UCLouvain
SAINT-LOUIS BRUXELLES

iee
Institut d'études européennes
Institute for European Studies

TRAVAIL DE FIN D'ÉTUDES
en vue de l'obtention du Master de spécialisation interdisciplinaire en Études européennes

---

La portée extraterritoriale du RGPD et les transferts de données entre l'UE et les États-Unis

Enjeux de souveraineté numérique, intérêts économiques et perspectives des relations transatlantiques

Camille Brasseur

Sous la direction d'Antoine Bailleux

Année académique 2024-2025

TABLE DES MATIÈRES

Liste des sigles et acronymes *2*

Introduction *4*

I. Première Partie : l'applicabilité du RGPD aux États-Unis – Chronologie et analyse juridique *5*

1. L'évolution des cadres juridiques transatlantiques **5**

a) Du premier cadre juridique transatlantique Safe Harbor à Schrems I 6

b) Un second cadre juridique transatlantique : du Privacy Shield à Schrems II 8

2. Portée extraterritoriale du RGPD et impact sur les entreprises américaines **10**

a) Application pratique du RGPD aux entreprises américaines : obligations et sanctions 10

b) Limites et difficultés d'application extraterritoriale : coopération et conflits de lois 12

II. Deuxième Partie : Réflexions critiques et prospectives *13*

1. Souveraineté numérique et capacité normative de l'UE **13**

a) L'UE comme puissance normative : le *Brussels Effect* 14

b) Les défis de la souveraineté numérique européenne face à la dépendance technologique 15

2. Perspectives d'avenir et nouveaux cadres juridiques transatlantiques **17**

a) Le Data Privacy Framework (DPF) : le nouveau cadre juridique 17

b) Des garanties encore insuffisantes : le DPF face aux doutes européens 17

c) Tensions et ambitions pour la gouvernance des transferts de données 19

Conclusion *21*

Bibliographie *24*

LISTE DES SIGLES ET ACRONYMES

APD	Autorité de protection des données
BCR	Règles d'Entreprise Contraignantes
CAA	Accord bilatéral CLOUD Act
CCPA	California Consumer Privacy Act
CCT	Clauses Contractuelles Types
CEDH	Cour européenne des droits de l'Homme
CJUE	Cour de justice de l'Union européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
DFFT	Data Free Flow with Trust
DPF	Data Privacy Framework
DPRC	Data Protection Review Court
EDPB (CEPD)	Comité européen de la protection des données
EDRi	European Digital Rights
EDPS	Contrôleur européen de la protection des données
NSA	National Security Agency
OCDE	Organisation de coopération et de développement économiques

PETs	Privacy-Enhancing Technologies
RGPD	Règlement général sur la protection des données

INTRODUCTION

Dans un monde où la technologie numérique occupe une place toujours plus centrale, la protection des données, qui lui est indissociable, constitue un défi crucial, non seulement pour les entreprises, mais également pour les individus. La circulation, le traitement et la protection des données personnelles soulèvent des enjeux majeurs de souveraineté, de droits fondamentaux et de compétitivité économique. Dans ce contexte, l'Union européenne (UE) a adopté le 27 avril 2016 le Règlement général sur la protection des données (RGPD)[1] (Parlement européen et Conseil de l'Union européenne, 2016). Ce Règlement, entré en application le 25 mai 2018, remplace la directive européenne sur la protection des données (DPD) 95/46/CE[2] (Thelisson, 2020). Selon son art. 1, il poursuit trois objectifs clés : assurer la protection des individus au sein de l'Union européenne, garantir leurs droits fondamentaux et permettre la libre circulation des données au sein de l'Union (CNIL, 2016, art. 1). Il 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 » (CNIL, 2016, art. 2). Il impose également des règles aux entreprises qui traitent les données personnelles des citoyens européens (Wolford, 2023).

Au-delà des frontières de l'UE, le RGPD étend son champ d'application aux entreprises étrangères traitant des données personnelles de résidents européens, en vertu de sa portée extraterritoriale définie à l'art. 3, al. 2 du Règlement (Gstrein et Zwitter, 2021). Ce principe d'extraterritorialité soulève des enjeux considérables de souveraineté numérique pour l'Union européenne, notamment concernant les transferts de données avec les États-Unis.

Les États-Unis représentent, en effet, le principal partenaire de l'Union en matière de services numériques. Selon American Chamber to the European Union (AmCham EU) (2023), 90 % des entreprises européennes dépendent des flux de données transatlantiques pour leurs activités. Toutefois, les modèles européens et américains sont profondément différents en termes de protection des données. D'un côté, l'UE cherche à tout prix à protéger les droits

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

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

fondamentaux des citoyens européens ; de l'autre, les États-Unis sont davantage axés sur la compétitivité, les intérêts économiques et la sécurité nationale. Ainsi, depuis près de deux décennies, la coopération transatlantique est marquée par des tensions récurrentes, notamment autour des cadres juridiques encadrant les transferts de données vers les États-Unis – Safe Harbor[3] et Privacy Shield[4] – invalidés successivement par la Cour de justice de l'Union européenne (CJUE) respectivement en 2015 et 2020 (Sigrist, 2025). Dans ce contexte, des figures emblématiques des géants du numérique comme Tim Cook, PDG d'Apple, sont favorables à l'instauration d'un règlement américain sur la protection des données similaire au RGPD. Selon *Le Monde* (2018), il a ainsi déclaré : **«** nos propres informations, de celles de tous les jours à la plus intime, sont utilisées comme une arme contre nous avec une efficacité militaire. Ces bouts de données, qui sont inoffensifs individuellement, sont assemblés avec soin, synthétisés, négociés et vendus. » (para. 6). (« Le patron d'Apple », 2018).

Dans le cadre de ce travail de fin d'études, il conviendra dans un premier temps de retracer la chronologie des cadres juridiques relatifs au RGPD, en analysant leurs conséquences. Cette étape comprendra également l'étude de la portée extraterritoriale du RGPD et de son application pratique aux entreprises américaines soumises au Règlement. Dans un deuxième temps, il s'agira d'apporter une réflexion critique sur les transferts des données entre l'Union européenne et les États-Unis, les enjeux liés à la souveraineté numérique et technologique, ainsi que les perspectives d'avenir au regard du nouveau cadre juridique adopté récemment.

I. PREMIÈRE PARTIE : L'APPLICABILITÉ DU RGPD AUX ÉTATS-UNIS – CHRONOLOGIE ET ANALYSE JURIDIQUE

1. L'évolution des cadres juridiques transatlantiques

Afin de bien saisir les mécanismes d'applicabilité du RGPD aux États-Unis, il convient tout d'abord de retracer le cadre réglementaire européen en matière de transferts de données à caractère personnel envers les pays tiers ainsi que les décisions jurisprudentielles majeures qui ont façonné la politique transatlantique.

[3] CJUE, arrêt Schrems I, 6 octobre 2015, C-362/14.
[4] CJUE, arrêt Schrems II, 16 juillet 2020, C-311/18.

Les transferts de données vers des pays tiers sont encadrés par les art. 44 à 50 du RGPD. Parmi les mécanismes prévus, l'art. 45 autorise la Commission européenne à adopter une décision d'adéquation, c'est-à-dire à approuver les transferts de données à caractère personnel vers un pays tiers. Cela signifie qu'un pays tiers, par exemple les États-Unis, offre un niveau de protection adéquat et équivalent au RGPD. Pour ce faire, la Commission européenne s'appuie sur plusieurs facteurs : l'État de droit, les libertés fondamentales, l'accès des autorités aux données personnelles, la présence d'autorité de contrôle indépendante et « les engagements internationaux pris par le pays tiers ou l'organisation internationale en question […] » Par ailleurs, une réévaluation doit avoir lieu au moins tous les quatre ans, et la Commission européenne peut révoquer sa décision si le niveau n'est plus jugé équivalent (CNIL, s.d.-e, art. 45). Néanmoins, dans la mesure où aucun niveau d'adéquation n'a été établi, d'autres mécanismes d'autorisation sont possibles, comme les transferts avec garanties appropriées au titre de l'art. 46 du RGPD. Celles-ci peuvent être des Clauses Contractuelles Types (CCT) ou des Règles d'Entreprise Contraignantes (BCR) (CNIL, s.d., art. 46 et 47).

