UCLouvain

Faculté de droit et de criminologie

Le Règlement Général de la Protection des Données (R.G.P.D) :

Un modèle international en matière de droit de la protection des données ?

Auteur : Alexandre DOMKEN
Promoteur : Alain STROWEL
Année académique 2018-2019
Master en Droit, finalité Droit Européen

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Remerciements

J'aimerais remercier chaleureusement Monsieur Alain STROWEL, promoteur de ce mémoire, pour la liberté et l'autonomie qu'il m'a laissé dans la rédaction de ce travail ainsi que pour ses conseils judicieux concernant ma question de recherche.

Ensuite, mes remerciements les plus sincères vont à ma chère amie Clémence ROMBAUT pour sa relecture attentive, ses remarques précises et son soutien continu tout au long de ce mémoire.

Enfin, Merci à mes proches qui m'ont soutenu durant ces 5 années d'études et tout particulièrement à mon père Dominique DOMKEN qui fut d'une aide et d'une disponibilité sans faille, dans cette épreuve comme dans chacune.

Table des Matières :

Introduction : 1

Titre 1 : Le RGPD en tant que modèle international : 3

Chapitre 1 : Le développement d'un modèle international 4

Section 1 : historique de l'approche européenne du droit à la protection des données 5

Section 2 : Les différentes générations de standards européens 8

§1 : La première génération : La convention 108 et les lignes directrices de l'OCDE 8

§2 : La deuxième génération : La directive 95/46/CE 9

§3 : La Troisième Génération : le RGPD ou le nouveau standard doré 10

Chapitre 2 : Une diffusion *de facto* des lois européennes en matière de vie privée 11

Section 1 : L'Union Européenne comme gardienne mondiale de la vie privée 12

Section 2 : Une forme d'impérialisme réglementaire ? 13

Titre 2 : Les éléments du RGPD qui poussent vers une applicabilité globale du Règlement 15

Chapitre 1 : Portée de la protection de la vie privée : 15

Section 1 : Portée matérielle 15

Section 2 : Portée territoriale 16

Chapitre 2 : Le principe de protection adéquate 17

Section 1 : Les décisions d'adéquation 17

Section 2 : Les sauvegardes adéquates 19

Chapitre 3 : Mécanismes d'exécution 19

Section 1 : Le Principe du Chef de file 20

Section 2 : Sanctions et amendes 21

Section 3 : Illustration Google LLC vs CNIL 22

Titre 3 : Comparaison et Influence sur d'autres juridictions 25

Chapitre 1 : Les Etats-Unis et l'influence européenne en Californie 26

Section 1 : Le « Californian Consumer Privacy Act » 27

§1 : Qu'est ce que le « Californian Consumer Privacy Act » ? 27
§2 : Comparaison choisie avec le RGPD 29
A. Portée Matérielle 29
B. Portée territoriale 30
C. Droits individuels 31
D. Mécanismes d'exécution 32
E. Influence et évolution future 33
Chapitre 3 : Le Japon 34
Section 1 : L'Acte de Protection des Informations personnelles 34
§1 Des amendements au texte et l'influence européenne 34
§2 : Champ d'application de la protection des données 35
A. Portée Matérielle : Définition des « informations personnelles » 35
B. Portée territoriale 36
§3 : Obligations des responsables de traitement et droits individuels 36
§4 : Des mécanismes d'exécutions LIMITES : 38
Section 2. La décision d'adéquation 39
§1 Objectifs de la décision d'adéquation 39
§2: Evaluation de la décision d'adéquation 42
A. Des éléments qui favorisent les standards européens contenus dans le RGPD 42
B. Critiques et interprétation 43
Chapitre 4 : l'Inde: en quête d'une approche indépendante ? 46
Section 1 : Le droit à la vie privée comme droit fondamental 46
Section 2 : Analyse du Personal Data Protection Bill 2018 47
§1 : Terminologie et définition des données personnelles 47
§2 Champ d'application du Personal Data Protection Bill 2018 48
§3 L'incorporation de standards européens et internationaux 49
Section 3 : Critique du PDPB et Raisonnement sur une potentielle décision d'adéquation de la Commission Européenne 51
§1: Motifs pour la légalité de traitement 52

§2: Le pouvoir discrétionnaire du Gouvernement en matière de traitement pour la sécurité de l'Etat 53

