur de consentement valable, dès lors que le consentement passera par un acte positif clair* »[45]. Cette consécration d'un consentement univoque et non pas indubitable comme précédemment dans la directive de 1995 a pour effet de couper l'herbe sous le pied du principe de l'*opt out*, consacré aux Etats-Unis. Cependant, nous verrons, qu'en pratique, la mise en oeuvre de ce principe n'est pas aussi simple qu'il n'y parait, notamment en raison du nombre exponentiel de demandes d'acceptation de conditions générales.
- Le « *droit à l'oubli* », autrement appelé « *droit au déréférencement* », ou encore « *droit à l'effacement* » est visé par l'article 17 du Règlement général sur la protection des données, et avait déjà fait l'objet d'une consécration dans l'arrêt *Google Spain*[46]. Cet article est sans nul doute l'un des plus importants de ce règlement à une époque où le numérique, contrairement aux humains, n'oublie rien. Dans ce contexte, l'oubli n'est jamais automatique mais doit faire l'objet d'un acte positif, d'une prise de décision ferme quant à l'envie et au besoin de supprimer l'information en question[47]. Cette disposition permet

---

[39] N. MARTIAL-BRAZ, « La proposition de règlement européen relatif aux données à caractère personnel: transposition du réseau trans Euro experts », Trans Europe Experts, 2014, Vol. 9, p.179.

[40] Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 », p.3

[41] Art. 15 RGPD

[42] Art. 16 RGPD

[43] Art 20 RGPD

[44] Art 4, 11) RGPD

[45] Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 », p.3

[46] C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain*, aff. C-131/12,

[47] C. DE TERWANGNE, « Droit à l'oubli numérique élément du droit à l'autodétermination informationnelle ?», in Le droit à l'oubli numérique : données nominatives – approche comparative (sous la dir. de D. DECHENAUD), Larcier, 2015.

également aux citoyens d'exercer un plus grand contrôle sur la circulation des données personnelles le concernant[48].

En outre, ce règlement est également mieux armé en terme de protection contre les violations de données car un panel de règles importantes a été adopté lorsque « *ladite violation est susceptible d'engendrer un risque pour les droits et les libertés des personnes physiques* »[49].

ii. **Champ d'application matériel**:

Comme l'indique l'article 2, « *le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »[50].

Quant à l'article 4,1), il précise la notion de données à caractère personnel comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable* »[51]. Par personne physique identifiable, il convient d'entendre « *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, psychologique, génétique, psychique, économique, culturelle ou sociale* »[52].
Cela signifie donc que le RGPD ne s'applique pas aux entreprises traitant des données sur les personnes morales (telles que l'objet social, la dénomination sociale etc), sauf si elles traitent également des données sur les représentants de ces personnes morales, ce qui est très souvent le cas[53]. Dès lors, malgré cette définition, on constate que très peu d'entreprises sont exclues du champ d'application matériel de ce règlement.

En outre, la CJUE a interprété de manière assez extensive la notion de données personnelles, notamment dans l'*arrêt Breye*r, rendu le 19 octobre 2016 par lequel la Cour de Justice déclare qu'une adresse IP dynamique peut constituer une donnée personnelle[54]. Or, une adresse IP vise un numéro de machine et non pas un numéro permettant d'identifier directement une personne physique. La Cour a continué dans ce sens, notamment dans son *arrêt Nowak*[55], rendu le 20 décembre 2017 par lequel elle déclare que « *les réponses écrites fournies lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces*

---

[48] S. CARNEROLI, « Le droit à l'oubli. Du devoir de mémoire au droit à l'oubli. », Larcier, 2016.

[49] Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 », p.3

[50] Article 2 RGPD

[51] Art 4, 1) RGPD

[52] Art 4, 1) TGPD

[53] « L'essentiel à connaitre sur le GDPR, RGPD: définition, périmètre, principes et mesures », disponible sur https://www.custup.com/introduction-gdpr-rgdp/

[54] C.J.U.E. (2ème Ch.), 19 octobre 2016, *Breyer*, aff. C-582/14, §43.

[55] C.J.U.E. (2ème Ch.), 20 décembre 2017*, Nowak c.Data Protection Commissione*r, aff. C-434/16

réponses constituent des données à caractère personnel du candidat »[56].
Il est donc indéniable que les autorités ont pris en compte la jurisprudence de la Cour afin de déterminer le champ d'application matériel de ce règlement.

Cependant, une critique peut néanmoins être émise à l'égard du considérant 26 qui énonce que « *il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable* »[57].
En effet, la directive de 1995 avait été critiquée car elle n'avait pas prévu d'éventuelles avancées technologiques, et l'évolution d'Internet. Or, en excluant ces données du champ d'application matériel du règlement, il est envisageable que ce dernier soit un jour dépassé, notamment en raison de moyens imprévisibles actuellement qui permettraient de ré-identifier ces données. Or, vu les sanctions imposées en cas de violation du RGPD aux entreprises, il est fort probable que l'anonymisation devienne un moyen courant d'échapper à cette règlementation[58]…

iii. **Champ d'application territorial**:

Avant même l'adoption du règlement, la notion d'établissement contenue dans la directive de 1995, avait fait l'objet d'une interprétation extensive à la suite de l'arrêt « *Google Spain* »[59].
Le problème principal dans cette affaire résidait notamment dans l'applicabilité ou non de la directive et sur la question suivante: « *la norme européenne peut-elle s'appliquer compte tenu de la localisation géographique de la société mère du groupe Google?* »[60]

Selon la Cour, l'objectif de la directive 95/46 était notamment « *d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privé, à l'égard du traitement des données à caractère personnel* »[61] et dès lors une interprétation extensive était nécessaire afin de se conformer à cet objectif.

Dès lors, le juge européen a considéré que « *compte tenu de cet objectif de la directive 95/46 et du libellé de son article 4, paragraphe 1, sous a), il y a lieu de considérer que le traitement de données à caractère personnel qui est fait pour les besoins du service d'un moteur de recherche tel que Google Search, lequel est exploité par une entreprise ayant son siège dans un État tiers mais disposant d'un établissement dans un État membre, est effectué «dans le cadre des activités» de cet établissement si celui-ci est destiné à assurer, dans cet État*

---

[56] Communiqué de presse de la Cour de justice de l'Union européenne n° 140/17, Luxembourg, le 20 décembre 2017, disponible sur https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-12/cp170140fr.pdf

[57] Considérant 26 du RGPD

[58] C. GALICHET, « Données personnelles: aonymisation, pseudonymisation », 2017, disponible sur https://www.village-justice.com/articles/donnees-personnelles-anonymisation-pseudonymisation,26194.html

[59]C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain,* aff. C-131/12

[60] M. POLIDORI, « L'arrêt Google Spain de la CJUE du 13 mai 2014 et le droit à l'oubli », disponible sur https://www.cairn.info/revue-civitas-europa-2015-1-page-243.htm

[61] Considérant 53 du RGPD

membre, la promotion et la vente des espaces publicitaires proposés par ce moteur de recherche, qui servent à rentabiliser le service offert par ce moteur »[62].

Par cette interprétation juridictionnelle de la Cour, l'affaire *Google Spain* a pu valablement rentrer dans le champ d'application territorial de la directive de 1995, ce qui a eu pour effet d'étendre la notion d'établissement afin de protéger les droits fondamentaux des citoyens européens.

C'est dès lors dans ce contexte de mondialisation, notamment en raison du fait que le traitement des données échappe aux barrières des frontières, que l'extension du champ d'application territorial établi par le règlement constitue une avancée. Le RGPD donne un véritable caractère transfrontalier à sa mise en oeuvre car son article 3 énonce que même lorsque les responsables du traitement des données ne sont pas établis dans l'Union, le règlement est applicable « *lorsque les activités de traitement sont liées a) à l'offre de biens ou de services à ces personnes concernées dans l'Union ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »[63].

Ce champ d'application permet de ne plus se poser de questions comme dans le cadre de l'affaire de *Google Spain* et d'englober dans le champ d'application territorial, les GAFAM installés aux Etats-Unis.

En conclusion, le RGPD s'appliquera d'office si le responsable du traitement est établi au sein de l'Union Européenne, mais également au responsable du traitement établi en dehors de l'Union s'il offre des biens et services à des personnes établies dans l'Union ou s'il suit le comportement de ces personnes. Dès lors, en guise d'illustration, une société japonaise qui crée des profils de clients belges, devra se conformer au RGPD. Par contre, si elle crée des profils de clients américains, le RGPD ne lui sera pas applicable[64].

En outre, le considérant 23 du règlement européen semble nous donner des pistes quant à l'interprétation de l'article 3, reprenant la jurisprudence établie notamment par l'*arrêt Pammer et Hotel Alpenhof* [65]. En effet, la question de l'interprétation des termes « *d'offre de biens et services* » ainsi que du « *suivi de comportement* » est susceptible de poser problème, raison pour laquelle le considérant 23 reprend certaines idées mises en avant par l'arrêt précité. Là où la possibilité d'utiliser une langue ou une monnaie courante d'un des Etats-membres avec la faculté de passer commande dans cette langue peut indiquer l'intention du responsable d'offrir des biens et services[66], la simple accessibilité du site internet ou d'une adresse électronique ne constitue en rien la preuve de cette intention[67].

En conclusion, l'extension du champ d'application territorial dans le cadre du règlement et à la suite de la jurisprudence établie par la Cour, constitue un point essentiel dans le domaine du traitement des données à l'échelle mondiale. Cependant, l'efficacité d'un tel système pose

---

[62] Considérant 55 du RGPD

[63] Article 3 RGPD

[64] « Dans quelle partie du monde le RGPD va s'appliquer? » disponible sur https://www.autoriteprotectiondonnees.be/champ-dapplication-territorial

[65] C.J.U.E (gde Ch.), 7 décembre 2010, *Pammer et Hôtel Alpenhof*, aff. C-585/08 et C-144/09

[66] Considérant 23 du RGPD

[67] Considérant 23 du RGPD; C.J.U.E (gde Ch.), 7 décembre 2010, *Pammer et Hôtel Alpenhof*, aff. C-585/08 et C-144/09

question notamment quant à la capacité de l'Union Européenne d'imposer ce règlement et surtout de veiller à son respect… Nous reviendrons sur ce point lors de l'analyse critique de ce règlement.

iv. **Différents droits consacrés**:

a. Le consentement

Le Règlement sur la protection des données personnelles s'articule autour du principe de transparence[68], qui oblige les entreprises à fournir les informations sur la manière dont les données à caractère personnel seront récoltées et traitées[69].
Il sera donc toujours possible pour les entreprises d'utiliser les données récoltées mais uniquement après en avoir informé les personnes visées.