a) Du premier cadre juridique transatlantique Safe Harbor à Schrems I

Dès l'année 2000, la Commission européenne a adopté la décision d'adéquation 2000/520/CE, reconnaissant que le cadre de protection des données des États-Unis, connu sous le nom de Safe Harbor, établi par le ministère américain du commerce (DoC), assurait un niveau de protection équivalent à la directive européenne 95/46/CE. Ce mécanisme permettait donc aux entreprises américaines de s'autocertifier annuellement afin d'adhérer aux principes définis par ce cadre juridique et de bénéficier des données personnelles venant de l'Union européenne (Service de recherche du Parlement européen, 2017). Néanmoins, en 2013, des failles ont été relevées, notamment suite aux révélations d'Edward Snowden[5] concernant les programmes de surveillance menés par le gouvernement américain dans le but, selon les autorités, de lutter contre le terrorisme suite aux attentats du 11 septembre 2001. Ces révélations ont mis en lumière l'existence de dérogations légales extensives aux États-Unis, permettant aux agences de renseignement, notamment la National Security Agency (NSA), d'effectuer une surveillance massive en collectant des données personnelles hébergées par des entreprises américaines telles que Microsoft, Google, YouTube, et Verizon. En outre, des opérations

[5] Edward Snowden est un informaticien qui a travaillé pour la National Security Agency (NSA) et la Central Intelligence Agency (CIA) (Institut de Recherche Stratégique de l'École Militaire, 2013).

d'espionnage visant les institutions européennes avaient également été mises en lumière (Institut de Recherche Stratégique de l'École Militaire, 2013).

Suite à ce scandale, Viviane Reding, alors vice-présidente de la Commission, avait déclaré en 2013 que les standards de protection des données des États-Unis n'étaient potentiellement pas équivalents à ceux de l'UE. Elle a également qualifié la décision d'adéquation Safe Harbor de faille juridique (McBride, Sotto, & Treacy, 2013). Par ailleurs, la même année, Max Schrems[6], avait déposé une plainte contre Facebook Ireland Ltd – plateforme qui transfère les données à caractère personnel de ses utilisateurs aux États-Unis – auprès de l'autorité irlandaise de protection des données car Facebook Ireland Ltd transférait massivement les données européennes vers les États-Unis, où elles pouvaient être utilisées par la NSA, violant ainsi le cadre juridique Safe Harbor et les droits fondamentaux européens (Schrems, 2013). Toutefois, suite au non-aboutissement de sa plainte par l'autorité irlandaise, au motif qu'il existait une décision d'adéquation validée par la Commission européenne, la Haute Cour irlandaise a établi un renvoi préjudiciel auprès de la Cour de justice de l'Union. La question était de savoir si une décision d'adéquation en vigueur pouvait empêcher une autorité nationale de protection de données (APD) d'examiner une plainte en toute indépendance. La seconde question était de préciser si la décision d'adéquation (ci-après Safe Harbor) respectait bien les droits fondamentaux, garantis par la Charte des droits fondamentaux de l'UE, notamment ses art. 7, 8 et 47. Dans l'arrêt Schrems I, la Cour de justice de l'Union a déclaré qu'une APD avait le droit d'examiner une plainte au regard des facteurs cités précédemment. Ainsi, sachant que la directive européenne 95/46/CE – remplacée depuis par le RGPD – interdisait tout transfert de données vers un pays tiers ne garantissant pas un niveau de protection substantiellement équivalent à celui de l'Union européenne et que la décision Safe Harbor reposait sur l'autocertification des entreprises, qui ne prévoit pas l'implication des autorités publiques américaines, la décision d'adéquation a été invalidée par la CJUE le 6 octobre 2015 (Cour de justice de l'Union européenne [CJUE], 2015). En outre, les art. 7 (droit à la vie privée), 8 (droit à la protection des données) et 47 (droit aux recours) de la Charte des droits fondamentaux de l'UE imposent que la protection des données soit substantielle et continue, ce que ne respectaient pas les États-Unis ici (Service de recherche du Parlement européen, 2017).

[6] Max Schrems est avocat autrichien et défenseur de la protection des données personnelles et connu pour avoir fait invalider les cadres juridiques Safe Harbor et Privacy Shield sous les noms respectifs de Schrems I et Schrems II. (Marcos, 2024).

À la suite de cette invalidation, bien que les transferts vers les États-Unis étaient devenus interdits, le Groupe de travail « art. 29 », aujourd'hui appelé Comité européen de la protection des données (EDPB ou CEPD)[7], avait confirmé que d'autres outils juridiques, tels que les CCT et les BCR restaient toujours valables, mais que les APD gardaient la main mise sur l'examen de ces clauses types et si nécessaire, pouvaient saisir les tribunaux (Comité européen de la protection des données, s.d. ; Commission européenne, s.d. ; Service de Recherche du Parlement européen, 2017).

b) Un second cadre juridique transatlantique : du Privacy Shield à Schrems II

Les APD ont rapidement demandé qu'un nouvel accord soit trouvé pour poursuivre les transferts de données personnelles entre l'Union européenne et les États-Unis, tout en garantissant une protection adéquate des citoyens européens et des entreprises européennes. Au début de l'année 2016, un accord parvient à être conclu, donnant naissance au cadre juridique EU-US Privacy Shield, qui succède ainsi à la décision Safe Harbor. Cette nouvelle décision d'adéquation imposait aux entreprises américaines une plus grande transparence sur le traitement des données, une coopération renforcée avec les APD, l'interdiction pour les États-Unis de recourir à une surveillance de masse indiscriminée, la désignation d'un médiateur (ombudsman) permettant aux citoyens européens de faire valoir leurs droits, ainsi que l'instauration d'une révision annuelle de l'accord. Néanmoins, malgré ce nouveau compromis, de nombreuses voix s'étaient élevées, dont celle de l'ancienne vice-présidente de la Commission européenne Viviane Reding qui mettait en doute la réelle avancée de ce nouveau cadre, dénonçant le manque d'obligations juridiquement contraignantes (« Le Privacy Shield », 2016). En outre, le GT art. 29 avait pointé du doigt, malgré ses recommandations *ad hoc* soumises à la Commission, l'ambiguïté du nouveau texte, l'indépendance discutable du médiateur américain, l'opacité des systèmes de recours, ainsi que le maintien d'une surveillance généralisée. Par ailleurs, le Contrôleur européen de la protection des données (CEPD) avait salué les progrès réalisés par rapport au Safe Harbor, mais avait malgré tout été critique en appelant à être cohérent avec le RGPD. (Service de Recherche du Parlement européen, 2017).

[7] Le Comité européen est composé des autorités nationales de protection des données de chaque État membre. (Union européenne, 2025).

Finalement, bien qu'il ait fait l'objet d'un certain scepticisme, le Privacy Shield a été approuvé le 8 juillet 2016 par la quasi-totalité des États membres de l'Union européenne. Ainsi, plusieurs principes fondamentaux ont été renforcés, tels que la transparence, la nomination d'une instance autonome pour le traitement des recours, le droit d'opposition, les obligations de transferts à des tiers, le droit d'accès, la sécurité, ainsi que la limitation de conservation (Service de Recherche du Parlement européen, 2017).

Malgré les quelques améliorations par rapport à son prédécesseur, le cadre juridique Privacy Shield a finalement été invalidé par la Cour de justice de l'Union le 16 juillet 2020 suite à l'arrêt Schrems II. Ce dernier oppose à nouveau Maximillian (Max) Schrems, Facebook Ireland Ltd et la Data Protection Commissioner. L'avocat accuse une fois de plus les États-Unis de ne pas garantir un niveau de protection adéquat des données des citoyens européens, en violation du RGPD et de la Charte des droits fondamentaux de l'UE. Si les CCT restent valides, la décision d'adéquation, en revanche, a été invalidée. Les principales raisons étaient liées au non-respect des mécanismes de surveillance restreints au minimum requis et l'insuffisance des dispositifs de recours pour les citoyens européens (Cour de justice de l'Union européenne, 2020).