§3: L'indépendance fictive de l'autorité Indienne de Protection des Données 54

§4: L'obligation de localisation des données sur le territoire Indien 55

§5: L'omission volontaire de certains droits individuels 57

Section 4: Un quatrième modèle de protection des données ? 57

Conclusion : Le RGPD, un modèle international en droit de la protection des données personnelles ?59

INTRODUCTION :

En matière de politique internationale ou d'affaires étrangères, l'Europe a depuis longtemps acquis une réputation de champion, ou de chevalier blanc, tant elle verse dans le multilatéralisme et encourage une forme de coopération universelle[1]. En effet, en tant que l'une des grandes puissances économiques mondiales, elle se distingue de ses plus proches semblables par une volonté prononcée de faire ce qui est juste ou bénéfique pour le plus grand nombre de citoyens, avec, toujours, ses propres citoyens en tête, mais aussi, souvent, en gardant à l'esprit le bien commun entendu dans une conception humaniste. Amin Maalouf résumait cet esprit en disant que « Forger l'Europe nouvelle, c'est forger une nouvelle conception de l'identité, pour elle, pour chacun des pays qui la composent, et un peu aussi pour le reste du monde. »[2] Cette phrase résume bien l'esprit européen, qui se veut fondamentalement tourné vers l'externalisme et est marqué par un désir de convergence global de ses standards juridiques.

Pour autant, cette dimension externaliste a rencontré nombre de critiques en ce qu'on a pu lui reprocher une approche impérialiste, impliquant de la sorte que si l'Europe n'impose pas unilatéralement ses politiques par la force, elle le fait par contre en se basant sur ses atouts économiques afin d'imposer ses standards aux pays qui sont dépendants de l'accès à son marché intérieur[3]. Pour autant, et nous nous faisons ici l'avocat de l'Union européenne, il nous faut reconnaître que l'Europe n'a jamais contraint aucun acteur économique à pénétrer sur son marché. Plutôt, elle impose une règle objective et applicable à tous, citoyens de l'union ou étrangers : ceux qui opèrent sur son marché se doivent d'en respecter les règles[4].

Cette règle s'applique bien évidemment en matière de protection des données, et particulièrement depuis la date fatidique du 25 Mai 2018, qui sera retenue dans l'histoire comme celle de l'entrée en vigueur du règlement général sur la protection des données

[1] A. BRADFORD, « The Brussels Effect », *107 Nw. U.L. Rev. 1*, 2015, p. 34.
[2] A. MAALOUF, « Les identités meurtrières », 1998.
[3] A. BRADFORD, *op. cit.,* p. 35.
[4] *Ibid.*

2016/679[5] (ci-après RGPD ou le Règlement)[6]. En effet, le nouveau Règlement promeut les standards les plus élevés jamais adoptés et tente de présenter des règles modernes et adaptées à la rapide évolution des technologies de l'information. De plus, le Règlement présente l'objectif de promouvoir des standards aisément transposable à d'autres juridictions, afin de renforcer, au niveau mondial, la protection des données personnelles ; ce désir de convergence globale vers un standard plus uniforme peut s'expliquer d'une part par le désir de protéger au mieux ses citoyens et de garantir une économie numérique qui ne soit pas fractionnée par des conditions d'accès ou d'exercice contradictoires. Pourtant, l'Internet est par nature ouvert à tous et international. De plus, il n'existe pas de structures légales uniformisées qui permettent de contrôler le sort des données exploitées sur le web. Il existe par conséquent un paradoxe entre un Internet ouvert et libre et le respect attendu de la vie privée des citoyens. Pour respecter le Paradoxe, le RGPD n'a sans doute pas d'autres choix que de recourir à une applicabilité large afin d'uniformiser globalement sa mise en place et favoriser le respect des règles protectrices mises en places par ses soins.

Les enjeux de notre question de recherche sont multiples et tenteront de déterminer dans quelle mesure on peut considérer que le RGPD représente un modèle international en droit de la protection des données.