Ce principe de transparence, s'articule autour du renforcement du consentement qui est défini comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel le concernant fasse l'objet d'un traitement* »[70]. Le règlement s'éloigne donc de la directive sur ce point, en développant le concept d'un consentement qui doit faire l'objet d'un acte positif, et non plus un consentement indubitable synonyme d'une certaine insécurité juridique. En outre, le règlement donne certaines pistes sur la façon dont le consentement peut être donné notamment en cochant une case ou en optant pour des paramètres techniques[71]. A ce propos, l'opinion de l'avocat général concernant l'affaire Planet49 est particulièrement intéressant car selon lui « *demander à un utilisateur de décocher une case et donc de devenir actif s'il n'est pas d'accord avec l'installation de cookies ne respecte pas le critère du consentement actif* »[72].

Cette disposition tente d'échapper au système de *l'opt out* applicable aux Etats-Unis, parfaitement illustré par la citation « *qui ne dit mot consent* » au profit de l*'opt in* où il faut consentir de manière positive. « *L'enjeu pour l'Europe est de ne pas se laisser imposer indirectement les règles du droit américain, étrangères aux traditions juridiques des Etats européens* »[73].

---

[68] Art 12 du RGPD

[69] « L'essentiel à connaitre sur le GDPR, RGPD: définition, périmètre, principes et mesures », disponible sur https://www.custup.com/introduction-gdpr-rgdp/

[70] Art 4, 11) du RGPD

[71] Considérant 32 du RGPD

[72] Conclusions de l'Avocat général, M. SZPUNAR présentées le 21 mars 2019 (1) dans l'Affaire C−673/17 Planet49 GmbH contre Bundesverband der Verbraucherzentralen und Verbraucherverbände Verbraucherzentrale Bundesverband e.V, disponible sur http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=6538073

[73] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe*?* » Larcier, 2015, p.36.

Dans ce contexte, notamment lié au nouveau « *droit à l'oubli* » consacré par le règlement, le consentement pourra être retiré à tout moment par la personne concernée[74].

Cependant, il semble irréel de croire que ce consentement permettra de répondre à l'ensemble des problèmes d'utilisation des données personnelles car ce droit peut facilement faire l'objet de critiques.

Premièrement, le concept de *privacy paradox* peut être soulevé en guise d'inquiétude. A l'ère de la révolution numérique, les utilisateurs d'internet sont à la fois partagés par le souci de protéger leur vie privée ainsi que leurs données personnelles mais également par l'envie de pouvoir bénéficier des nouvelles technologies, mais surtout de pouvoir partager au quotidien des choses particulièrement privées qui devraient à mon sens, plus rester dans la sphère privée[75].
Depuis l'avénement de certains réseaux sociaux tels que Instagram et Facebook, les jeunes ne cessent de publier des photos, des informations privées afin d'être vus et remarqués quitte à faire une croix sur la protection de leur vie privée. « *Cet étalage intime est dû à l'émulation créée par l'interaction avec autrui qui conduit à en révéler toujours davantage et surtout plus que ce que l'on croit* »[76]. Dès lors, face à un tel comportement, où l'envie de poster est omniprésente, la réelle portée de ce consentement peut poser question…

En outre, ce paradoxe de la vie privée n'est pas le seul motif d'inquiétude quant à l'efficacité du consentement introduit par ce règlement. En effet, le principe de transparence qui veut que les utilisateurs soient informés des conditions générales ainsi que de la manière dont seront traité les données récoltées engendre un effet pervers[77]. A l'heure actuelle, il n'est plus possible de naviguer sur internet sans devoir face à un nombre important, voire énorme, de demandes d'acceptation des conditions générales du site ainsi que des cookies. Dans ce contexte, il est devenu presque automatique dans le chef des internautes de cliquer sur le bouton « *j'accepte* » sans pour autant lire les différentes conditions générales. Il est certain que le consentement des utilisateurs, épuisés par ces demandes répétitives est privé d'une grande partie de réflexion…

b. **Droit d'accès**:

L'article 15 du RGPD confère à « *la personne concernée le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel sont ou non traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel* »[78].

Ce droit existait déjà auparavant mais a été renforcé à la suite de la réforme, permettant d'une part de demander à un organisme s'il dispose d'informations nous concernant et le cas

---

[74] Art 7, 3 du RGPD

[75] B. BRAS, « Le privacy paradox et comment le dépasser », disponible sur https://www.cairn.info/revue-francaise-de-gestion-2012-5-page-87.htm

[76] L. PAILLER, « *Les réseaux sociaux sur internet et le droit au respect de la vie privée »,* Larcier, 2012*,* p.112.

[77] B. SHERMER, B. CUSTERS, S. VAN DER HOF, « *The crisis of consent : how stronger legal protection may lead to weaker consent in data protection* », Ethics and Information Technology, vol.16, 2014, p. 177.

[78] Art 15 du RGPD

échéant d'avoir accès à ces dernières[79]. Ce droit est perçu par une majorité de citoyens européens comme le droit le plus important notamment car il permet de savoir quelles sont les informations détenues par les entreprises et dès lors de restaurer une certaine confiance entre les intervenants[80].

En outre, ce droit a été enrichi en permettant aux personnes concernées d'avoir accès à l'origine des données, ce qui est bénéfique sur deux points. D'une part, cela permet de savoir par qui et comment les informations ont été obtenues, ce qui inquiète souvent les personnes concernées[81]. D'autre part, cela permet également de vérifier la licéité de la collecte des données et d'intervenir auprès du premier détenteur si cela a été fait en violation des règles juridiques établies [82].

Dans ce contexte, les utilisateurs ont également le droit de demander à rectifier leurs données si elles ne sont pas correctes afin d'éviter que de fausses informations ne se propagent à l'avenir[83]. Ce droit d'accès et de rectification semble pouvoir répondre à une demande exprimée par les personnes concernées de reprendre le contrôle de leurs données et ainsi , de vérifier l'usage qui en est fait.

c. **Droit à la portabilité**:

Ce droit est intimement lié au droit d'accès et permet aux personnes concernées de reprendre le contrôle des données personnelles transmises à un responsable de traitement, comme l'indique l'article 20 du RGPD.
Ce droit permet aux personnes concernées de recevoir leurs données de la part du responsable de traitement dans un « *format structuré, couramment utilisé et lisible par machine* »[84] et donne également la possibilité de les réutiliser en les transmettant à un autre responsable de traitement.
Cependant, ce droit ne pourra être exercé que lorsque le traitement de données repose sur le consentement ou a lieu dans le cadre de l'exécution d'un contrat, mais ne pourra pas être mis en oeuvre lorsque les données sont utilisées sur base de la loi par exemple[85].

Des lignes directrices ont été adoptées par le groupe de travail « *Article 29* » afin de déterminer comment ce droit peut être mis en oeuvre et également afin de solliciter l'adoption de standards interopérables par les associations professionnelles[86].

---

[79] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.104.

[80] « Selon le RGPD: qu'est-ce-que le droit d'accès? », disponible sur https://www.fairandsmart.com/droit-dacces-donnees-personnelles-rgpd/

[81] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.105.

[82] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.105.

[83] Art 16 du RGPD

[84] Art 20 du RGPD

[85] « Portabilité des données : le nouveau droit consacré par le RGPD *!* », disponible sur https://lexing.be/portabilite-des-donnees-le-nouveau-droit-consacre-par-le-rgpd/

[86] « Portabilité des données : le nouveau droit consacré par le RGPD ! », disponible sur https://lexing.be/portabilite-des-donnees-le-nouveau-droit-consacre-par-le-rgpd/

Ce droit facilite la libre circulation des données entre les différents responsables de traitement au sein de l'Union Européenne et stimule ainsi la concurrence entre ces derniers ainsi que leur compétitivité[87].

Cependant, il faut veiller, lors de la mise en oeuvre de ce droit à la portabilité, de ne pas porter atteinte aux droits et libertés des tiers[88]. Comme l'indique le considérant 68, « *lorsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes conformément au présent règlement* »[89].
Dès lors, afin de protéger les données personnelles des personnes tierces, le traitement par un autre responsable est permis uniquement si les données sont conservées sous le contrôle unique de l'utilisateur demandeur et à des fins personnelles et domestiques[90]. En aucun cas, le responsable de traitement destinataire, ne pourra utiliser ces données à des fins propres, auquel cas ceci pourrait constituer une traitement illicite et abusif[91].

d. **Droit à l'oubli ou droit à l'effacement**:

Déjà Friedrich Nietzsche avait vu clair au 19ème siècle en écrivant cette citation: « *le futur appartient à celui qui a la plus longue mémoire* ». Transposée au monde du numérique, cette citation prend tout son sens car là où la mémoire humaine est faillible, la mémoire d'internet ne l'est pas. Contrairement à la mémoire de l'homme, où l'oubli est issu d'un processus naturel dans lequel l'humain ne retient que les choses importantes, faisant l'impasse sur des détails insignifiants, la mémoire numérique n'oublie rien, sauf si une demande allant dans ce sens est introduite[92].

En l'absence de consécration dans un instrument juridique, le droit à l'oubli ou droit à l'effacement ou encore droit au déréférencement a été reconnu par la Cour de Justice de l'Union Européenne dans l'arrêt de principe, *Google Spain*[93]. Dans cette affaire, un ressortissant espagnol, Monsieur Costeja avait demandé à Google que certaines informations soient supprimées afin qu'elles n'apparaissent plus dans les résultats d'une recherche[94]. En effet, par l'intermédiaire des moteurs de recherche, un nombre incalculable d'informations

---

[87] Lignes directrices du 13 décembre 2016 relatives au droit à la portabilité des données (WP 242), p. 3, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

[88] Lignes directrices du 13 décembre 2016 relatives au droit à la portabilité des données (WP 242), p. 13, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf.