Dès l'invalidation du Safe Harbor par la CJUE en 2015, de nombreux experts s'étaient indignés afin d'alerter sur l'urgence d'une réponse coordonnée et conforme au droit européen de la protection des données. De nombreuses organisations comme EPiC[8] et Privacy International[9] estimaient qu'un nouveau cadre similaire à celui de Safe Harbor serait voué à l'échec (Service de Recherche du Parlement européen, 2017). Ces critiques reflétaient déjà une incohérence croissante entre les principes européens et les pratiques américaines, et se sont d'ailleurs avérées fondées, comme en témoigne cette seconde invalidation, en 2020, de la décision d'adéquation Privacy Shield. La succession de ces deux annulations de cadres juridiques révèle une évolution constante des exigences du droit européen en matière de protection des données personnelles. Ainsi, au-delà des critères formels, notamment définis à l'art. 45 du RGPD, la jurisprudence de la CJUE a renforcé la protection des droits fondamentaux des citoyens de l'Union européenne en exigeant des pays tiers le respect et l'effectivité des

[8] EPiC (Electronic Privacy Information Center) est une organisation non gouvernementale (ONG) américaine qui agit pour la protection de la vie privée, la liberté d'expression et les valeurs démocratiques à l'ère numérique. (EPiC, s.d.).
[9] Privacy International est une organisation non gouvernementale (ONG) basée à Londres qui milite pour la défense des droits de l'homme, en particulier le droit à la vie privée. (Privacy International, s.d.).

normes en matière de protection des données. Cela impliquait notamment la possibilité de recours effective et la limitation stricte des ingérences étatiques, en particulier dans le cadre des programmes de surveillance.

2. Portée extraterritoriale du RGPD et impact sur les entreprises américaines

a) Application pratique du RGPD aux entreprises américaines : obligations et sanctions

L'une des innovations majeures du RGPD réside dans sa portée extraterritoriale, qui s'applique à toute entreprise située en dehors de l'Union européenne (« Tout savoir », 2025). Ainsi, au-delà d'une décision d'adéquation, les entreprises basées aux États-Unis traitant des données personnelles des citoyens européens peuvent être directement soumises aux obligations du RGPD. D'une part, selon l'art. 3, al. 2 du RGPD, le Règlement s'applique en dehors de l'Union européenne si le responsable du traitement[10] ou le sous-traitant[11] est établi dans l'Union européenne, peu importe où les données sont traitées. En d'autres termes, si une entreprise basée aux États-Unis décide d'implanter une filiale, une succursale ou tout autre établissement dans un État membre de l'UE, celle-ci doit obligatoirement se conformer aux principes du RGPD. D'autre part, l'art. 3, al. 2 du RGPD vise les entreprises non européennes qui i) offrent des biens et services à des personnes situées dans l'Union européenne ou ii) surveillent le comportement de ces personnes au sein de l'Union (CNIL, 2016, art. 3). Le suivi des comportements est souvent utilisé pour la publicité ciblée, notamment via une activité sur Internet. Dès lors, le responsable du traitement ou le sous-traitant ne doit pas forcément cibler la personne pour être soumis aux obligations du Règlement, mais peut simplement suivre le comportement d'un citoyen établi au sein de l'Union dans le but d'exploiter ses données *a posteriori*. Au-delà de la publicité ciblée, le suivi peut inclure la géolocalisation, le suivi en ligne via les cookies, ou encore la surveillance par vidéo (Rapin, Berti, & Rodieux, 2021). En outre, le RGPD peut s'appliquer à certains établissements situés en dehors de l'UE, où le droit national d'un État membre s'applique en vertu du droit international public. Les exemples les plus courants sont les ambassades ou les consulats d'un État membre implantés en dehors de ses frontières (Deshoulières Avocats, 2025). L'élargissement du champ d'application du RGPD

[10] « Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. »(CNIL, s.d.-b).
[11] « Le sous-traitant est la personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation. » (CNIL, s.d.-c).

fait suite à la décision de la Cour de justice de l'Union dans l'affaire *Google Spain*, dans laquelle la Directive 95/46/CE – remplacée par le RGPD – a été interprétée de manière extensive. En l'espèce, puisque les données concernaient un ressortissant européen et que Google Spain était établi dans l'Union, Google avait l'obligation de respecter les exigences de la Directive. Cette décision a ainsi posé des bases majeures pour la portée extraterritoriale (Rapin et al., 2021).

Afin d'assurer l'effectivité de cette applicabilité extraterritoriale, le Règlement prévoit, à l'art. 27, al.1, l'obligation pour les responsables de traitement ou sous-traitants non établis dans l'Union qui traitent des données de citoyens européens, de désigner un représentant au sein de l'UE. Celui-ci agit comme intermédiaire entre l'entreprise non établie dans l'Union et les autorités nationales de contrôle de protection des données européennes et doit être basé dans l'un des États membres des personnes concernées par le traitement des données (« Nommer un représentant », 2023). Par exemple, une entreprise basée aux États-Unis qui proposent des biens ou des services à des personnes résidant au sein de l'UE est tenue de nommer un représentant. Chaque État membre bénéficie de sa propre autorité de contrôle : l'Autorité de la protection des données en Belgique**,** la Commission nationale de l'informatique et des libertés (CNIL) en France ou encore l'Office of the Data Protection Ombudsman en Finlande (European Data Protection Board, s.d). Toutefois, l'art. 27 ne s'applique pas en cas de traitements sporadiques de données peu sensibles ou si ceux-ci sont effectués par une entité publique (« Nommer un représentant », 2023). Si une entreprise ne respecte pas cette obligation, elle risque des sanctions importantes, notamment des amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (Rapin et al., 2021).

Cette application extraterritoriale ne se limite pas à un principe théorique puisque plusieurs décisions concrètes ont été prononcées pour non-respect des obligations prévues par le Règlement. À titre d'exemple, l'entreprise américaine Clearview AI, spécialisée dans la commercialisation de logiciels de reconnaissance faciale, a, en 2022, écopé d'une amende de 20 millions d'euros de la part de l'Autorité italienne de protection des données pour violation du RGPD. Elle avait traité, sans aucun droit, des données biométriques[12] de citoyens italiens afin d'alimenter sa base de données de reconnaissance faciale, bien qu'elle ne soit pas active sur le marché européen. La société a ainsi été contrainte d'effacer toutes les données des citoyens italiens et de désigner un représentant au sein de l'Union européenne, assurant la

[12] « La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. » (CNIL, s.d.-d)

protection des droits des citoyens européens (Noyb European Center for Digital Rights, 2022). Par ailleurs, en 2024, c'est l'Autorité irlandaise de protection des données qui a infligé une amende de 91 millions d'euros à Meta Platforms Ireland Limited (MPIL) pour avoir collecté des mots de passe sans cryptage ni protection. La Commission irlandaise de protection des données a constaté que Meta Platforms Ireland Limited (MPIL) avait violé plusieurs articles du RGPD, notamment l'art. 33, al. 1 et 5, puisque Meta n'a pas notifié à la Commission irlandaise la violation des données personnelles dans le délai imparti et a omis de documenter lesdites violations. Meta a également méconnu les art. 5 et 32 du Règlement qui imposent respectivement de garantir un niveau de sécurité approprié et de mettre en œuvre les moyens nécessaires pour l'assurer (Data Protection Commission, 2024). Ces sanctions constituent des exemples emblématiques des conséquences encourues en cas de non-respect du RGPD. Elles illustrent l'importance cruciale, pour les entreprises, d'appliquer ces normes afin de ne pas tomber dans l'illégalité.

b) Limites et difficultés d'application extraterritoriale : coopération et conflits de lois

Malgré l'ambition du RGPD et les exemples concrets de sanctions, la portée extraterritoriale du RGPD soulève des défis majeurs, à la fois internes à l'UE et dans ses relations transatlantiques. Comme le rappelle Yves Poullet, expert en droit de protection des données, l'objectif du RGPD réside dans la mise en place d'un cadre juridique uniforme dans toute l'Union européenne afin d'éviter une législation fragmentée selon chaque État membre. Dans cette logique, le Règlement prévoit, notamment en vertu de son art. 60, une collaboration accrue entre les autorités nationales de protection des données (APD) de chaque État membre. Il instaure également le principe du guichet unique, c'est-à-dire qu'une entreprise a le droit de s'adresser qu'à une seule APD d'un État membre où se trouve son activité principale, même si cette dernière concerne plusieurs États membres (Poullet, 2024 ; CNIL, 2018). Néanmoins, la mise en œuvre concrète de ces mécanismes reste délicate. D'une part, les APD n'interprètent pas toujours le RGPD de la même manière, créant une incertitude persistante pour les entreprises et les citoyens de l'Union (Commission européenne, 2024). D'autre part, les procédures, dans le cas d'un dépôt de plainte par exemple, sont propres à chaque État membre, ce qui rend l'application du RGPD et du guichet unique plus complexe et moins efficace (Poullet, 2024). Enfin, les petites et moyennes entreprises (PME), notamment en France, considèrent les obligations du RGPD complexes, en raison de leur technicité et du poids financier associé (Dal Ponte, 2025).