Dans le premier Titre, nous nous attarderons sur les éléments constitutifs d'un modèle international. Pour ce faire, nous dresserons l'historique et l'évolution des standards européens en la matière, qui ont permis de développer les standards portés par le RGPD (Chapitre 1). Ensuite, nous aborderons les facteurs de diffusion de ces standards afin de comprendre dans quelle mesure l'Union européenne a-t-elle la capacité d'imposer son propre régime de façon unilatérale et d'illustrer les conditions sous-jacentes à une telle diffusion réglementaire (Chapitre 2).

Dans le second Titre, nous procéderons à l'analyse juridique de certains éléments choisis du RGPD qui permettent une applicabilité globale de ses dispositions, favorisant ainsi une forme de convergence réglementaire. Parmi ceux-ci, nous étudierons le champ d'application et la portée du Règlement (Chapitre 1), le Principe de protection adéquate (Chapitre 2) et les

[5] 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, *J.O.U.E.*, L 119/1, 4 mai 2016, p. 1 (ci-après "RGPD").

[6] M. RUSTAD et T. KOENIG, « Towards a Global Data Privacy Standard », *Florida Law Review,* vol. 71, no. 2, March 2019, p. 375.

mécanismes d'exécution (Chapitre 3) qui assurent le respect des droits et des obligations contenus dans le texte.

Dans le troisième titre, nous procéderons à une analyse comparée de Juridictions étrangères qui présentent un intérêt particulier du fait de leur rôle en tant que puissances économiques qui présentent à l'origine des approches différentes de l'approche européenne. En premier lieu, nous analyserons l'approche Américaine et les implications et influences portées par le nouvel acte de l'État de Californie (Chapitre 1). Par la suite, c'est le régime japonais que nous passerons à la loupe afin d'examiner les éléments qui furent significatifs dans la décision d'adéquation récemment rendue par la Commission européenne à son égard. Enfin, c'est le régime de l'Inde qui fera l'objet de notre analyse (Chapitre 3).

TITRE 1 : LE RGPD EN TANT QUE MODELE INTERNATIONAL :

Adopté le 27 avril 2016 et entré en vigueur le 18 mai 2018, le RGPD est la nouvelle législation européenne pour la protection des données à caractère personnel dans l'Union européenne (ci-après l'UE ou L'Union), remplaçant ainsi la directive 95/46/CE[7]. Le principal objectif du RGPD étant de "développer une approche globale et cohérente garantissant le respect absolu du droit fondamental à la protection des données à l'intérieur du territoire de l'UE et au-delà[8]", le Règlement contient des règles qui protègent les personnes physiques du traitement de leurs données à caractère personnel tout en garantissant la libre circulation des ces données entre les États membres. De plus, le RGPD protège à son tour le droit à la protection des données à caractère personnel en tant que droit fondamental[9].

Au cours de la période de transition de deux ans qui a précédé son entrée en vigueur, les citoyens et les entreprises européennes ont réajusté leurs activités afin de se conformer à ses dispositions strictes. Cependant, la portée matérielle et territoriale du RGPD implique que ce ne sont pas seulement les entreprises de l'UE qui devraient œuvrer à une mise en conformité,

[7] 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, *J.O.C.E*, L 281/3, 23 novembre 1995, *p. 31* (ci-après "directive données personnelles").

[8] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions - «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», p. 4.

[9] Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C 364 du 18 décembre 2000, Article 8.

mais pareillement toutes les entreprises hors UE qui entrent dans le champ d'application élargi du RGPD[10].

Tout d'abord, ce chapitre montre comment le RGPD s'efforce de devenir l'instrument international permettant à l'Union européenne de mener sa politique de protection des données à l'échelle internationale (chapitre 1). Ensuite, nous discuterons des facteurs qui en permettent la diffusion ainsi que de la manière européenne de traiter de la protection des données (chapitre 2).

CHAPITRE 1 : LE DEVELOPPEMENT D'UN MODELE INTERNATIONAL

Ces dernières années, et plus particulièrement depuis des événements tels que les révélations d'Edward Snowden sur le programme PRISM[11] en 2013 ou le scandale Facebook Cambridge Analytica[12] en 2018, le monde s'est progressivement mis d'accord sur la nécessité d'améliorer les réglementations en matière de protection des données personnelles au niveau international. Il semblerait aujourd'hui que l'Union européenne soit le chef de file des dernières discussions sur la protection des données et qu'elle s'en soit octroyée la place de leader incontesté avec l'entrée en vigueur du RGPD[13]. Au niveau international en effet, plus de 120 pays ont promulgué des lois sur la confidentialité des données inspirées du cadre législatif européen[14] et plus de 30 pays ont promulgué des projets de loi officiels sur le sujet qui en reprennent les grands principes[15].