[89] Considérant 68 du RGPD

[90] Lignes directrices du 13 décembre 2016 relatives au droit à la portabilité des données (WP 242), p.14, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

[91] Lignes directrices du 13 décembre 2016 relatives au droit à la portabilité des données (WP 242), p.14, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

[92] C. DE TERWANGNE, « Droit à l'oubli numérique élément du droit à l'autodétermination informationnelle ?», in Le droit à l'oubli numérique : données nominatives – approche comparative (sous la dir. de D. DECHENAUD), Larcier, 2015

[93] C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain*, aff. C-131/12

[94] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p.10.

peuvent facilement être trouvées. Ce faisant, la Cour de Justice a déclaré qu' « u*ne personne peut, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte demander que l'information en question ne soit plus mise à disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information* »[95]. Cependant, par cet arrêt, même si cela constituait une réelle avancée, la Cour a plutôt mis en avant un droit au déréférencement plutôt qu'un droit à l'effacement, un droit à l'oubli du passé.

Il a donc fallu attendre l'adoption du Règlement sur la protection des données pour assister à la consécration officielle de ce droit à l'oubli, de ce droit à l'effacement par l'intermédiaire de l'article 17. Le règlement permet « *l'effacement de ses données, c'est-à-dire leur suppression pure et simple des contenus éditoriaux, tout en imposant des garde-fous, notamment pour éviter d'attenter à la liberté de presse* »[96].

Ce droit à l'oubli numérique n'est pas illimité ni absolu[97] car il se heurte notamment à l'exercice du droit à la liberté d'expression et d'information consacré par l'Union Européenne. En outre, le considérant 153 du règlement, indique également qu'une interprétation large de la notion de « *journalisme* » est nécessaire afin de garantir la liberté d'expression et d'information[98]. De plus, récemment, la Cour de justice de l'Union Européenne a considéré qu'il n'existait pas de droit à l'oubli des données personnelles figurant dans un registre de commerce et a ainsi refusé le droit à l'oubli au nom du droit à l'information[99]. Dans ce contexte, il est permis de douter de l'efficacité de ce droit eu égard aux différentes limitations imposées par le règlement, et à la récente jurisprudence en la matière.

v. **Analyse critique**:

Le règlement sur la protection des données personnelles était un outil indispensable afin de conférer une certaine confidentialité aux données des personnes concernées, tout en respectant le principe de la libre circulation des données.

Assurément, les données personnelles constituent des informations essentielles pour bon nombre d'entreprises commerciales afin de développer une demande qui correspond à la réalité, tout en permettant une innovation sans cesse plus grande. Dans cet ordre d'idée, il semble faux, par exemple, de dire que Facebook est gratuit, car il regorge de données dont la valeur commerciale est inestimable. En outre, l'Union Européenne a affirmé que les données permettaient à la fois le développement économique, la création d'emplois et le progrès sociétal[100].

---

[95] C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain*, aff. C-131/12, §99

[96] S. CARNEROLI, « Le droit à l'oubli. Du devoir de mémoire au droit à l'oubli. », Larcier, 2016, p.72.

[97] Article 17, 3.

[98] Considérant 153

[99] C.J.U.E., 9 mars 2017, *Manni*, C-398/15.

[100] Communication from the Commission "Building a European data economy", COM(2017) 9 final, January 2017, disponible sur https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-9-F1-EN-MAIN-PART-1.PDF

En conséquence et face à ce phénomène mondial, il était obligatoire de développer un instrument juridique à portée internationale car à la suite du développement du commerce international et des nouvelles technologies, le transfert des données ne s'arrêtait plus aux frontières étatiques.
Cependant, face à un tel outil, certaines questions se posent quant à l'efficacité de ce système et nous aborderons, dès lors, en guise de conclusion sur la partie relative à l'Union Européenne, certaines limites (ou critiques) qui peuvent être émises à l'égard de ce règlement

Premièrement, une question se pose quant à l'impact du RGPD sur la compétitivité des entreprises, c'est-à-dire « *leur capacité à faire face à la concurrence sur un marché* »[101]. Un des objectifs avoués lors de la rédaction de ce règlement était de favoriser la concurrence des entreprises situées au sein de l'Union avec les entreprises multi-nationales, souvent situées hors Europe et qui bénéficiaient de règles beaucoup moins strictes. C'est la raison pour laquelle, le RGPD a vocation à s'appliquer de manière extra-territoriale, comme expliqué précédemment. Dans ce contexte, le RGPD est-il réellement bénéfique pour les entreprises et engendre-t-il réellement une concurrence plus équitable entre les Etats?

D'un côté, il est certain que le RGPD a une influence positive sur les entreprises situées en Europe en leur permettant d'avoir le même cadre règlementaire que les entreprises implantées hors de l'Union Européenne, ce qui renforce leur compétitivité. En outre, un point souhaité également par cette réforme était de réduire les coûts ainsi que les exigences administratives, permettant dès lors aux entreprises de se concentrer sur d'autres points[102].
En ce qui concerne les services digitaux, une concurrence réelle existe entre les différents opérateurs, souhaitant conquérir un maximum de clients à travers des services tels que l'offre de musique, les moteurs de recherche, les messageries en ligne[103]… Ces services font l'objet d'une personnalisation sans cesse plus grande et l'analyse des données personnelles constitue un enjeu pour ces entreprises, leur permettant de se distinguer de leur concurrent, en créant des offres différentes qui correspondent parfaitement aux envies de leurs clients. Dès lors, l'application uniforme des règles sur la protection des données personnelles à la fois aux entreprises situées au sein et hors de l'Union, permet d'éviter une attractivité des offres plus importante ailleurs, grâce à une législation qui y serait plus favorable[104].

Néanmoins, cette volonté d'établir une compétitivité plus importante entre les entreprises, peut entrainer un effet regrettable. Il est affirmé depuis de nombreuses années, que l'analyse des données entraine un développement de l'économie et permet une innovation de plus en plus importante de la part des entreprises. En outre, les entreprises analysent nos comportements afin d'établir une offre qui soit la plus adéquate possible. Cette tendance s'observe dans bon nombre de domaines au niveau mondial, tels que l'environnement, la sécurité, l'énergie, l'intelligence artificielle[105]… Or, l'impact du RGPD sur la force d'innovation des entreprises est une question qui mérite d'être soulevée…

---

[101] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p. 157.

[102] « Le RGPD, nouvelles opportunités, nouvelles obligations », Commission Européenne, p.2, disponible sur https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_fr.pdf.

[103] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p. 157.

[104] C. CASTETS-RENARD, « Quelle protection des données personnelles en Europe? » Larcier, 2015, p. 158.

[105] Communication from the Commission "Building a European data economy", COM(2017) 9 final, January 2017, p2., disponible sur https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-9-F1-EN-MAIN-PART-1.PDF

Deuxièmement, « *la qualité du cadre juridique pertinent est aisée à assurer lorsque la réalité qu'il est appelé à régir est stable et intelligible. En revanche, lorsque les faits sont sujets à variation et/ou que leurs implications sont difficiles à appréhender, le régulateur perd ses repères et la malfaçon législative guette* »[106]. Ces propos illustrent parfaitement une des difficultés majeures de ce règlement. En réalité, la combinaison d'un progrès technique rapide et imprévisible, de processus complexes et d'une dimension transnationale constitue un obstacle important à la mise en oeuvre d'un tel instrument juridique.

L'histoire est un éternel recommencement car déjà il y a plus de 30 ans, il était impossible d'imaginer l'avénement des *Big Data* ou encore le développement de l'intelligence artificielle, ce qui a notamment rendu la directive de 1995 complètement obsolète[107]. Or, encore à l'heure d'aujourd'hui, la plus grosse crainte quant à l'application de ce règlement réside dans l'imprévisibilité de l'évolution technologique et numérique de demain.

Troisièmement, il est permis de douter de l'efficacité de ce dispositif eu égard au caractère transnational de celui-ci. En effet, comme développé dans la section réservée au champ d'application territorial, ce règlement a vocation à s'appliquer aux entreprises implantées hors Union qui traitent des données de personnes établies au sein de l'Union. Dès lors, cette disposition signifie également que les autorités européennes doivent contrôler l'application des règles, et le cas échéant sanctionner en cas de manquement[108]. L'exécution des décisions prises sur base du RGPD hors Union constitue aussi une difficulté non-négligeable pour les autorités européennes et fera l'objet d'une analyse ultérieure. L'Union Européenne a développé et mis sur pied ce système afin d'éviter que les Etats-Unis et la Chine n'imposent leurs propres lois en termes de données personnelles, mais il est manifeste qu'il ne sera pas aussi simple qu'il n'y parait de mettre en oeuvre ce système et de veiller à son respect, notamment en raison des différents principes qui régissent les autres systèmes juridiques tels que l'*Opt out* américain.

Et quatrièmement, afin de clôturer cette analyse critique, il semble qu'un élément sur lequel les autorités européennes n'ont pas prise, risque de rendre la mise en oeuvre de ce règlement compliquée. En effet, une spirale négative quant à la protection de la vie privée semble continuer de se dessiner car vu l'ampleur des différents réseaux sociaux, les utilisateurs ne cessent de publier des informations privées, des photos… Alors même si les outils ont été développés, le système ne peut fonctionner qu'avec la collaboration des personnes concernées. Si celles-ci ne lisent pas les conditions, mais donnent quand même leur consentement, les objectifs de ce règlement ne seront pas totalement rencontrés…

---

[106] A. EPINEY, D. SANGSUE, « L'ère numérique et la protection de la sphère privée », Schulthess, 2018, p.29.

[107] A. EPINEY, D. SANGSUE, « L'ère numérique et la protection de la sphère privée », Schulthess, 2018, p.30.