Ces défis internes illustrent la complexité, encore plus grande, de parvenir à des accords internationaux harmonisés, en particulier avec les États-Unis, où les divergences juridiques en matière de protection des données sont encore plus marquées. Par exemple, le CLOUD Act (Clarifying Lawful Overseas Use of Data Act) adopté par les États-Unis en 2018[13], peut entrer en conflit avec le droit européen, notamment dans le cadre du RGPD. En effet, cette loi permet aux autorités judiciaires américaines d'accéder, dans le cadre d'enquêtes criminelles, aux données personnelles des utilisateurs concernés, même si ces données sont situées en dehors des États-Unis (Christakis & Terpan, 2021). Or, en vertu de l'art. 48 du RGPD, une autorité étrangère peut exiger un transfert de données seulement s'il existe un accord international entre l'UE et le pays tiers. Dans le cas du CLOUD Act, il peut exister un accord bilatéral CAA, mais cette loi n'oblige pas les autorités américaines à respecter toutes les protections prévues par cet accord ni le droit européen, ce qui est susceptible de rendre le transfert illégal au regard du RGPD (Rojszczak, 2020). Un cas emblématique illustrant cette tension juridique est l'amende de 1,2 milliard d'euros infligée à Meta par la Data Protection Commission (DPC) irlandaise en 2023 pour avoir transféré des données personnelles de citoyens européens vers les États-Unis, violant ainsi le RGPD. Les raisons de cette amende record étaient notamment l'absence de mécanismes valides de transfert, tels que les CCT ainsi que la soumission des données transférées aux lois américaines telles que le CLOUD Act et la Section 702 du FISA (Foreign Intelligence Surveillance Act)[14], dont les garanties étaient jugées insuffisantes au regard de la législation européenne (Winters & Delanghe, 2023). Il est important de souligner qu'à ce moment-là, aucun cadre juridique entre l'Union européenne et les États-Unis n'avait été établi depuis l'invalidation du Privacy Shield, ce qui représentait une menace d'autant plus importante pour la protection des données.

II. DEUXIÈME PARTIE : RÉFLEXIONS CRITIQUES ET PROSPECTIVES

1. Souveraineté numérique et capacité normative de l'UE

L'analyse des mécanismes juridiques d'adéquation et les limites pratiques du RGPD soulignent les difficultés à rendre le droit de l'Union européenne effectif dans les pays tiers, particulièrement aux États-Unis, où la protection de droits des individus semble faiblement

[13] Le CLOUD Act a été adopté à la suite de l'affaire Microsoft v. United States afin de préciser si les autorités américaines peuvent obliger une entreprise américaine à transmettre des données stockées à l'étranger, même si cela enfreint la loi sur le territoire local. ((Rojszczak, 2020).

[14] Le Foreign Intelligence Surveillance Act (FISA) régit la surveillance physique et électronique des personnes physiques et morales étrangères, sur le territoire américain et à l'étranger. (Bômont, 2024)

garantie. Dès lors, la capacité de l'UE à faire valoir sa souveraineté numérique face aux grandes puissances est un réel défi. La question est donc de savoir dans quelle mesure le RGPD peut permettre à l'Union européenne d'imposer ses normes sur la scène internationale, en particulier face aux États-Unis.

a) L'UE comme puissance normative : le *Brussels Effect*

La protection des données ne relève plus uniquement du droit ou de la technique, elle est devenue un enjeu géopolitique majeur. Face à la recrudescence des cyberattaques, l'amplification de la surveillance étatique et la domination des géants du numérique – les MAMAA (GAFAM)[15] – aux États-Unis, l'Union européenne aspire à renforcer sa souveraineté numérique (Sigrist, 2025). Malgré les limites de la portée extraterritoriale du RGPD, l'Union européenne dispose d'une influence normative mondiale, notamment dans le domaine de la protection des données, grâce au phénomène connu sous le nom de The Brussels Effect (l'Effet de Bruxelles). Ce concept, introduit en 2012 par Anu Bradford[16], permet à l'Union européenne d'imposer ses normes juridiques au-delà de ses frontières, notamment grâce à l'influence majeure de son marché unique sur les marchés mondiaux. En 2020, Anu Bradford publie un livre intitulé *The Brussels Effect* : *How the European Union Rules The World*, qui analyse de façon concrète ce mécanisme (Groupe d'Étude Géopolitique, s.d.). Bradford (2021) soutient que l'influence et le pouvoir du marché unique suffisent pour inciter les autres pays à adopter les normes européennes, notamment dans le domaine de la protection des données. Ce phénomène, appelé mondialisation réglementaire unilatérale (*unilateral regulatory globalization*), s'opère de manière non intentionnelle et automatique, dès lors que la juridiction exerce une influence mondiale normative. Pour ce faire, cinq conditions doivent être remplies de façon simultanée : un marché suffisamment vaste, une capacité réglementaire et institutionnelle forte, des normes strictes, des cibles inélastiques – c'est-à-dire des sujets qui ne peuvent échapper à l'application de ces normes –, et enfin des normes non divisibles, ce qui signifie que les entreprises ne peuvent modifier leur conformité selon la juridiction (Gunst & De Ville, 2021).

[15] Depuis 2021, les géants de la tech sont appelés MAMAA, pour Meta (ex Facebook), Amazon, Microsoft, Apple, Alphabet (ex Google) (Isautier, 2022).
[16] Anu Bradford est professeure de droit et d'organisations internationales à la Columbia Law School à New York. (Groupe d'Étude Géopolitique, s.d.).

De nombreuses entreprises américaines sont désireuses d'accéder au marché européen, l'un des plus importants et exigeants au monde. Elles sont alors contraintes d'adopter les normes de l'UE, sous peine d'en être exclues. Ainsi, certaines entreprises optent pour une uniformisation de leurs produits ou services pour des enjeux stratégiques telles que l'image, la réputation et la confiance, mais également pour des raisons structurelles, comme les obligations juridiques, les défis techniques ou la recherche d'économie d'échelles (Bradford, 2021). L'un des exemples les plus concrets est évidemment le RGPD : pour accéder au marché européen, les entreprises américaines parmi lesquelles figurent des géants de la tech, doivent se conformer aux règles strictes en matière de protection de données personnelles imposées par l'UE. Ce phénomène se manifeste sous deux formes distinctes: d'un côté, le *de facto* Brussels Effect, c'est-à-dire que les entreprises multinationales se conforment aux normes de l'Union européenne pour éviter de devoir gérer plusieurs systèmes réglementaires, et de l'autre côté, le *de jure* Brussels Effect, qui désigne l'introduction, par certains États, dans leur droit national, des normes similaires ou identiques à celles de l'UE (Furtak, 2022). L'art. 3 du RGPD qui définit sa portée extraterritoriale est un exemple significatif de ce phénomène puisqu'il impose le respect des standards européens à toute structure qui traite des données personnelles des citoyens de l'UE, où qu'elle se trouve. Par ailleurs, l'influence du RGPD s'est étendue au-delà des frontières de l'UE, comme en témoigne le California Consumer Privacy Act (CCPA), adopté en 2018 par l'État de Californie, qui, selon plusieurs experts, s'en serait en partie inspiré. Il en va de même pour le Royaume-Uni post-Brexit : malgré sa sortie de l'UE, Londres ne pourrait éviter les normes européennes et disposerait d'aussi peu de marge de manœuvre que la Californie. (Gunst et De Ville, 2021).

b) Les défis de la souveraineté numérique européenne face à la dépendance technologique

Bien que les États-Unis soient contraints de se conformer aux exigences législatives de l'Union européenne pour pouvoir accéder au marché européen, il est important de souligner que l'UE reste, à bien des égards, dépendante des infrastructures numériques américaines (cloud, systèmes d'exploitation, réseaux sociaux), une dépendance qui n'est pas sans conséquence sur sa souveraineté numérique. Depuis 2020, Ursula von der Leyen, Présidente de la Commission européenne, souligne l'importance cruciale de la souveraineté numérique pour l'avenir de l'UE. Or, cette souveraineté est aujourd'hui confrontée à plusieurs défis liés à la dépendance technologique. Pour certains experts, il en va à l'UE de prendre en main une

souveraineté technologique, qui va au-delà de la souveraineté numérique. Celle-ci désigne la maîtrise complète, du développement à la sécurisation, des technologies stratégiques telles que l'intelligence artificielle, le cloud computing ou encore les semi-conducteurs, devenus essentielles dans les équilibres géopolitiques. Pour y parvenir, l'UE doit bénéficier d'une vision à long terme, investir massivement et avoir une volonté politique forte (Renaissance Numérique, 2022).