La concrétisation idéale de cette tendance internationale à la convergence globale en matière de législation sur la confidentialité des données aurait été de créer un cadre international qui favoriserait mondialement les mêmes normes et standards de confidentialité, permettant l'édification d'un vaste marché mondialisé et harmonisé en cette ère numérique. Avant le RGPD, divers instruments de protection des données, tels que des conventions internationales

[10] O. KARADUMAN, "The General Data Protection Regulation: Achieving compliance for EU and non-EU companies", *Business Law International*, Volume 18, Issue 3, 2017, p. 1.

[11] Le 6 juin 2013, les journaux de renom *The Guardian* et *The Washington Post* révélèrent des documents confidentiels -précédemment délivrés par Edward Snowden – en rapport avec le programme de surveillance de masse PRISM, utilisé par la National Security Agency américaine (NSA) pour accéder aux services internet et de communication à travers le globe.

[12] Cambridge Analytica est une entreprise britannique qui récolta les données personnelles de 87 millions de personnes – en ce inclus 2,7 millions de citoyens européens- en exploitant une faille dans les systèmes du réseau social Facebook.

[13] P. ALBRECHT, « How the GDPR will change the world », *European Data Protection Law*, 2016, p. 287.

[14] G. GREENLEAF, « Global Data Privacy Laws », *145 Privacy Laws and Business Int'l Report*, 2017, pp. 10-13.

[15] *Ibid.*

ou des lignes directrices émises par des organisations internationales, étaient déjà en vigueur. Toutefois, ces divers instruments étaient pour la plupart trop dispersés et sectoriels, et souvent non juridiquement contraignants. Ces éléments compliquaient la possibilité de créer un cadre international unique[16] et un standard commun. En effet, pour déterminer comment un tel cadre pourrait fonctionner, les différences culturelles et juridiques entre les différents systèmes doivent être contrôlées par le haut[17] et, si possible, également contraignantes pour leurs sujets.

SECTION 1 : HISTORIQUE DE L'APPROCHE EUROPEENNE DU DROIT A LA PROTECTION DES DONNEES

Pour comprendre comment le RGPD a pu voir le jour et dans quelle mesure sa mise en vigueur a pu révolutionner l'approche européenne, il est intéressant de revenir quelque peu sur le processus et sur le cadre juridique qui a précédé son adoption. Mieux encore, cette section tentera de résumer brièvement l'historique européen en matière de protection des données afin de comprendre d'une part, cette conception – typiquement européenne jusqu'il y a peu – de considérer le droit à la vie privée comme un droit fondamental pour les citoyens et d'autre part, comment la création d'un modèle international est indissociable de la promotion de différents niveaux de standards que ce modèle tente de faire adopter globalement.

La conception européenne de la protection des données et, plus généralement, du droit à la vie privée trouve son origine en 1950. En effet, à la sortie de la seconde guerre mondiale, l'Europe considéra, de façon assez compréhensible, le droit à la vie privée comme un droit fondamental pour chacun de ses citoyens[18]. C'est en effet à l'article 8 de la Convention européenne des droits de l'homme (ci-après "CEDH") que l'on retrouve les premières dispositions protégeant le droit à la vie privée en Europe en ce que cet Article 8 dispose « Chacun a le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance»[19]. La Cour européenne des droits de l'homme a en effet interprété cette

[16] C. KUNER, « The European Union and the Search for an International Data Protection Framework », *Groningen Journal of International Law*, 2014, p. 58.
[17] *Ibid*., p. 66.
[18] C. GLON., « Data Protection in the European Union : a closer look at the current patchwork of Data Protection Laws and the proposed reform that could replace them all », *International Journal of Legal Information,* vol. 42.3*,* 2015, p. 472.
[19] Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et Protocole additionnel, signé à Paris le 20 mars 1952, approuvés par la loi du 13 mai 1955, *M.B.,* 19 août 1955, p. 5028 (ci-après "CEDH"), Article 8.

notion de vie privée très largement afin d'y inclure la notion de protection des données personnelles, et cette jurisprudence s'est confirmée dans plusieurs affaires[20].