[108] L. CHERUY, ., « Protection des données personnelles : se mettre en conformité d'ici le 25 mai 2018 », Montrouge, Editions Législatives, 2017, p.23.

SECTION 4: LES ETATS-UNIS

Après avoir dressé un aperçu du Règlement sur la protection des données personnelles adopté par l'Union Européenne, la question se pose de savoir si les Etats-Unis offrent une protection équivalente en termes de données à caractère personnel.
A cette fin, l'analyse de l'*affaire Schrems* et de ses conséquences, notamment l'invalidation de l'accord *Safe Harbor* et de l'adoption dans la foulée, du *Privacy Shield* sera nécessaire. Dans ce contexte, il sera également intéressant de se pencher sur la décision rendue par la commission européenne le 12 juillet 2016 à travers laquelle l'équivalence de la protection des données personnelles a été reconnue entre les Etats-Unis et l'Union Européenne[109].
Nous examinerons ensuite les différentes raisons qui ont poussé l'Union à reconnaître cette équivalence ainsi que les garanties offertes par les Etats-Unis. Ces propos permettront de clôturer notre travail sur une conclusion à deux vitesses car la décision à laquelle la commission est arrivée peut faire l'objet de certaines critiques.

1. L'affaire Schrems

Bien que le scandale Cambridge Analytica ait été très médiatisé, cette affaire ne fut pas la première en ce qui concerne la protection des données personnelles. Auparavant, une affaire dénommée affaire Schrems avait été retentissante entrainant une première prise de conscience de la part de nos dirigeants politiques. Il est certain que c'est à la suite de ce premier scandale que les autorités se sont rendu compte du réel fléau et de l'intérêt de mettre en oeuvre un nouveau dispositif juridique. Dans le cadre de ce travail, une attention toute particulière sera consacrée à l'analyse des conséquences de cette affaire, notamment par l'intermédiaire du Privacy Shield et de la décision de la commission européenne du 12 juillet 2016.

Max Schrems a fait de cette lutte pour la protection de la vie privée, un combat personnel. Dans cette affaire, Schrems s'est rendu compte qu'une partie, voire la totalité de ses données recueillies sur Facebook avaient été transférées vers un serveur américain. Or, à la suite des révélations d'Edward Snowden sur les pratiques américaines en termes de surveillance de masse, Max Schrems a porté plainte auprès des juridictions irlandaises, craignant une potentielle violation de sa vie privée vu les législations américaines insuffisantes en la matière[110]. Cette affaire particulièrement complexe a été portée devant la Cour de Justice de l'Union Européenne[111] qui a notamment déclaré que « *pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou*

---

[109] 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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016.

[110] PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, p. 256.

[111] C.J.U.E. (gde Ch.), 6 octobre 2015, *Schrems*, aff. C-362/14

que les intéressés aient ou non subi d'éventuels inconvénients en raison de cet ingérence»[112].
Dans cette affaire, il a été jugé que les Etats-Unis n'offraient pas une protection essentiellement équivalente à celle de l'Union Européenne et que de ce fait, certains droits fondamentaux contenus dans la charte des droits fondamentaux avaient été violés[113]. C'est à la suite de cette affaire, que la CJUE a invalidé l'accord *Safe Harbor*[114] qui permettait un transfert de données entre les Etats-Unis et l'Union Européenne, notamment utilisé par de nombreuses sociétés commerciales**[115]**.

A la suite de la caducité de l'accord *Safe Harbor*, l'Union Européenne ainsi que les Etats-Unis sont intervenus afin de mettre sur pied un nouveau bouclier quant à la protection des données personnelles en adoptant le *Privacy Shield* . Ce nouvel instrument juridique a ensuite été jugé par la Commission Européenne comme « *garantissant un niveau de protection adéquat des données à caractère personnel transférées de l'Union à des organisations situées aux Etats-Unis*»[116].
La section suivante sera donc réservée à l'analyse des conséquences de cette affaire sur le plan des données à caractère personnel.

2. Les conséquences de l'affaire Schrems

Comme expliqué précédemment, les conséquences de cette affaire sont pour le moins importantes et la nécessité de les développer s'impose.
Premièrement, elle a eu pour effet d'entraîner l'invalidation du *Safe Harbor*, autrefois applicable entre l'Union Européenne et les Etats-Unis en cas de transfert de données. Ce mécanisme n'offrait nullement une sécurité juridique satisfaisante et une protection adéquate des données comme le souhaitait l'Union Européenne[117].

Deuxièmement, à la suite de l'invalidation de cet accord, la nécessité de développer un nouveau bouclier de protection des données personnelles n'a cessé de croître, raison pour laquelle le *Privacy Shield* a été adopté, en vue de répondre à ces critiques et d'offrir une protection équivalente entre l'Union Européenne et les Etats-Unis.

Troisièmement, et certainement le point crucial de ce travail, la Commission Européenne a reconnu l'équivalence de la protection des données personnelles du régime américain octroyé par l'intermédiaire de cet accord avec celui applicable au sein de l'Union. Les différentes caractéristiques du régime américain seront donc analysées afin de comprendre la raison pour laquelle la Commission a pris une telle décision.

---

[112]C.J.U.E. (gde Ch.), 6 octobre 2015, *Schrems*, aff. C-362/14; §87.

[113] PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, p.257; C.J.U.E. (gde Ch.), 6 octobre 2015, Schrems, aff. C-362/14; §73-74

[114] C.J.U.E, Schrems, op. cit., §106

[115] H. KUCHLER« Max Schrems, l'homme qui est parti en guerre contre Facebook et l'a gagnée », 2018, disponible sur. https://www.lenouveleconomiste.fr/financial-times/max-schrems-lhomme-qui-est-parti-en-guerre-contre-facebook-et-la-gagnee-63115/

[116] PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, p.257.

[117] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, p.125.

a. Abolition de Safe Harbor

Le *Safe Harbor* a été négocié au début des années 2000 entre les Etats-Unis et la Commission Européenne et impliquait un ensemble de principes basés en grande partie sur ceux repris dans la directive européenne n°95/46 du 24 octobre 1995[118]. Cet accord prévoyait des droits tels que l'information des personnes; le consentement explicite pour certaines données plus sensibles; le droit d'accès et de rectification; la possibilité de s'opposer à un transfert ou une utilisation des données à caractère personnel pour des finalités différentes et bien d'autres[119]…

La naissance de ce dispositif est en réalité issue du fait que la directive de 1995 interdisait le transfert de données à caractère personnel de l'Union vers des pays tiers sauf si ces derniers offraient un niveau adéquat de protection[120]. Cependant, le terme « *adéquation* » a soulevé de nombreuses questions, raison pour laquelle il était nécessaire de développer un cadre plus prévisible contenant des principes précis, ce qui a été mis en oeuvre par l'intermédiaire de l'accord *Safe Harbor*[121].
Par ce système, les organisations et entreprises américaines qui adhéraient à cet accord, s'engageaient à assurer un niveau de protection équivalent à celui accordé au sein de l'Union Européenne[122] et « *de cette manière, les Etats-Unis et les seules entreprises qui avaient adhéré au Safe Harbor, constituaient une exception à l'interdiction de principe d'exportation des données à caractère personnel européennes, hors de l'Union Européenne* »[123].

Cependant, dans le cadre de l'*affaire Schrems*, la légalité de l'accord a été remise en question, notamment en raison du fait que celui-ci ne semblait plus octroyer un niveau de protection adéquat des données. Or, à la suite des révélations d'Edward Snowden sur la collecte de masse des informations personnelles, de plus en plus de doutes émergeaient sur le niveau de protection offert par les Etats-Unis jusqu'à cet arrêt rendu le 6 octobre 2015 par lequel la Cour de Justice de l'Union Européenne a invalidé l'accord *Safe Harbor*[124].

Dans ce contexte, les conséquences de cette invalidation étaient plus que colossales car « *tout transfert de données personnelles vers les Etats-Unis était illégal, sauf autorisation expresse*

---

[118] « Safe Harbor », disponible sur https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf

[119] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, p.125.

[120] « Guide to self-certification » US and UE, safe harbor framework » p.10, disponible sur https://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

[121]« Guide to self-certification » US and UE, safe harbor framework » p.10, disponible sur https://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

[122] O. ITEANU, « Safe Harbour et Privacy Shield pour les nuls », disponible sur https://www.eurocloud.fr/safe-harbour-privacy-shield-nuls/

[123] O. ITEANU, « Safe Harbour et Privacy Shield pour les nuls », disponible sur https://www.eurocloud.fr/safe-harbour-privacy-shield-nuls/

[124] C.J.U.E. (gde Ch.), 6 octobre 2015, *Schrems*, aff. C-362/14

d'une CNIL Européenne qui pouvait être accordée au cas par cas sur demande, ou à l'intérieur d'un groupe, ou sur la base de contrats conclus entre les opérateurs »[125].

Dès lors, et à la suite de cette décision, l'urgence était de mise dans le chef de la Commission européenne d'adopter un nouvel accord permettant l'échange de données à caractère personnel afin d'éviter l'impact désastreux sur le flux transfrontalier ainsi que sur les potentielles pertes économiques[126]. C'est ainsi qu'un nouveau bouclier de protection des données personnelles, le *Privacy Shield* a été adopté prévoyant « *des normes renforcées en matière de protection des données personnelles, assorties de contrôles plus rigoureux visant à en assurer le respect* »[127].

b. Adoption du Privacy Shield

Ce programme appelé *Privacy Shield* ou encore « *bouclier de protection des données* » a été adopté le 12 juillet 2016 et est devenu opérationnel le 1er août 2016[128].
Mais en quoi, ce programme diffère-t-il de son prédécesseur et quelles sont les garanties offertes par les Etats-Unis afin d'offrir une protection essentiellement équivalente comme réclamée à la suite de l'*arrêt Schrems*? Le *Privacy Shield* offre-t-il une meilleure protection que le *Safe Harbor* ou sommes-nous plutôt face à un *Safe Harbor 2.0*?