Cette ambition ne peut se reposer uniquement sur l'investissement de technologies très innovantes ni sur la seule émergence de géants numériques européens. Elle doit également s'appuyer sur la maîtrise de plusieurs couches technologiques de taille, c'est-à-dire de la matière première à l'exploitation des données. L'une des stratégies possibles pour y parvenir est la coopétition, c'est-à-dire la formation de partenariats entre les entreprises européennes les plus avancées afin de renforcer la compétitivité. Une autre approche est la coopération favorisant l'interopérabilité des systèmes (Renaissance Numérique, 2022). Le projet Gaia-X, mis en œuvre en 2020, est l'un des exemples les plus concrets de cette démarche : il vise à créer une infrastructure européenne des données pour garantir la souveraineté numérique de l'Union européenne afin de rivaliser avec les grandes multinationales américaines du Cloud telles que Amazon Web Services, Microsoft Azure ou encore Google Cloud, qui possèdent actuellement 68 % du marché mondial du cloud (Renaissance Numérique, 2022 ; Musiani, 2025 ; Le Picard, 2025). Contrairement à ces derniers, Gaia-X n'est pas un seul système de Cloud, il s'agit plutôt d'un ensemble de fournisseurs de services indépendants qui collaborent tout en étant connectés par des règles communes. Il favorise la transparence, la portabilité des données, et l'interopérabilité. Une concrétisation pratique de ce projet et qui permettrait de rivaliser avec les Big Tech serait de mettre en place des plateformes européennes interopérables, respectueuse de la liberté d'expression et des valeurs européennes. Dans cette logique, l'Union européenne a investi dans des infrastructures stratégiques, comme les supercalculateurs, les centres de données et les AI Factories, qui pourraient limiter les transferts transatlantiques des données, la surveillance étatique des États-Unis et permettrait à l'UE d'avoir la maîtrise des données personnelles des citoyens de l'UE (de Biase, 2025). Néanmoins, Gaia-X peine à se déployer pleinement et efficacement. Musiani (2025) observe que, « Bien que porteur d'une vision novatrice, ce projet reste fragile, en raison de tensions dans sa gouvernance, d'une maturité technique encore insuffisante et d'un manque d'alignement stratégique entre les différents acteurs européens. »

2. Perspectives d'avenir et nouveaux cadres juridiques transatlantiques

a) Le Data Privacy Framework (DPF) : le nouveau cadre juridique

À la suite de l'invalidation du cadre juridique Privacy Shield, Joe Biden, alors Président des États-Unis, avait signé un décret présidentiel (Executive Order) ayant pour objectif de renforcer les mesures de protection relatives à l'exploitation des données personnelles par les autorités américaines. Ce décret a ainsi permis l'instauration du nouveau cadre juridique désormais appelé EU-US Data Privacy Framework (CNIL, 2024). Avant d'être adopté, ce dernier a été évalué par le Comité européen de la protection des données, qui, dans son avis du 28 février 2023, s'est basé sur le RGPD, les droits fondamentaux de l'UE – Charte des droits fondamentaux et CEDH –, la jurisprudence de la Cour de justice de l'Union et les critères d'adéquation. Parmi les principales améliorations figurent : les principes de nécessité et de proportionnalité, introduits dans le droit américain, c'est-à-dire que les données ne peuvent être collectées, à moins que cela soit nécessaire et proportionné et l'instauration d'une nouvelle voie de recours pour les citoyens européens : la Data Protection Review Court (DPRC) qui est indépendante et dispose d'un pouvoir renforcé. Néanmoins, l'EDPB souligne des préoccupations persistantes liées à ce nouveau cadre juridique, notamment quant au traitement des données à grande échelle sans qu'aucune autorisation indépendante préalable ne soit requise, ni qu'un contrôle régulier ne soit effectué *a posteriori*. En outre, La Foreign Intelligence Surveillance Court (FISC)[17], ne vérifie pas si les programmes de surveillance respectent les nouvelles exigences du cadre juridique, ce qui pourrait mener à un risque d'abus. L'EDPB dénonce également la réponse type apportée par le DPRC lors du recours d'un plaignant : soit il n'y a pas de violation, soit celle-ci a été réparée, sans que le requéreur puisse faire appel de cette décision (European Data Protection Board, 2023).

b) Des garanties encore insuffisantes : le DPF face aux doutes européens

Le réseau European Digital Rights (EDRi)[18] dénonce une perpétuelle surveillance des données, malgré l'accord du nouveau cadre juridique transatlantique. Elle accuse la Commission européenne de minimiser des problèmes déjà identifiés par la Cour de justice de l'Union dans les arrêts Schrems I et II, notamment concernant la surveillance étatique américaine. En outre, le nouveau tribunal de recours – Data Protection Review Court (DPRC)

[17] La Foreign Intelligence Surveillance Court (FISC) veille au respect du FISA (Bômont, 2024).
[18] Le European Digital Rights (EDRi) est le plus grand réseau d'Europe œuvrant pour les droits civils et humains dans le domaine du numérique ((European Digital Rights, s.d.).

– semble pour l'instant plutôt utopique et des doutes persistent quant à son indépendance et son efficacité. Par exemple, l'accès à ce tribunal reste difficile pour les particuliers, car il leur incombe de déposer une plainte dans un cadre légal très strict. En conséquence, très peu de recours sont menés à bien. Autre préoccupation concernant le DPF est le manque de contrôle sur la manière dont les entreprises américaines traitent les données personnelles à des fins commerciales. En plus de la surveillance étatique, il existe également une surveillance commerciale dont les données issues du marketing digital peuvent ensuite être achetées par des agences gouvernementales américaines. Par ailleurs, la supervision du système d'autocertification, où les entreprises doivent elles-mêmes déclarer si elles souhaitent recevoir des données européennes, n'est pas systématique, et les sanctions liées en cas de non-respect sont peu dissuasives. Enfin, l'essor de l'Intelligence Artificielle (IA) n'arrange pas ces problématiques. Les systèmes d'IA, notamment ceux des géants numériques américains, collectent des quantités astronomiques de données, ce qui augmente le risque de violations de la vie privée et complique le contrôle lié à l'utilisation de ces données (de Olazábal, 2024).

Max Schrems, à l'origine des arrêts Schrems I et Schrems II, a récemment déclaré que bien que les lois américaines en matière de surveillance des données violent toujours les droits fondamentaux des Européens, il n'envisage pas de saisir la justice pour l'instant. Selon lui, l'administration Trump, qui a récemment fragilisé les mécanismes de contrôle indépendants en renvoyant trois membres démocrates du Privacy and Civil Liberties Oversight Board (PCLOB)[19], devrait être suffisante afin de décrédibiliser le DPF (Navarro, Mugande et Flakoll, 2025). En effet, le PCLOB, composé de seulement deux membres, au lieu de cinq légalement, n'est plus capable d'atteindre le quorum nécessaire pour délibérer et voter, ce qui fragilise son rôle de contrôle dans le DPF (Cording, 2025). Par ailleurs, en novembre 2023, Philippe Latombe, député français et membre de la CNIL, avait, quant à lui, intenté un recours d'urgence contre le DPF auprès de la CJUE, lequel a, jusqu'à présent, été rejeté faut de preuve d'un préjudice grave en cas de non-suspension de la décision (Cavada, Kieffer, & Bouckaert, 2024).

[19] Le Privacy and Civil Liberties Oversight Board (PCLOB) est une agence américaine indépendante qui a pour objectif de contrôler les programmes de surveillance du gouvernement (Privacy and Civil Liberties Oversight Board, 2022).