Depuis lors, différents instruments internationaux et européens ont vu le jour et ont participé à construire les différents standards de protection de la vie privée que nous connaissons aujourd'hui. Pour commencer, il est bon d'aborder deux instruments internationaux qui sont à la base de la directive, d'abord, et du Règlement ensuite et qui virent le jour dans les années 1980.

Premièrement, les lignes directrices de l'Organisation de coopération et de développement économiques (ci-après OCDE) régissant la protection de la vie privée et les flux transfrontières de données à caractères personnel[21] constituent l'un des premiers textes internationaux à promouvoir un ensemble de principes et de sauvegardes de la vie privée. Ces lignes directrices constituent une réponse à deux problématiques : la première étant la volonté de reconnaître l'importance des informations personnelles dans une économie globale – et particulièrement à l'aube de la digitalisation – , la seconde afin d'anticiper le possible impact sur les droits individuels résultant des premiers traitements de données personnelles par la première génération d'ordinateurs[22]. Ces lignes directrices représentent la première forme de standards et de principes mis à la disposition des gouvernements pour protéger la vie privée de leurs citoyens et furent à la base de nombreux textes de lois qui constituent les premières réglementations en matière de protection de la vie privée parmi les Etats Membres[23] de l'OCDE. Également, et surtout au niveau international, ces lignes directrices se révélèrent particulièrement influentes pour des Etats non-européens comme les Etats-Unis, le Japon, le Canada ou encore l'Australie[24].

Deuxièmement, ce fut au tour du conseil de l'Europe de participer au développement du régime de protection de la vie privée en adoptant, en 1981, la Convention pour la protection

---

[20] Cour eur. D.H., arrêt *Amann c. Suisse,*16 février 2000, *Rec. Cour eur. D.H.*, 2000-II, point 65 ; Cour eur. D.H., arrêt *Rotaru c. Roumani*e, 4 mai 2000, *Rec. Cour eur. D.H.*, 2000-V, point 43 ; Cour eur. D.H., arrêt *Copland c. Royaume-Uni,* 25 juin 1997, *Rec. Cour eur. D.H.*, 1997-III, point 41.

[21] Ces lignes directrices ont depuis été mises à jour en 2013 ; *2013 OECD Privacy Guidelines,* ORG. ECoN**.** CO-OPERATION & DEV., 2013, disponible sur: http://www.oecd.org/sti/ieconomy/oecd- privacy-framework.pdf., consulté le 30 Mai 2019.

[22] OECD, « 30 years after the OECD Privacy Guidelines », 2011, disponble sur: http://www.oecd.org/sti/ieconomy/49710223.pdf , consulté le 30 Mai 2019.

[23] *Ibid.* p. 3.

[24] P. HUSTINX, « EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation » *in New technologies and EU Law,* M. CREMONA (dir.), Oxford Scholarship online, 2017, p. 7.

des personnes à l'égard du traitement automatisé des données à caractère personnel, plus connue sous le nom de « Convention 108 »[25]. La Convention 108 fut véritablement le premier instrument international à être juridiquement contraignant[26] pour ses signataires. De plus, ce traité a eu dès son entrée en vigueur une vocation universelle et fut considéré comme le premier cadre de référence pour l'adoption de lois nationales relative à la protection de données personnelles[27].

Malgré le consensus international selon lequel cet instrument pourrait servir de base à une norme internationale de protection des données, il ne s'applique pas directement à une partie quelconque en tant que convention et ne crée aucun droit individuel pour les citoyens[28]. Contrairement à leur nom, les conventions du Conseil européen sont ouvertes aux signataires extérieurs à l'Europe[29] [30], mais exigent que les Etats signataires appliquent volontairement leurs principes et leurs mécanismes d'application dans leur droit national. Ce processus législatif indirect contribue donc au caractère dispersé du cadre créé par ce type d'instruments[31]. En effet, au sein de l'Union, la réception et surtout l'implémentation de la Convention 108 ne se sont pas déroulées de façon uniforme dans tous les Etats Membres[32], ces divergences perturbant le bon fonctionnement du marché européen.