Le *Safe Harbor* fut un succès durant ses premières années jusqu'au moment où de nombreuses critiques ont été émises à son égard, notamment en raison d'un manque de contrôle et de sanction, qui ont mené à son invalidation comme expliqué auparavant. Le rôle de l'échange des données personnelles dans la relation Union Européenne et Etats-Unis constitue un aspect essentiel dès lors que tous deux poursuivent des objectifs économiques et politiques communs. Il était nécessaire d'adopter de manière urgente un nouvel accord concernant cet échange et ce transfert des données car « *de nombreux transferts de données vers les Etats-Unis étaient devenus illégaux, car un très grand nombre d'entreprises se fondaient sur les dispositions d'une décision qui n'existait plus pour transmettre des données aux Etats-Unis* »[129].

Afin de remplacer le dispositif précédent, le 2 février 2016, un premier accord politique a été adopté sous le nom « *bouclier vie privé UE-Etats-Unis* », celui-ci visant « *à protéger les droits fondamentaux des citoyens de l'Union lorsque leurs données sont transférées vers les États-Unis et à apporter une sécurité juridique aux entreprises* »[130].

---

[125] O. ITEANU, « Safe Harbour et Privacy Shield pour les nuls », disponible sur https://www.eurocloud.fr/safe-harbour-privacy-shield-nuls/

[126] A. GROSJEAN, « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, p.125.

[127] Communiqué de presse de V. JOUROVA, Commission européenne, « La Commission européenne lance le bouclier de protection des données UE-États-Unis: une protection renforcée pour les flux de données transatlantiques », Bruxelles, le 12 juillet 2016.

[128] B. DOCQUIR, « Vers un droit européen de la protection des données? », Larcier, 2017, Bruxelles, p.71.

[129] Groupe de travail « ARTICLE 29 », « Document de travail 01/2016 sur la justification des ingérences dans les droits fondamentaux à la vie privée et à la protection des données découlant de mesures de surveillance lors du transfert de données à caractère personnel (garanties essentielles européennes) », 13 avril 2016.

[130] Communiqué de presse de la Commission Européenne, « 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» », Strasbourg, le 2 février 2016.

Cependant, afin d'être jugé comme offrant une protection essentiellement équivalente, cet accord devait tenir compte à la fois de certaines recommandations faites par la Commission Européenne avant l'*affaire Schrems* et bien entendu des exigences énoncées par la CJUE à la suite de cette affaire. Néanmoins, dans un premier temps, certains manquements avaient été pointés du doigt, à la fois par le groupe de travail « *Article 29* » (ci-après G29) et par le contrôleur européen des données personnelles[131]. Selon ce dernier, le projet tel que rédigé en février 2016 n'offrait notamment pas « *l'ensemble des garanties nécessaires à la sauvegarde des droits de la personne au respect de la vie privée et à la protection des données de l'UE, ni en ce qui concerne les recours judiciaires* »[132].
Quant au G29, il regrettait l'absence de certaines garanties essentielles, nécessaires à la protection des droits fondamentaux des citoyens européens. Selon ce groupe de travail, il était inconcevable que ce projet ne mette pas en lumière une certaine limitation de la durée de la conservation des données. En outre, « *le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens* »[133].

A la suite de certaines modifications dans ce projet, le 12 juillet 2016, une décision d'adéquation a été adoptée par la Commission européenne, « *constatant qu'un pays tiers offre un niveau de protection adéquat des données à caractère personnel, par l'application de sa législation nationale et le respect de ses engagements internationaux* »[134]. Cette décision, essentielle, a permis que les données soient à nouveau transférées en toute légalité par les entreprises américaines qui ont adhéré à cet accord.

c. Décision d'adéquation du Privacy Shield par la Commission Européenne

A l'heure où un partenariat entre les Etats-Unis et l'Union européenne s'avère être d'une importance capitale, notamment à travers le secteur commercial mais également dans le domaine des services répressifs, il était urgent de redonner confiance aux Européens et ce grâce à de solides garanties[135].

C'est dans ce contexte, que la Commission a adopté une décision d'adéquation du bouclier de protection des données le 12 juillet 2016[136].
A travers cette section réservée à cette décision, nous tenterons d'examiner les raisons qui ont

---

[131] Contrôleur européen de la protection des données personnelles, « Résumé de l'avis du Contrôleur européen de la protection des données concernant le «Bouclier vie privée UE - États-Unis» (Privacy Shield) — Projet de décision d'adéquation »

[132] Contrôleur européen de la protection des données personnelles, « Résumé de l'avis du Contrôleur européen de la protection des données concernant le «Bouclier vie privée UE - États-Unis» (Privacy Shield) — Projet de décision d'adéquation »

[133] « Adoption de la décision d'adéquation du Privacy Shield par la Commission Européenne », 2016, disponible sur https://www.cnil.fr/fr/adoption-de-la-decision-dadequation-du-privacy-shield-par-la-commission-europeenne

[134] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

[135] Communication de la Commission au Parlement Européen et au Conseil, « Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides », 29 février 2016.

[136] 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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016.

influencé la Commission à conclure en faveur de l'équivalence. Cependant, peu après l'entrée en vigueur de cet accord, certaines critiques ont déjà été émises quant à la réelle efficacité de ce dispositif. L'enjeu de ce travail réside en grande partie à travers cette analyse…

- **Les principes du Privacy Shield**

Afin d'analyser les raisons pour lesquelles la Commission a opté pour l'équivalence du système américain, indispensable pour permettre la commercialisation des données hors Union Européenne, il sera utile d'examiner les grands principes de ce dispositif.

A l'instar de l'accord *Safe Harbor*, le *Privacy Shield* repose sur un système d'auto-certification par lequel les entreprises qui ont adhéré à celui-ci s'engagent à respecter et à mettre en oeuvre les différents principes qui y sont développés[137]. Ce point-ci constitue une différence importante avec le système du RGPD, qui ne repose pas sur le fait d'y adhérer mais est automatique lorsque certaines conditions sont réunies tel qu'expliqué auparavant dans l'analyse du Règlement.

Cet accord met à charge des entreprises des exigences plus strictes et renforce les mesures de contrôle et de sanction, jugées insuffisantes dans le dispositif précédent. Cependant, une analyse en profondeur de ces principes ne s'avère malheureusement pas possible à travers un tel travail, dès lors nous examinerons principalement les 3 grands volets sur lesquels repose le bouclier de protection des données personnelles.

Premièrement, les entreprises qui traitent des données personnelles devront respecter des obligations plus strictes, et ce afin de protéger les droits fondamentaux des citoyens européens[138].

D'abord, l'annexe II du *Privacy Shield*, publiée par le ministère américain du commerce, prévoit toute une série d'informations qui doivent nécessairement se retrouver dans les politiques de confidentialité des entreprises qui ont adhéré à ce dispositif, afin de permettre une transparence beaucoup plus importante[139].

Ensuite, les obligations des entreprises ont été renforcées en cas de transfert ultérieur de données vers d'autres entreprises, telles que des sous-traitants. Le même niveau de protection doit être offert à chaque étape, dès lors si une entreprise n'est plus capable d'offrir une protection appropriée, des mesures spécifiques devront être prises[140].

En outre, des mécanismes de surveillance ont été mis en place afin de vérifier que les entreprises qui ont adhéré à ce système respectent les principes auxquels elles se sont

---

[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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016, §14.

[138] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

[139] B. DOCQUIR, « Vers un droit européen de la protection des données? », Larcier, 2017, Bruxelles, p.73.

[140] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

engagées[141]. Le cas échéant, en cas de manquement, certaines sanctions peuvent être prises et ceci pouvant aller jusqu'à la radiation[142].

Enfin, afin de répondre aux critiques émises notamment par le G29, la décision d'adéquation du *Privacy Shield* a été rendue possible en raison de l'évolution du projet et de l'insertion d'une disposition concernant la conservation des données qui stipule que « *les entreprises ne peuvent conserver des données à caractère personnel qu'aussi longtemps que leur conservation répond aux finalités pour lesquelles elles ont été initialement collectées* »[143].

Deuxièmement, et ceci à la suite des révélations d'Edward Snowden à propos de la surveillance de masse, le gouvernement américain s'est engagé à limiter l'accès et l'utilisation des données personnelles à des fins de sécurité nationale. En effet, « *le bouclier de protection des données garantit que les autorités publiques américaines n'accèderont à nos données que dans la mesure nécessaire à la poursuite d'un objectif d'intérêt public, tel que la sécurité nationale ou l'application des lois* »[144].
A travers cet accord, la Commission a réussi à obtenir une promesse du gouvernement américain de donner la priorité à une collecte de données ciblées par rapport à une collecte de masse[145]. Certains parlent de « *promesses fortes* » prises par les Etats-Unis qui garantissent qu'aucune surveillance de masse ne sera observée sur les données à caractère personnel, tandis que d'autres estiment qu'il ne s'agit ici que d'une manoeuvre hypocrite visant à obtenir cette décision d'adéquation car en réalité, rien n'a été modifié dans le droit américain. En effet, la collecte des données peut toujours être justifiée par des fins de sécurité nationale, « *un motif comprenant des objectifs aussi larges que non définis* »[146].

Dans ce contexte, les Etats-Unis se sont engagés à collecter des données en « *vrac* » uniquement sous certaines conditions car « *la collecte de renseignements doit toujours être « aussi ciblée que possible » et la communauté du renseignement doit accorder une priorité élevée à la disponibilité d'autres informations et d'autres solutions appropriées et faisables* »[147].

---

[141] S. LE CALME, « Le CNNum estime que le Pricacy Shiel, l'accord entre l'UE et les USA sur les transferts de données doit être renégocié », 21 septembre 2017, disponible sur https://www.developpez.com/actu/161504/Le-CNNum-estime-que-le-Privacy-Shield-l-accord-entre-l-UE-et-les-USA-sur-les-transferts-de-donnees-doit-etre-renegocie/

[142] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

[143] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

[144] « Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.6.