En résumé, le DPF suscite une profonde inquiétude auprès des experts européens de protection des données car il ignore les problèmes majeurs déjà soulevés lors de l'invalidation des deux derniers cadres juridiques par la CJUE. Sans une réforme significative des lois américaines de surveillance, le DPF risque d'être invalidé tout comme ses prédécesseurs. Le réseau EDRi insiste à ne pas attendre un Schrems III et appelle la Commission européenne à respecter pleinement les principes du RGPD, sans les compromettre en faveur d'intérêts géopolitiques ou économiques (de Olazábal, 2024). Par ailleurs, d'autres experts et organisations ont, au contraire, salué la mise en place du DPF. Le Centre for Information Policy Leadership (CIPL)[20] (2024) a salué le renforcement des garanties contraignantes, une limitation proportionnée de l'accès aux données et des moyens de recours adéquats pour les citoyens de l'UE. Cependant, il souligne également que les entreprises émettent une certaine prudence suite à l'invalidation consécutive des deux cadres juridiques précédents et continuent ainsi d'utiliser les CCT.

c) Tensions et ambitions pour la gouvernance des transferts de données

Si un accord plus ou moins fructueux – du moins pour certains – est conclu entre l'Union européenne et les États-Unis, un obstacle majeur persiste : l'absence d'une législation fédérale américaine sur la protection des données équivalente au RGPD et remplaçant le CCPA californien, et ce, malgré la pression exercée par l'Union américaine pour les libertés civiles (ACLU) ainsi que plusieurs grands acteurs du numérique tels qu'Amazon, IBM, Mastercard, ou encore Internet Association, le lobby des géants de la tech (Raynouard et Le Grix, 2020). Par ailleurs, les puissants lobbys américains cherchent à défendre la compétitivité des entreprises américaines en continuant à faire pression pour alléger ce qu'ils considèrent comme un fardeau bureaucratique que représente le RGPD. Un exemple emblématique est la réforme potentielle de l'art. 30 du RGPD – qui impose aux responsables de traitement de tenir un registre des activités de traitement – par la Commission européenne, suscitant une vive inquiétude auprès des experts de protection des données (Derouet, 2025). En effet, la Commission européenne propose de réduire les contraintes liées à ce registre, notamment pour les petites et moyennes entreprises (PME). Dans une lettre du 8 mai 2025 adressée à la Commission, L'EDPB et l'EDPS (le Contrôleur européen de la protection des données), ont également fait part de leurs réserves sur certains points quant à cette révision envisagée, invoquant

[20] Le Centre for Information Policy Leadership (CIPL) est un think tank international spécialisé dans la politique des données et de la vie privée (Centre for Information Policy Leadership, 2025).

l'importance cruciale de conserver l'obligation de tenir un registre des activités de traitement en cas de traitements à haut risque (Talus, 2025).

Dans cette perspective de recherche d'un cadre plus stable pour les transferts de données, il est crucial de souligner qu'au cours des dernières années, l'Union européenne et les États-Unis ont intensifié leurs efforts en la matière, notamment à travers des initiatives multilatérales et diplomatiques. Par exemple, la Déclaration de l'OCDE sur l'accès des gouvernements aux données personnelles détenues par le secteur privé signées en 2022 par 38 pays, dont l'UE et les États-Unis, marque une étape majeure dans la coopération internationale pour une protection accrue de la vie privée. Cela montre également que l'UE n'est pas seule à pousser pour davantage de garanties. Cette Déclaration établit sept principes communs encadrant l'accès des pouvoirs publics aux données personnelles détenues par le secteur privé : celui-ci doit s'inscrire dans un cadre légal bien défini, avoir des finalités légitimes et bénéficier d'un contrôle antérieur. En outre, les données doivent être limitées et protégées, les règles transparentes et des voies de recours doivent être mises en place (Organisation for Economic Co-operation and Development, 2022). Cette initiative a pour but de renforcer la confiance dans les échanges de données transfrontaliers et repose sur le respect de la vie privée, des libertés fondamentales et de la transparence (Organisation for Economic Co-operation and Development, 2022-b). Bien que la Déclaration de l'OCDE ne soit pas juridiquement contraignante, elle peut servir de base dans les (futures) discussions d'accords de transferts de données entre l'UE et les États-Unis.

Par ailleurs, le Data Free Flow with Trust (DFFT), initié par le Japon lors du sommet du G20 à Osaka en 2019 et soutenu par le G7, l'Union européenne et les États-Unis, s'inscrit également dans la volonté de concilier transferts des données et protection des droits fondamentaux. Son objectif principal est de supprimer les obstacles liés aux divergences des réglementations nationales en matière de protection des données, afin d'établir des règles harmonisées pour les transferts internationaux. Le DFFT ne cherche pas à uniformiser les lois, mais à les rendre interopérables, c'est-à-dire à assurer leur compatibilité pour permettre des échanges de données sans tensions ni conflits De nombreux efforts sont réalisés pour aboutir au succès de ce cadre international : l'OCDE et la Global Privacy Assembly (GPA) – une association internationale d'autorités de protection des données – jouent un rôle clé dans sa mise en œuvre concrète, en adoptant des résolutions et recommandations, ainsi qu'en établissant des analyses comparatives en prenant en compte le RGPD. (Kopp, 2025).

En parallèle des efforts réglementaires et diplomatiques pour arriver à un compromis sur les transferts des données transatlantiques, il existerait une approche technologique supplémentaire pour assurer la protection des données fondée sur les Privacy-Enhancing Technologies (PETs). Ces technologies sont soutenues par l'Organisation de coopération et de développement économiques (OCDE) le G7, l'Organisation des Nations Unies (ONU), mais aussi par des instances européennes telles que le European Data Protection Board (EDPB) et l'Agence européenne pour la cybersécurité (ENISA). Concrètement, selon Ford (2024) du think tank Centre for European Policy Studies, les PETs sont des « technologies permettant de collecter, traiter, analyser et partager des données tout en protégeant leur confidentialité. » Elles sont capables de masquer une information, traiter des données encryptées et simplifier la coopération pour l'apprentissage à partir de données décentralisées. Ces récentes révolutions ne règlent cependant pas les problèmes juridiques liés à la surveillance et ne viennent pas remplacer le DPF, mais pourraient servir de pilier supplémentaire afin de définir des standards communs et ainsi renforcer la protection des données et faciliter les transferts transatlantiques (Ford, 2024).

CONCLUSION

En définitive, il ne fait aucun doute que les transferts de données personnelles entre l'Union européenne et les États-Unis mettent en évidence une complexité hors norme, où les tensions juridiques, politiques et commerciales sont omniprésentes et sans cesse attisées par des divergences législatives. L'approche européenne, fondée sur la primauté des droits fondamentaux et du principe de protection de la vie privée est, peut-on dire, aux antipodes de la vision américaine, centrée sur la sécurité nationale et la compétitivité économique. Cette opposition structurelle a clairement mis en lumière la fragilité juridique entre les partenaires transatlantiques, comme l'a montré l'invalidation de deux décisions d'adéquation, et pourrait conduire à une énième annulation avec l'actuel Data Privacy Framework (DPF).

En outre, l'UE, de par sa construction politique et juridique unique et de ses 27 États membres, dont les systèmes juridiques sont variés, et les priorités politiques parfois paradoxales, l'application du RGPD présente déjà, à l'échelle intraeuropéenne, des défis considérables. Dès lors, concilier le Règlement européen en composant avec les exigences américaines en matière de sécurité américaine et les intérêts des géants technologiques apporte une touche encore plus délicate à la convergence d'un cadre commun satisfaisant pour les deux parties.

Ainsi, l'avenir des transferts transatlantiques fait face à un équilibre fragile entre coopération et rivalité. Une solution durable se traduirait par des réformes profondes des législations américaines en matière de protection et sécurité nationale, afin de limiter les pouvoirs des services de renseignement américains. Hélas, les États-Unis, en tant que puissance mondiale où sont établis les champions numériques, rendent extrêmement difficile toute négociation qui pourrait nuire à leur compétitivité internationale. Dans ce contexte, l'Union européenne, dépendante des infrastructures dominées par les États-Unis, demeure en quelque sorte peu crédible.

C'est pourquoi la construction d'une souveraineté numérique et technologique est un enjeu primordial. Elle suppose à la fois le renforcement de l'indépendance technologique et le soutien financier des acteurs européens dans les secteurs stratégiques et innovants tels que l'intelligence artificielle, la cybersécurité ou le cloud-souverain. Cette indépendance européenne permettrait de paraître davantage crédible face aux États-Unis et d'entreprendre des négociations de façon concrète. Sans mobilisation réelle des moyens, l'Union européenne restera une puissance normative théorique et non véritablement pratique.