Pour pallier à ce problème, et afin d'harmoniser l'échange de données personnelles entre les Etats membres, la commission se basa sur la Convention 108 et sur les lignes directrices de l'OCDE lors des propositions de rédaction de la Directive 95/46/EC. En effet, le but premier de la directive était de fournir des standards supérieurs en matière de protection de la vie privée à ce qui se faisait jusqu'alors avec la Convention 108, comme le souligne la Commission : « les principes généraux énoncés dans la Convention du Conseil de l'Europe sont une référence à prendre en compte car ils constituent déjà une base commune pour les pays l'ayant ratifié. Ainsi, tout en adoptant des solutions compatibles avec celles de la

[25] Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n°108), faite à Strasbourg le 28 janvier 1981.
[26] En 1980, les « OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data » avaient déjà été adoptées mais il s'agit là d'un instrument international non contraignant.
[27] G. GONZALEZ FUSTER, *The emergence of Personal Data Protection as a Fundamental Right of the EU*, Etats-Unis, Springer International, 2014, p. 92.
[28] C. KUNER, « The European Union and the Search for an International Data Protection Framework », *op. cit.,* p. 58.
[29] G. GREENLEAF, « The influence of European data privacy standards outside europe: Implications for globalization of convention 108 », *International Data Privacy Law*, Vol. 2, 2012, p. 69.
[30] L'Uruguay fut le premier Etat tiers à ratifier la convention en 2013.
[31] M. LANGHEINRICH, « The Golden Age of Privacy ? », *IEEE Pervasive Computing,* 2018, p. 4.
[32] P. HUSTINX, *op. cit*., p. 7

Convention, la directive complète ces principes généraux afin d'établir une protection (...) de haut niveau »[33].

Lors de son adoption, la Directive vit le jour afin de faciliter les échanges de données personnelles entre les Etats membres tout en préservant les droits fondamentaux des citoyens. Également, la Commission a très vite reconnu que les traitements de données réalisé par un acteur tiers, et qui plus est en dehors du territoire européen, ne pouvaient en aucun cas influencer le niveau de protection offert aux citoyens européens en matière de protection de la vie privée.

SECTION 2 : LES DIFFERENTES GENERATIONS DE STANDARDS EUROPEENS

Il semble aujourd'hui que le RGPD soit apte à propager globalement les standards européens en matière de protection des données personnelles, et soit également reconnu comme tel[34]. Pour autant, et comme cela a été démontré dans la section précédente, ce n'est pas le premier instrument européen qui ait eu une portée internationale. Ce qui le rend si singulier, c'est aussi et surtout le niveau élevé de protection qui le caractérise, en ce que le RGPD est l'aboutissement d'une troisième génération de standards européens.

§1 : LA PREMIERE GENERATION : LA CONVENTION 108 ET LES LIGNES DIRECTRICES DE L'OCDE

La première génération de standards fut majoritairement constituée par les lignes directrices de l'OCDE, d'une part, et la Convention 108, d'autre part[35]. Ces deux instruments internationaux ont produit les grands principes qui furent repris à travers le globe comme les principes fondamentaux de protection de la vie privée. Il semblerait qu'en 2018, pas moins de 126 pays disposent de lois qui reprennent les standards repris à l'article 4 de la Convention 108[36].

Le droit à la protection des données personnelles fut construit par cette première génération de standards. Le conseil de l'Europe, via la Convention 108, proposa une protection proactive des droits des citoyens face à tout type de traitement de leurs données. Cette protection encouragea les Etats signataires à créer un système de contrepoids afin de garantir une

[33] Première proposition de Directive, exposé des motifs, p. 18.
[34] G. GREENLEAF, « Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018 », *UNSW Law Research Paper No. 18-56*., 24 Mai 2018, p. 2.
[35] *Ibid.* p. 3
[36] *Ibid*.

protection structurelle à un large nombre d'individus, face à des situations de traitements issus tant du secteur privé que public[37].