[145] S. LE CALME, « Le CNNum estime que le Pricacy Shiel, l'accord entre l'UE et les USA sur les transferts de données doit être renégocié », 21 septembre 2017, disponible sur https://www.developpez.com/actu/161504/Le-CNNum-estime-que-le-Privacy-Shield-l-accord-entre-l-UE-et-les-USA-sur-les-transferts-de-donnees-doit-etre-renegocie/

[146] S. LE CALME, « Le CNNum estime que le Pricacy Shiel, l'accord entre l'UE et les USA sur les transferts de données doit être renégocié », 21 septembre 2017, disponible sur https://www.developpez.com/actu/161504/Le-CNNum-estime-que-le-Privacy-Shield-l-accord-entre-l-UE-et-les-USA-sur-les-transferts-de-donnees-doit-etre-renegocie/

[147] 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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016, §71.

Enfin, afin de mettre tout en oeuvre pour éviter une surveillance de masse, ce qui effraie la population européenne, les autorités américaines se sont également engagées à créer un nouveau mécanisme de contrôle et de surveillance en la personne du médiateur du bouclier de protection des données personnelles[148]. Celui-ci permet une meilleure sécurité juridique car il veille d'une part à ce que les réclamations soient bien traitées et d'autre part, que les lois des Etats-Unis aient bien été respectées et en cas de violation de ces dernières, que des sanctions soient appliquées[149]. De plus, ce dispositif de contrôle n'est pas uniquement applicable aux réclamations portées à l'encontre d'entreprises ayant adhéré au *Privacy Shield* car il s'applique à tous types de transferts commerciaux de données personnelles depuis l'Union Européenne vers les Etats-Unis[150].

Bien que ceci ne constitue pas des évolutions juridiques au sens strict, étant donné qu'il ne s'agit « *que de promesses* » et que la loi américaine reste en grande partie inchangée à cet égard, il s'agit d'un signal politique fort de la part des Etats-Unis qui souhaite montrer au reste du monde, et en particulier à l'Union Européenne que les choses évoluent…

Troisièmement, et dernier volet du bouclier, les citoyens européens bénéficieront d'une protection plus efficace et plus effective qu'auparavant notamment grâce à des mécanismes de recours. En effet, il a souvent été reproché à l'accord *Safe Harbor*, un vide juridique en ce qui concerne les voies de recours et le règlement de litiges. Dorénavant, le bouclier permet aux citoyens européens qui estiment que leurs données personnelles ont été utilisées à des fins abusives, d'obtenir réparation et ce par l'intermédiaire de différents recours plus accessibles et plus abordables qu'auparavant.

En effet, le non-respect des règles auxquelles se sont engagées les entreprises lorsqu'elles ont adhéré au bouclier entraîne dans le chef des personnes, un droit à porter réclamation et à obtenir réparation en cas d'utilisation abusive de leurs données[151]. Face à de tels manquements, plusieurs solutions s'offrent aux plaignants.

D'une part, ils ont la possibilité d'introduire une réclamation directement à l'entreprise qui a adhéré au bouclier et qui sera chargée de traiter la plainte elle-même. Cependant, les entreprises ont également la possibilité d'adhérer gratuitement à un mécanisme de recours indépendant qui constitue un mode extrajudiciaire de règlement des litiges[152]. « *Ces organismes doivent être en mesure d'imposer des actions correctrices et des sanctions efficaces pour garantir que la société adhérant au bouclier de protection des données remplit son obligation* »[153]. Si la société n'opte pas pour cette solution, elle a également la possibilité de choisir d'être sous la surveillance d'une autorité nationale de l'Union Européenne chargée de la protection des données (Data Protection Authority).

---

[148] 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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016, §65.

[149]« Guide du bouclier de protection des données personnelles UE- Etats-Unis », pp. 9 à 10.

[150] « Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.10.

[151]« Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.5.

[152] Fiche d'information de la commission européenne, « Le bouclier de protection des données UE-États-Unis: Foire aux questions », Bruxelles, le 12 juillet 2016.

[153] « Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.7.

D'autre part, en tout état de cause, les particuliers auront toujours la possibilité d'introduire une réclamation devant une DPA qui pourra ensuite porter celle-ci devant le Ministère du commerce américain ou devant la Commission fédérale du commerce qui devront tous deux traiter cette plainte dans les plus brefs délais afin de garantir le droit à la protection des données aux particuliers[154].

Cependant, si aucune solution n'est apportée à la suite de ces différents recours, ou si un particulier la juge insuffisante et/ou insatisfaisante, il aura la possibilité en dernier ressort de recourir à un mécanisme d'arbitrage contraignant[155].

Parallèlement à ces trois volets que nous venons de développer, les particuliers disposent d'autres droits s'insérant dans la volonté de protéger leurs données personnelles telles que le droit d'être informé, le droit d'accéder à leurs données ainsi que le droit d'en demander la rectification si cela s'avère nécessaire.

C'est en raison de l'ensemble des garanties reprises dans le cadre du *Privacy Shield* et de tout ce qui vient d'être développé que la Commission a adopté une décision d'adéquation à l'égard de ce système et a conclu en faveur de l'équivalence du système américain. Cette décision était nécessaire au regard des enjeux économiques que représente le flux transfrontalier de données entre l'Union et les Etats-Unis mais fait déjà l'objet de nombreuses critiques peu après son entrée en vigueur. Nous allons donc en aborder quelques-unes avant de nous pencher sur quelques caractéristiques et valeurs fondamentales applicables aux Etats-Unis; celles-ci permettent de remettre en question la conclusion à laquelle est arrivée la Commission à propos de l'équivalence de la protection des données personnelles aux Etats-Unis et au sein de l'Union Européenne.

- **Les critiques**

Ce n'est pas parce que la Commission a adopté cette décision d'adéquation, que le système est parfait et ne fait pas l'objet de critiques, bien au contraire…

En effet, peu après l'adoption de cette décision, le G29 déplorait notamment l'absence de garanties plus strictes par rapport à l'indépendance du médiateur, actif notamment lorsque les pouvoirs publics accèdent aux données personnelles[156]. De plus, la question de l'effectivité des engagements pris par le gouvernement américain est souvent remise en question dans le cadre de la surveillance de masse.

En outre, le G29 se plaint également de l'existence de discordances entre le régime américain et le régime européen, ce qui ne permet pas selon lui une réelle équivalence et surtout nous fait penser que le *Privacy Shield* n'est en réalité qu'un dispositif transitoire, construit sur des bases similaires que le *Safe Harbor,* et le cas échéant susceptible de connaitre le même destin que ce dernier[157].

---

[154] « Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.8.

[155] « Guide du bouclier de protection des données personnelles UE- Etats-Unis », p.8.

[156] Groupe de travail « ARTICLE 29 », « Déclaration du G29 relative à la décision de la Commission européenne concernant le Privacy Shield (bouclier de protection des données UE-États-Unis) », 29 juillet 2016.

[157] O. ITEANU, « Safe Harbour et Privacy Shield pour les nuls », disponible sur https://www.eurocloud.fr/safe-harbour-privacy-shield-nuls/

De plus, la Commission a rendu un premier rapport annuel qui met en lumière des lacunes, relevées également par le G29 et auxquelles il faut remédier de manière urgente notamment en raison d'un manque d'accessibilité aux informations aussi bien pour les sociétés qui adhèrent au *Pricacy Shield* qu'aux citoyens européens ainsi que les interrogations par rapport aux garanties offertes par les Etats-Unis dans le traitement de données à caractère personnel à des fins de sécurité nationale[158].

Le 5 juillet 2018, le Parlement Européen a adopté une résolution non-coercitive visant à suspendre cet outil, ce qui prouve que la perspective d'avenir de ce dispositif semble plus sombre que ce que souhaite la Commission[159].

Dès lors, le *Privacy Shield* s'impose plutôt comme un dispositif transitoire, dans l'attente d'un nouvel instrument qui permettrait de répondre à toutes les préoccupations actuelles et non pas comme un accord applicable sur du long terme…

In fine, la Commission a conclu grâce à sa décision d'adéquation que le régime applicable aux Etats-Unis était essentiellement équivalent à celui en vigueur au sein de l'Union, mais plusieurs caractéristiques du système américain permettent de mettre en doute la décision d'équivalence prise par la Commission et c'est ce que nous allons examiner dans la prochaine section.

3. Les raisons de douter de l'équivalence

Bien que la Commission ait conclu à l'équivalence des deux régimes étudiés dans le cadre de ce travail, certaines caractéristiques essentielles du système américain semblent remettre en cause cette conclusion. Une brève analyse du 1er amendement de la Constitution et du *Cloud Act* nous permettra de mettre en avant des pistes qui nous autorisent à douter que la conclusion à laquelle est arrivée la Commission Européenne soit la plus adéquate…

a. Le 1er amendement de la Constitution américaine

Face au monde numérique dans lequel nous vivons aujourd'hui, la notion de vie privée a été chamboulée car les individus ne cessent de publier des informations privées, qui par la force des choses deviennent connues à la fois par les entreprises et par d'autres personnes[160].
Confrontée à cette situation, l'Union Européenne est intervenue afin de protéger la vie privée des individus, ce qui constitue un droit essentiel garanti par l'article 8 de la CEDH.

Dans une vision quasi opposée, les Etats-Unis défendent la liberté d'expression et de presse notamment par l'intermédiaire du 1er amendement qui stipule que « *le Congrès ne pourra*

---

[158] S. PEYROU, « *Transfert de données à caractère personne UE - Etats Unis: nouvel épisode du feuilleton « Privacy Shield »* », le 1er janvier 2018, disponible sur http://www.gdr-elsj.eu/2018/01/01/informations-generales/transfert-de-donnees-a-caractere-personnel-ue-etats-unis-nouvel-episode-du-feuilleton-privacy-shield-reflexions-a-propos-du-rapport-du-groupe-de-larticle-29-re/

[159] Résolution du Parlement européen du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis, 2018/2645, point 35.

[160] J. GONDOLO, « RGPD: l'Europe et l'Amérique se divisent sur la vie privée », 25 juillet 2018, disponible sur https://www.contrepoints.org/2018/07/25/321084-rgpd-leurope-et-lamerique-se-divisent-sur-la-vie-privee.

faire aucune loi ayant pour objet l'établissement d'une religion ou interdisant son libre exercice, de limiter la liberté de parole ou de presse (...) »[161].