Par ailleurs, la position de la Commission européenne est celle de privilégier la protection de la vie privée et des droits fondamentaux des citoyens de l'UE. Cependant, elle tend à adopter une approche conciliatrice envers Washington afin de lisser les tensions diplomatiques tout en préservant le nouveau Data Privacy Framework (DPF), en particulier depuis le retour de Donald Trump à la Maison-Blanche, événement qui a, sans contexte, ravivé les différends.

À l'international, les projets multilatéraux qui constituent un énième levier d'influence, tels que la Déclaration de l'OCDE ou les Privacy-Enhancing Technologies (PETs), sont aujourd'hui pleinement actifs – avec certains toujours en cours d'aboutissement comme le DFFT – mais leur pérennisation se heurte encore toujours à des défis politiques, juridiques et techniques.

En réalité, les transferts de données entre l'Union européenne et les États-Unis représentent certes une divergence bilatérale, mais la problématique de gouvernance numérique est également mondiale. Tout est finalement une question de rapports de puissance et d'intérêts économiques et politiques. Dans cette optique, si l'Union européenne arrive à se positionner en tant que puissance normative tout en construisant une réelle indépendance technologique, elle

pourra être perçue comme une puissance mondiale capable d'imposer ses standards juridiques de manière contraignante.

BIBLIOGRAPHIE

American Chamber of Commerce to the European Union. (2023). T*ransatlantic data flows: time for a sustainable framework. AmCham EU.*

Blanchard, R. (2020, 25 février). *Données personnelles : la Californie adopte son propre règlement général sur la protection des données*. Deloitte Société D'Avocats. https://blog.avocats.deloitte.fr/donnees-personnelles-californie-adopte-propre-reglement-general-protection-donnees/.

Bômont, C. (2024, juin 3). *Extension de la loi FISA : La « souveraineté numérique » européenne loin des préoccupations américaines (Brève stratégique n°70).* Institut de recherche stratégique de l'École militaire (IRSEM).

Bradford, A. (2021, mars). *The European Union in a globalised world: The "Brussels effect".* Governing Globalization, 2021(1), 75-79. Éditions R.E.D. https://doi.org/10.3917/red.002.0076.

Cavada, J.-M., Kieffer, T., & Bouckaert, C. (2024, mars 25). La décision d'adéquation EU-USA & l'application du Data Privacy Framework (DPF). iDFRights. https://idfrights.org/fr/la-decision-adequation-eu-usa-data-privacy-framework/.

Centre for Information Policy Leadership. (2024, mai 31). *Response to the European Commission questionnaire for EU-US Data Privacy Framework* [PDF]. Hunton Andrews Kurth LLP. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_

eu_commission_questionnaire_for_eu-us_data_privacy_framework__31_may_2024_.pdf.

Centre for Information Policy Leadership. (2025). About. Hunton Andrews Kurth LLP. https://www.informationpolicycentre.com/about.html.

Christakis, T., & Terpan, F. (2021). EU–US negotiations on law enforcement access to data: Divergences, challenges and EU law procedures and options. *International Data Privacy Law*, 11(2), 101-118. https://doi.org/10.1093/idpl/ipaa022.

Comité européen de la protection des données. (s.d.). *L'ancien groupe de travail « article 29 »*. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_fr.

Commission européenne. (2024, 25 juillet). Deuxième rapport sur l'application du règlement général sur la protection des données (COM(2024) 357 final). https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A52024DC0357.

Commission européenne. (s.d.). *Qu'est-ce que le Comité européen de la protection des données (EDPB)*. https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_fr.

Commission Nationale de l'Informatique et des Libertés (CNIL). (2018, 9 juillet). Le guichet unique. https://www.cnil.fr/fr/le-guichet-unique.

Commission Nationale de l'Informatique et des Libertés (CNIL). (s.d.-d). Biométrie. Consulté le 30 juin 2025, sur https://www.cnil.fr/fr/definition/biometrie.

Commission Nationale de l'Informatique et des Libertés. (2016, 23 mai). CHAPITRE I - Dispositions générales CHAPITRE I - Dispositions générales. CNIL. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article1.

Commission nationale de l'informatique et des libertés. (2024, 17 juillet). Adéquation des États-Unis : les premières questions-réponses. CNIL. https://www.cnil.fr/fr/adequation-des-etats-unis-les-premieres-questions-reponses.

Commission nationale de l'informatique et des libertés. (s. d.-b). Responsable de traitement. CNIL. https://www.cnil.fr/fr/definition/responsable-de-traitement.

Commission nationale de l'informatique et des libertés. (s. d.-c). Sous-traitant. CNIL. https://www.cnil.fr/fr/definition/sous-traitant.

Commission Nationale de l'Informatique et des Libertés. (s.d.-e). Chapitre V - Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales, section. Consulté le 12 juin 2025 sur https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article44.

Cording, S. (2025). *Le Data Privacy Framework entre l'UE et les États-Unis : historique, fonctionnement et perspectives (L'AVIS DE L'EXPERT EUROPEEN No. 52).* Comité CCBE. https://www.dbfbruxelles.eu/wp-content/uploads/2025/03/AVISEXPERTEUROPEEN52.pdf.

Cour de justice de l'Union européenne (CJUE). (2015, 6 octobre). *Maximillian Schrems c. Data Protection Commissioner, Affaire C-362/14*. ECLI:EU:C:2015:650. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

Cour de justice de l'Union européenne. (2020, 16 juillet). *Arrêt dans l'affaire C-311/18 Data Protection Commissioner/Maximillian Schrems et Facebook Ireland : La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis* (Communiqué de presse n° 91/20) [PDF]. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf.

Dal Ponte, C. (2025,20 juin). RGPD : quel bilan en 7 ans d'application ? INCYBER NEWS. https://incyber.org/article/rgpd-quel-bilan-en-7-ans-dapplication/.

Data Legal Drive. (2025, 21 janvier). *Tout savoir sur l'application du RGPD hors UE*. https://datalegaldrive.com/rgpd-international-application-rgpd-hors-ue/.

Data Protection Commission. (2024, 27 septembre). Irish Data Protection Commission fines Meta Ireland €91 million. https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta.

de Biase, L.(2025, 10 juin). Gagner la guerre d'indépendance numérique européenne. https://legrandcontinent.eu/fr/2025/06/10/gagner-la-guerre-dindependance-numerique-europeenne/.

de Olazábal, I. (2024, 10 novembre) Promises unkept: The EU-US Data Privacy Framework under fire. https://edri.org/our-work/promises-unkept-the-eu-us-data-privacy-framework-under-fire/.

Derouet, T. (2025, 9 juin). *RGPD : sabrer le registre, ou comment Bruxelles scie la branche de la conformité.* IT For Business. https://www.itforbusiness.fr/rgpd-sabrer-le-registre-ou-comment-bruxelles-scie-la-branche-de-la-conformite-91801.

Deshoulières Avocats. (2025, 24 avril). *RGPD : êtes-vous concerné sans être en Europe ?* https://www.deshoulieres-avocats.com/rgpd-etes-vous-concerne-sans-etre-en-europe/.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Journal officiel n° L 281 du 23/11/1995, p. 31-50. EUR-Lex. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046.

Electronic Privacy Information Center. (s. d.). EPIC. https://epic.org/.

European Data Protection Board. (2023, 28 février). *Avis 5/2023 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le cadre de protection des données UE–États-Unis* [PDF]. https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_fr.pdf.

European Data Protection Board. (s.d.). Membres. Consulté le 7 juin 2025, sur https://www.edpb.europa.eu/about-edpb/about-edpb/members_fr.

European Digital Rights. (s. d.). About us. https://edri.org/about-us/.

European Union. (2025). European Data Protection Board (EDPB). https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_fr.

Ford, C. (2024, 23 février). The EU-US Data Privacy Framework is a sitting duck. PETs might be the solution. CEPS. https://www.ceps.eu/the-eu-us-data-privacy-framework-is-a-sitting-duck-pets-might-be-the-solution/.

Furtak, D. (2022). *Review of The Brussels Effect: How the European Union Rules the World, by A. Bradford*. Recenzje. Sprawozdania Reviews. Reports, Jagiellonian University, Doctoral School of Social Sciences, 29(2), 115–118. https://doi.org/10.17951/k.2022.29.2.115-118.