Il est important de souligner que cette première génération de standards, aussi cruciale fut-elle au développement législatif que nous connaissons depuis les années 1990[38], ne constitue plus aujourd'hui un niveau de standard adéquat, mais plutôt simplement un critère minimal qui sert, entre autre, à anticiper le contrôle d'adéquation de la Commission européenne lors de l'examen des sauvegardes adéquates d'un Etat tiers à l'Union européenne. En effet, on peut lire au considérant 105 du RGPD que la Commission européenne est invitée à prendre en compte la Convention 108 lors de l'évaluation de l'adéquation d'un système étranger[39]. Afin de pallier à cette problématique, et pour que la Convention 108 puisse être pertinente en tant que premier niveau de standard à atteindre dans le cadre européen, le texte de la convention a récemment fait l'objet d'une réforme, sous le nom de Convention 108+[40]. Celle-ci se rapproche du niveau d'exigence qui fut développé à sa suite, par la Directive 95/46/EC d'abord, et par le Règlement ensuite. Cette réforme s'avérant nécessaire afin de maintenir une cohérence avec le cadre européen actuel[41].

§2 : LA DEUXIEME GENERATION : LA DIRECTIVE 95/46/CE

La directive permit à l'Europe d'aller plus loin que la Convention 108 et que les lignes directrices de l'OCDE. En effet, c'est par ce nouvel instrument que l'Europe a commencé à promouvoir un modèle de protection des données globalement applicable. La directive fut le premier instrument à promouvoir des recours pour les citoyens afin d'obtenir une mise en œuvre de leurs droits, un droit à la destruction des données ou à l'anonymisation, le principe d'un traitement équitable et légitime, ainsi que les premières formes du droit d'objection, parmi d'autres. Également, elle instaura les autorités de protection des données dans chaque Etat membre

---

[37] P. HUSTINX, *op. cit.*, p. 10.

[38] G. GREENLEAF, « Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018 », op. cit.

[39] Considérant 105, RGPD : « la Commission devrait tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en ce qui concerne la protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel ».

[40] Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 mai 2018.

[41] Rapport explicatif de la Convention 108 telle que modifiée par le Protocole d'amendement, série des traités du Conseil de l'Europe n°223, 2018, p. 2.

L'intérêt de cette deuxième génération pour ce travail réside surtout dans le fait que le modèle réglementaire de la Directive fut largement repris sur la scène internationale[42].

§3 : LA TROISIEME GENERATION : LE RGPD OU LE NOUVEAU STANDARD DORE

Ce n'est autre que le RGPD qui constitue la 3e génération de standards du régime européen, constituant à ce jour les standards globalement applicables les plus élevés, tant au niveau européen qu'au niveau international. Là où le Règlement innove, c'est dans sa façon de rendre la protection des données plus efficace en pratique, par une grande implémentation de ses principes au niveau européen et également par un accent mis sur les mécanismes d'exécutions qui garantissent les droits et les obligations contenus dans son texte[43]. Une particularité propre au RGPD, qui caractérise également son niveau de protection élevé, s'explique par le fait que le règlement n'apporte plus autant d'importance à la *localisation* des données traitées, mais plutôt à la *responsabilité* et à *l'impact* de ce traitement sur les individus[44]. En effet, l'approche européenne a évolué d'un contrôle *a priori*, sous la directive, à un contrôle *a posteriori* et à une responsabilité poussée pour les entreprises sous le RGPD. Cette évolution pourrait presque être qualifiée de révolution copernicienne[45], en ce que l'Europe s'est éloignée de ses exigences de conformité quelque peu bureaucratiques afin de promouvoir une conformité plus concrète et pratique, des droits individuels plus étendus et une meilleure harmonisation de ces standards parmi les Etats membres[46].

C'est aussi et avant tout le constat d'une applicabilité très large qui renforce la protection des citoyens en ce que les responsables de traitements ne peuvent plus « jouer avec les règles territoriales » qui entourent le traitement des données, comme c'était encore le cas sous la directive[47].

On pourrait dégager trois caractéristiques de ces standards dorés, qui sont aujourd'hui repris en référence pour le développement du régime de protection des données.

Premièrement, le Règlement dispose d'une portée étendue, qui peut être qualifiée d'extraterritoriale. Alors que nous développerons précisément le champ d'application du

[42] S-K. PRASAD, , « Back to the Basics: Framing a New Data Protection Law for India », 30 Janvier 2018, p. 5.
[43] P. HUSTINX, *op. cit*., p. 29.
[44] *Ibid*., p. 42.
[45] C. KUNER, « The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 11 PVLR 215, 2 Juin 2012, pp. 1-15.
[46] *Ibid.*
[47] *Ibid.*

RGPD dans le prochain titre, il est bon de souligner ici que la première amélioration de la protection offerte par le RGPD s'explique par le fait que le Règlement s'applique pour tout type de traitement aussitôt qu'une entreprise est établie en Europe, mais également dès que les activités économiques de cette entreprise sont ne fût-ce que dirigées vers le marché européen ou que le comportement des citoyens européens est contrôlé, nonobstant le lieux de traitement de ces données[48] .