La protection octroyée à la liberté d'expression symbolise le fossé qui existe entre les Etats-Unis et l'Europe car selon Richard Posner, « *la notion de Privacy est nocive pour le marché en ce qu'elle prive d'informations les agents dans leurs prises de décisions* »[162]. En effet, là où l'Europe envisage le droit à la vie privée comme un droit sacré, les Etats-Unis considèrent la liberté d'expression comme le droit le plus fondamental.

Il découle de cette différence philosophique, une différence juridique entre les deux systèmes car là où l'Union a adopté des lois générales et des directives afin de protéger les données à caractère personnel, les Etats-Unis n'ont jamais opté pour une loi générale, globale notamment en raison de leurs idées plus libérales[163].

En outre, à la suite des attentats du 11 septembre 2001, les Etats-Unis ont développé une vision plus sécuritaire, en créant notamment le *Patriot Act* visant à renforcer le pouvoir des services de renseignements tandis que l'Union Européenne renforçait quant à elle les libertés individuelles[164].
Les différences culturelles qui existent depuis de nombreuses années entre ces deux acteurs, renforcées par le contexte terroriste et la manière d'approcher ce danger n'ont fait qu'augmenter le gouffre qui les sépare.

Il est certain qu'en tant qu'Européen, notre approche semble la plus cohérente et la plus structurée mais celle-ci est perçue comme étant trop lourde et contraignante aux Etats-Unis où la vision libérale, exprimée par l'adage « *laissez-faire, laissez passer* » s'impose.

b. Le Cloud Act

Une des menaces les plus importantes de la protection des données personnelles réside dans l'adoption d'un instrument juridique inquiétant: le *Cloud Act.*

A l'heure où le RGPD est entré en vigueur, le *Cloud Act* pourrait entraîner des conséquences néfastes sur la protection des données à caractère personnel développées par le dispositif européen. Cet instrument est entré en vigueur le 23 mars 2018 et oblige les compagnies américaines actives dans le secteur des communications « *à fournir des informations concernant toutes les datas stockées sur leurs serveurs, peu importe si celles-ci se trouvent sur le territoire américain ou à l'étranger* »[165].

---

[161] 1er amendement de la Constitution américaine

[162] J. GONDOLO, « RGPD: l'Europe et l'Amérique se divisent sur la vie privée », 25 juillet 2018, disponible sur https://www.contrepoints.org/2018/07/25/321084-rgpd-leurope-et-lamerique-se-divisent-sur-la-vie-privee.

[163] F. CHARLET, « Pourquoi les USA et l'Europe n'ont pas la même vision de la vie privée? », 25 mars 2014, disponible sur https://francoischarlet.ch/2014/pourquoi-les-usa-et-leurope-nont-pas-la-meme-vision-de-la-vie-privee/.

[164] F. CHARLET, « Pourquoi les USA et l'Europe n'ont pas la même vision de la vie privée? », 25 mars 2014, disponible sur https://francoischarlet.ch/2014/pourquoi-les-usa-et-leurope-nont-pas-la-meme-vision-de-la-vie-privee/.

[165] L. FOUCHER, « Le Cloud Act: une atteinte à la protection des données dans l'Union Européenne? », disponible sur https://ictrecht.be/fr/featured-2/le-cloud-act-une-atteinte-a-la-protection-des-donnees-dans-lunion-europeenne/.

Cette loi, très peu médiatisée, facilite donc l'accès aux données détenues par les entreprises et ce même en dehors du territoire américain, pour les autorités américaines, ce qui est aux antipodes des objectifs contenus dans le RGPD. Et même s'il existe des garde-fous, il est naturel de s'inquiéter sur l'avenir d'un tel dispositif à l'heure où l'Union Européenne souhaite nous offrir une protection renforcée.

La décision d'adéquation du *Privacy Shield* avait été influencée positivement par les engagements pris par les autorités américaines de limiter leur ingérence dans les données à caractère personnel. Or, cette loi renforce une fois de plus les pouvoirs des agences de surveillance américaine, ce qui suscite de vives inquiétudes dans le camp européen[166].

De plus, la diversité des instruments juridiques ne fait que de créer une bulle d'insécurité juridique, qui à notre sens ne peut que profiter aux grandes entreprises et non pas aux petits particuliers, perdus face à tous ces dispositifs juridiques.

Dès lors, il est certain que le *Cloud Act* ne peut s'avérer compatible avec les objectifs poursuivis par le RGPD et qu'il peut également entraîner des conséquences négatives sur le *Privacy Shield*, remettant en cause les garanties apportées par les Etats-Unis afin d'assurer une équivalence de la protection des données personnelles. Il semble donc que cet instrument constitue une brèche dans l'affirmation de la Commission selon laquelle les Etats-Unis offrent une protection essentiellement équivalente à celle de l'Union Européenne…

[166] J-H, GAVETTI, « Le Cloud Act, une nouvelle loi qui renforce l'ingérence des autorités américaines sur les opérateurs de Cloud des US », le 6 avril 2018, disponible sur https://www.lesechos.fr/idees-debats/cercle/le-cloud-act-une-nouvelle-loi-qui-renforce-lingerence-des-autorites-americaines-sur-les-operateurs-de-cloud-des-us-131174.

SECTION 5: CONCLUSION

Conclure aujourd'hui une telle thématique n'est pas chose aisée, c'est pour cette raison que nous tacherons d'établir une conclusion à deux vitesses quant à la réponse à apporter à la question suivante: « *existe-t-il une équivalence de protection des données personnelles en Union Européenne et aux Etats-Unis?* »

Si la Commission Européenne a adopté une décision d'adéquation du *Privacy Shield* le 12 juillet 2016, c'est notamment en raison des différentes garanties offertes par les Etats-Unis afin d'établir une protection adéquate et essentiellement équivalente à celle de l'Union Européenne. Il était urgent et nécessaire d'établir un accord entre l'Union et les Etats-Unis afin d'éviter des conséquences désastreuses d'un point de vue économique sur le flux des données transfrontalier. Cette nécessité et cette urgence, n'ont-elles pas entrainé dans le chef de la Commission, une volonté d'établir un instrument coûte que coûte, malgré certaines faiblesses, aujourd'hui établies?

Au vu des critiques émergentes à propos de cet accord, il est donc permis de douter de la réelle équivalence des régimes américain et européen et que celle-ci soit réellement rencontrée dans la pratique. La décision d'adéquation ne constitue-t-elle pas une sorte de coquille vide en vue de permettre un transfert de données, et une collaboration essentielle entre ces deux entités?

En outre, si la Commission a conclu à une équivalence, c'est peut-être également parce que les risques exposés par *Snowden*, *Cambridge Analytica* et *Schrems* n'ont pas été établis à leur juste valeur.

Dès lors, il semble que le *Privacy Shield* et cette décision d'adéquation qui en découle ne constituent en réalité qu'un outil de transition, avant d'établir un instrument qui permette une équivalence effective entre ces deux entités. Il semble, à l'heure d'aujourd'hui, que les différences culturelles et juridiques entre l'Union Européenne et les Etats-Unis ne permettent pas d'établir, contrairement à ce qui a été conclu par la Commission Européenne, une réelle équivalence entre ces deux systèmes.

Cependant, depuis l'entrée en vigueur en 2018 du RGPD, il est permis à nouveau d'imaginer la possibilité de voir émerger une réelle équivalence entre ces deux systèmes, à l'avenir car malgré des divergences manifestes, le RGPD signe peut-être le début d'une future convergence entre les deux systèmes.

SECTION 6: BIBLIOGRAPHIE

✦ OUVRAGES

CARNEROLI, S., « Le droit à l'oubli. Du devoir de mémoire au droit à l'oubli. », Larcier, 2016.

CASTETS-RENARD, C., « Quelle protection des données personnelles en Europe? » Larcier, 2015, pp 10 à 158.

CHERUY, L., « Protection des données personnelles : se mettre en conformité d'ici le 25 mai 2018 », Montrouge, Editions Législatives, 2017, p.23.

DE TERWAGNE, C., « Droit à l'oubli numérique élément du droit à l'autodétermination informationnelle ?», in Le droit à l'oubli numérique : données nominatives – approche comparative (sous la dir. de D. DECHENAUD), Larcier, 2015.

DOCQUIR, B., « Vers un droit européen de la protection des données? », Larcier, 2017, Bruxelles, pp. 71 à 73.

EPINEY, A., SANGSUE, D., « L'ère numérique et la protection de la sphère privée », Schulthess, 2018, pp. 29 à 82.

GROSJEAN, A., « Enjeux Européens et mondiaux de la protection des données personnelles », Larcier, 2015, pp. 15 à 125.

MARTIAL-BRAZ, N., « La proposition de règlement européen relatif aux données à caractère personnel: transposition du réseau trans Euro experts », Trans Europe Experts, 2014, Vol. 9, p.179.

PAILLER, L. « Les réseaux sociaux sur internet et le droit au respect de la vie privée », Larcier, 2012, p.112.

PUBLICATION OFFICE OF THE EUROPEAN UNION, « Handbook on European data protection », 2018, Luxembourg, pp. 29 à 257.

SHERMER, B., CUSTERS, B., VAN DER HOF, S., « The crisis of consent : how stronger legal protection may lead to weaker consent in data protection », Ethics and Information Technology, vol.16, 2014, p. 177.

✦ARTICLES

BRAS, B., « Le privacy paradox et comment le dépasser », disponible sur https://www.cairn.info/revue-francaise-de-gestion-2012-5-page-87.htm

CHARLET, F., « Pourquoi les USA et l'Europe n'ont pas la même vision de la vie privée? », 25 mars 2014, disponible sur https://francoischarlet.ch/2014/pourquoi-les-usa-et-leurope-nont-pas-la-meme-vision-de-la-vie-privee/.