Groupe d'Études Géopolitiques. (2021). Anu Bradford. https://geopolitique.eu/auteurs/anu-bradford/.

Gstrein, O. J., & Zwitter, A. J. (2021). *Extraterritorial application of the GDPR: Promoting European values or power?* Internet Policy Review, 10(3). https://doi.org/10.14763/2021.3.1576.

Gunst, S., & De Ville, F. (2021). The Brussels effect: How the GDPR conquered Silicon Valley. *European Foreign Affairs Review*, *26*(3), 437-458.https://doi.org/10.54648/eerr2021036.

ICTjournal. (2016, 3 février). *Le Privacy Shield pour remplacer le Safe Harbor*. ICTjournal. https://www.ictjournal.ch/news/2016-02-03/le-privacy-shield-pour-remplacer-le-safe-harbor.

Institut de Recherche Stratégique de l'École Militaire (IRSEM). (2013, 28 septembre). *L'affaire Snowden : révélations, enjeux et conséquences* (Infoveilles n°26). https://www.irsem.fr/storage/file_manager_files/2025/03/infoveilles-26-affaire-snowden.pdf.

Institut de Recherche Stratégique de l'École Militaire. (2013). *Infoveille n°26 : Affaire Snowden* [PDF]. IRSEM. https://www.irsem.fr/storage/file_manager_files/2025/03/infoveilles-26-affaire-snowden.pdf.

Institut des Droits Fondamentaux du Numérique (iDFrights). (2023). *La décision d'adéquation EU-USA & l'application du Data Privacy Framework (DPF).* iDFrights. https://idfrights.org/fr/la-decision-adequation-eu-usa-data-privacy-framework/.

Isautier, C. (2022, 1 juin). Lois de régulation des géants du web, les MAMAA, Meta, Facebook, Amazon, Microsoft, Apple, Alphabet, Google. Tech for Good Canada.

https://techforgoodcanada.com/lois-de-regulation-des-geants-du-web-les-mamaa-meta-facebook-amazon-microsoft-apple-alphabet-google/.

Kopp, N. (2025). *Data Free Flow with Trust (DFFT): Free flow of data while maintaining a high level of protection*. activeMind.legal. https://www.activemind.legal/guides/dfft/.

Le patron d'Apple défend à Bruxelles l'idée d'une loi américaine sur les données personnelles. (2018, 24 octobre). Le Monde. https://www.lemonde.fr/pixels/article/2018/10/24/le-patron-d-apple-defend-a-bruxelles-l-idee-d-une-loi-americaine-sur-les-donnees-personnelles_5373982_4408996.html.

Le Picard, H. (2025). *Startups européennes et IA générative : dépasser la domination des Big Tech (Études de l'Ifri). Institut français des relations internationales (Ifri).* https://www.ifri.org/sites/default/files/2025-04/ifri_le_picard_startups_europeennes_et_ia_2025_0.pdf.

Marcos, K. (2024, 6 septembre). *En vidéo : Qui est Max Schrems, l'activiste autrichien en lutte pour nos données personnelles* [Vidéo]. Le Temps. https://www.letemps.ch/videos/little-sister/en-video-qui-est-max-schrems-l-activiste-autrichien-en-lutte-pour-nos-donnees-personnelles.

McBride, N., Sotto, L. J., & Treacy, B. (2013). *Privacy & data security: The future of the US-EU Safe Harbor* [PDF]. Hunton & Williams LLP. https://www.hunton.com/assets/htmldocuments/uploads/sites/18/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf.

Musiani, F. (2025, 18 juin). Gaia-X : le pari d'un cloud européen souverain. *Polytechnique Insights (La revue de l'institut polytechnique de Paris).* https://www.polytechnique-insights.com/tribunes/digital/gaia-x-le-pari-dun-cloud-europeen-souverain/.

Narvarro, P., Mugande, E., & Flakoll, R. (2025, 2 mai). *The legal uncertainty facing EU–US Data Transfers – Storm over the Atlantic*. Clifford Chance. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/05/the-legal-uncertainty-facing-eu-us-data-transfers-storm-over-the-atlantic.html.

Noyb European Center for Digital Rights. (2022, 10 mars). 20 millions d'euros d'amende pour Clearview AI en Italie. https://noyb.eu/fr/20-millions-deuros-damende-pour-clearview-ai-en-italie.

Organisation for Economic Co-operation and Development. (2022-b, 14 décembre). Adoption d'un accord historique sur la protection de la vie privée dans l'accès aux données relatives à l'application de la loi et à la sécurité nationale. https://www.oecd.org/fr/about/news/press-releases/2022/12/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.html.

Organisation for Economic Co-operation and Development. (2022, 14 décembre). *Declaration on Government Access to Personal Data Held by Private Sector Entities* (OECD-LEGAL-0487). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

Parlement européen & Conseil de l'Union européenne. (2016). *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).* Journal officiel de l'Union européenne, L 119, 1-88. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

Poullet, Y. (2024*). En marge d'un colloque : les sanctions au service du RGPD – une arme à double tranchant*. Communication Commerce Électronique, (4), 24-28. https://pure.unamur.be/ws/portalfiles/portal/96637966/9052.pdf.

Privacy and Civil Liberties Oversight Board. (2022, 14 octobre). History and mission. https://www.pclob.gov/About/HistoryMission.

Privacy International. (s.d.). About Privacy International. https://privacyinternational.org/fr/about.

Rapin, C., Berti, M., & Rodieux, V. (2021, 29 mars). *L'application extraterritoriale du RGPD* [PDF]. Jusletter. https://www.walderwyss.com/assets/content/publications/230718_Lapplication-extraterritoriale-du-RGPD.pdf.

Raynouard, A., & Le Grix, A. (2020). Données personnelles : la Californie adopte son propre règlement général sur la protection des données. Deloitte Blog.

https://blog.avocats.deloitte.fr/donnees-personnelles-californie-adopte-propre-reglement-general-protection-donnees/.

Renaissance Numérique. (2022). *La souveraineté technologique européenne* (Note). https://www.renaissancenumerique.org/wp-content/uploads/2022/01/renaissancenumerique_note_souverainetetechnologique.pdf.

RGPD : Nommer un représentant au sein de l'Union Européenne. (2023, 20 juin). *Data Legal Drive*. https://datalegaldrive.com/rgpd-representant-ue/.

Rojszczak, M. (2020). *CLOUD Act agreements from an EU perspective.* Computer Law & Security Review, 38, Article 105442. https://doi.org/10.1016/j.clsr.2020.105442.

Schrems, M. (2013*). Complaint against Facebook Ireland Ltd – 23 "PRISM"* [PDF]. Europe vs. Facebook. http://www.europe-v-facebook.org/prism/facebook.pdf.

Service de recherche du Parlement européen. (2017, janvier). Le règlement général sur la protection des données (RGPD) (EPRS IDA(2017)595892). https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_FR.pdf.

Sigrist, M. (2025, 15 janvier). La protection des données par l'Union européenne : quels enjeux ? Centre d'Etudes en Diplomatie et Relations Extérieures (CEDIRE). https://www.cedire.fr/articles/la-protection-des-donnees-par-lunion-europeenne-quels-enjeux.

Talus, A. (2025, 8 mai). *Letter to the European Commission on the draft proposal for simplification of record-keeping obligations under the GDPR* [PDF]. https://www.edpb.europa.eu/system/files/2025-05/20250508_edpb-edps-letter-commission-draft-proposal-simplification-record-keeping-obligations-gdpr_en.pdf.

Thelisson, E. (2020). La portée du caractère extraterritorial du Règlement général sur la protection des données. *Revue Internationale de Droit Économique, t. XXXIII*(4), 501 533. https://doi.org/10.3917/ride.334.0501.

Tout savoir sur l'application du RGPD hors UE. (2025, 21 janvier). *Data Legal Drive.* https://datalegaldrive.com/rgpd-international-application-rgpd-hors-ue/.

Winters, K., & Delanghe, L. (2023, May 12). EUR 1.2 billion fine against Meta over EU US data transfers. PwC Legal. https://www.pwclegal.be/en/news/1-2-billion-euros-fine-against-meta-over-eu-us-data-transfers.html.

Wolford, B. (2023, septembre 14). Does the GDPR apply to companies outside of the EU? GDPR.eu. https://gdpr.eu/companies-outside-of-europe/.