FOUCHER, L. « Le Cloud Act: une atteinte à la protection des données dans l'Union Européenne? », disponible sur https://ictrecht.be/fr/featured-2/le-cloud-act-une-atteinte-a-la-protection-des-donnees-dans-lunion-europeenne/.

GALICHET, C., « Données personnelles: aonymisation, pseudonymisation », 2017, disponible sur https://www.village-justice.com/articles/donnees-personnelles-anonymisation-pseudonymisation,26194.html

GASSEND, J., « *RGPD, GDPR…votre entreprise est-elle prête*? », 2017, disponible sur https://www.digitalwallonia.be/fr/publications/gdpr

GAVETTI, J-H.,« Le Cloud Act, une nouvelle loi qui renforce l'ingérence des autorités américaines sur les opérateurs de Cloud des US », le 6 avril 2018, disponible sur https://www.lesechos.fr/idees-debats/cercle/le-cloud-act-une-nouvelle-loi-qui-renforce-lingerence-des-autorites-americaines-sur-les-operateurs-de-cloud-des-us-131174.

GEELKENS, M., « Données volées, données protégées… L'année du scandale Cambridge Analytica », 2019, disponible sur https://www.levif.be/actualite/international/donnees-volees-donnees-protegees-l-annee-du-scandale-cambridge-analytica/article-normal-1069869.html

J. GONDOLO, « RGPD: l'Europe et l'Amérique se divisent sur la vie privée », 25 juillet 2018, disponible sur https://www.contrepoints.org/2018/07/25/321084-rgpd-leurope-et-lamerique-se-divisent-sur-la-vie-privee.

GUIMOLLES, A., « L'Europe va mieux protéger la vie privée », 2018, disponible sur https://www.la-croix.com/Economie/Monde/LEurope-mieux-proteger-vie-privee-2018-05-24-1200941278

ITEANU, O., « Safe Harbour et Privacy Shield pour les nuls », disponible sur https://www.eurocloud.fr/safe-harbour-privacy-shield-nuls/

KUCHLER, H., « Max Schrems, l'homme qui est parti en guerre contre Facebook et l'a gagnée », 2018, disponible sur. https://www.lenouveleconomiste.fr/financial-times/max-schrems-lhomme-qui-est-parti-en-guerre-contre-facebook-et-la-gagnee-63115/

LAUSSON, J. « RGPD: 15 questions pour comprendre le règlement sur la protection des données personnelles », 2019, disponible sur https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-internaute.html

LE CALME, S., « Le CNNum estime que le Pricacy Shiel, l'accord entre l'UE et les USA sur les transferts de données doit être renégocié », 21 septembre 2017, disponible sur https://www.developpez.com/actu/161504/Le-CNNum-estime-que-le-Privacy-Shield-l-accord-entre-l-UE-et-les-USA-sur-les-transferts-de-donnees-doit-etre-renegocie/

MANOKHA, I., « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » disponible sur https://www.cairn.info/revue-cultures-et-conflits-2018-1-page-39.htm

PEYROU, S., « *Transfert de données à caractère personne UE - Etats Unis: nouvel épisode du feuilleton « Privacy Shield »* », le 1er janvier 2018, disponible sur http://www.gdr-elsj.eu/2018/01/01/informations-generales/transfert-de-donnees-a-caractere-personnel-ue-etats-unis-nouvel-episode-du-feuilleton-privacy-shield-reflexions-a-propos-du-rapport-du-groupe-de-larticle-29-re/

POLIDORI, M., « L'arrêt Google Spain de la CJUE du 13 mai 2014 et le droit à l'oubli », disponible sur https://www.cairn.info/revue-civitas-europa-2015-1-page-243.htm

TUAL, M., « Trois ans après les révélations Snowden, la surveillance de masse se porte bien », 2016, disponible sur https://www.lemonde.fr/pixels/article/2016/11/24/trois-ans-apres-les-revelations-snowden-la-surveillance-de-masse-se-porte-bien_5037022_4408996.html

UNTERSINGER, M., « Surveillance: quel bilan tirer, cinq ans après le début des révélations d'Edward Snowden », 2018, disponible sur https://www.lemonde.fr/pixels/article/2018/06/05/surveillance-quel-bilan-tirer-cinq-ans-apres-le-debut-des-revelations-d-edward-snowden_5310017_4408996.html

WESSBECHER, L., « Netflix et les données personnelles: doit-on craindre pour la protection de notre vie privée? », 2018, disponible sur https://www.france24.com/fr/20180428-netflix-donnees-personnelles-doit-on-craindre-protection-notre-vie-privee

« Adoption de la décision d'adéquation du Privacy Shield par la Commission Européenne », 2016, disponible sur https://www.cnil.fr/fr/adoption-de-la-decision-dadequation-du-privacy-shield-par-la-commission-europeenne

« Dans quelle partie du monde le RGPD va s'appliquer? », disponible sur https://www.autoriteprotectiondonnees.be/champ-dapplication-territorial

« L'essentiel à connaitre sur le GDPR/RGPD: définition, périmètre, principes et mesures », 2017, disponible sur https://www.custup.com/introduction-gdpr-rgdp/

« Portabilité des données : le nouveau droit consacré par le RGPD ! », disponible sur https://lexing.be/portabilite-des-donnees-le-nouveau-droit-consacre-par-le-rgpd/

« Safe Harbor », disponible sur https://www.cnil.fr/sites/default/files/typo/document/CNIL-transferts-SAFE_HARBOR.pdf

« Selon le RGPD: qu'est-ce-que le droit d'accès? », disponible sur https://www.fairandsmart.com/droit-dacces-donnees-personnelles-rgpd/

« Surveillance: ce que contient la nouvelle loi sur le renseignement britannique », 2016, disponible sur https://www.lemonde.fr/pixels/article/2016/11/21/surveillance-ce-que-contient-la-nouvelle-loi-sur-le-renseignement-britannique_5035373_4408996.html

« Why the Cambridge Analytica scandal matters », disponible sur https://thespinoff.co.nz/politics/21-03-2018/why-the-cambridge-analytica-scandal-matters/

✦ AUTRES

Communication de la Commission au Parlement européen et au Conseil, « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 ».

Communication de la Commission au Parlement Européen et au Conseil, « Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides », 29 février 2016.

Communication from the Commission "Building a European data economy", COM(2017) 9 final, January 2017, disponible sur https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-9-F1-EN-MAIN-PART-1.PDF

Communiqué de presse de la Cour de justice de l'Union européenne n° 140/17, Luxembourg, le 20 décembre 2017, disponible sur https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-12/cp170140fr.pdf

Communiqué de presse de la Commission Européenne, « 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» », Strasbourg, le 2 février 2016.

Communiqué de presse de V. JOUROVA, Commission européenne, « La Commission européenne lance le bouclier de protection des données UE-États-Unis: une protection renforcée pour les flux de données transatlantiques », Bruxelles, le 12 juillet 2016.

Conclusions de l'Avocat général, M. SZPUNAR présentées le 21 mars 2019 (1) dans l'Affaire C−673/17 Planet49 GmbH contre Bundesverband der Verbraucherzentralen und Verbraucherverbände Verbraucherzentrale Bundesverband e.V, disponible sur http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=6538073

Contrôleur européen de la protection des données personnelles, « Résumé de l'avis du Contrôleur européen de la protection des données concernant le «Bouclier vie privée UE - États-Unis» (Privacy Shield) — Projet de décision d'adéquation »

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-Etats-Unis, *J.O.U.E.*, L 207 du 1er août 2016

FAQ sur l'arrêt Big Brother Watch et autres c. Royaume-Uni, disponible sur https://www.echr.coe.int/Documents/Press_Q_A_Brother_Watch_FRA.pdf

Fiche d'information de la commission européenne, « *Le bouclier de protection des données UE-États-Unis: Foire aux questions* », Bruxelles, le 12 juillet 2016.

Groupe de travail « ARTICLE 29 », « Document de travail 01/2016 sur la justification des ingérences dans les droits fondamentaux à la vie privée et à la protection des données découlant de mesures de surveillance lors du transfert de données à caractère personnel (garanties essentielles européennes) », 13 avril 2016.

Groupe de travail « ARTICLE 29 », « Déclaration du G29 relative à la décision de la Commission européenne concernant le Privacy Shield (bouclier de protection des données UE-États-Unis) », 29 juillet 2016.

« Guide to self-certification » US and UE, safe harbor framework » p.10, disponible sur https://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

« Guide du bouclier de protection des données personnelles UE- Etats-Unis », pp. 5 à 10.

« Le RGPD, nouvelles opportunités, nouvelles obligations », Commission Européenne, p.2, disponible sur https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_fr.pdf

Lignes directrices du 13 décembre 2016 relatives au droit à la portabilité des données (WP 242), p.14, disponible sur https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

Résolution du Parlement européen du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis, 2018/2645, point 35.

✦ LEGISLATIONS

Convention européenne des Droits de l'Homme.

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

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 fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

Investigatory Powers Act 2016, disponible sur http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

Règlement (UE) n°2016/679 du Parlement et du Conseil du 27 avril 2016.

✦JURISPRUDENCE

C.E.D.H., 13 septembre 2018, *Big Brother Watch et autres c. Royaume-Uni*, 58170/13.

C.J.U.E (gde Ch.), 7 décembre 2010, *Pammer et Hôtel Alpenhof*, aff. C-585/08 et C-144/09

C.J.U.E. (gde Ch.), 8 avril 2014, *Digital Rights Ireland Ltd*, aff. C-293/12, (ECLI:EU:C:2014:238)

C.J.U.E. (gde Ch.), 13 mai 2014, *Google Spain*, aff. C-131/12,

C.J.U.E. (gde Ch.), 6 octobre 2015, *Schrems*, aff. C-362/14

C.J.U.E. (2ème Ch.), 19 octobre 2016, *Breyer*, aff. C-582/14, §43. C.J.U.E. (2ème Ch.)

C.J.U.E., 9 mars 2017, *Manni*, C-398/15.

C.J.U.E. (2ème Ch.), 20 décembre 2017*, Nowak c.Data Protection Commissione*r, aff. C-434/16