Deuxièmement, le Règlement requiert que les données personnelles ne soient pas transférées dans un Etat tiers, sauf dans la situation où l'état récipient peut faire valoir un niveau de protection adéquat ou qu'il parvient à fournir des sauvegardes adéquates. Si ces conditions étaient déjà présentes sous la directive, le RGPD les clarifie et surtout permet d'autres options dans des situations spécifiques, tout comme les règles d'entreprises contraignantes, contenues à l'article 47 du RGPD.

Troisièmement, le RGPD encourage au développement d'une coopération internationale entre les autorités de protection des données ; le pouvoir de marché de l'union européenne, représentant approximativement 500 millions d'utilisateurs, est en mesure d'encourager une convergence globale des standards européens en ce que les entreprises transfrontalières se verront contraintes d'adapter leurs propres standards aux standards européens. De plus, il faut garder à l'esprit que les régimes de la Convention 108 ou des lignes directrices de l'OCDE ont été adaptés afin de respecter le régime européen, de la directive et ensuite du règlement. Le fait que ces deux instruments aient été réécrits dans une approche qui respecte les standards européens permet de centraliser ces standards autour d'un seul instrument suprême - le RGPD – et d'en promouvoir les grands principes à tous les niveaux de la protection des données.

CHAPITRE 2 : UNE DIFFUSION *DE FACTO* DES LOIS EUROPEENNES EN MATIERE DE VIE PRIVEE

L'approche européenne avec le RGPD, en ligne avec ce qui avait été accompli avec la Directive 95/46, peut donc être justifiée par le fait qu'aucune organisation contraignante ne pourrait jouer le rôle de superviseur international en matière de protection des données. En conséquence, le RGPD est caractérisé par une tension entre la volonté de renforcer un cadre

[48] P. HUSTINX, *op. cit.*, p. 42.

juridique international et l'accent de plus en plus focalisé sur le droit fondamental à la protection des données personnelles reconnu par l'UE à ses citoyens[49].

Il semble clair aujourd'hui que la manière européenne de traiter la protection des données au niveau international passe par l'application de ses propres lois de façon extraterritoriale[50]. En fait, l'UE étend sa protection juridique à tout traitement de données concernant les citoyens européens, quelle que soit leur localisation, et remplit ainsi la même fonction qu'un cadre international uniforme. À la recherche d'un cadre international et confrontée au manque de solutions de rechange valables, l'UE a donc décidé de prendre les choses en main avec le RGPD. La portée extraterritoriale du RGPD «Article 3», qui sera détaillée dans la section suivante, permet à ses dispositions de protéger les données des citoyens de l'UE chaque fois que ces informations sont transférées hors du territoire européen[51]. Parallèlement à sa vaste portée territoriale, le RGPD exige que les pays tiers souhaitant pénétrer sur son marché se conforment aux normes de protection des données de l'UE, car les transferts internationaux de données sont soumis au principe d'adéquation[52].

SECTION 1 : L'UNION EUROPEENNE COMME GARDIENNE MONDIALE DE LA VIE PRIVEE

Avec le RGPD, l'Europe est de facto devenue la «police de la vie privée» au niveau mondial[53]. Plus précisément, les causes de la diffusion de la réglementation européenne sur la protection des données personnelles résultent du fait que l'UE associe un vaste pouvoir de marché à une grande préoccupation pour le droit à la vie privée des citoyens ; l'Union promeut ces deux aspects dans sa politique internationale et les brandit dans ses négociations avec tout acteur qui souhaite pénétrer sur son territoire. En effet, L'UE possède des arguments de poids en ce qu'elle représente la deuxième économie mondiale et le deuxième marché de consommateur le plus vaste[54].

Plus important encore, l'UE a toujours été un chef de file dans le secteur des technologies de l'information et des services de télécommunications, représentant ainsi un important marché-

[49] C. KUNER, « The European Union and the Search for an International Data Protection Framework », *op. cit.*, p. 66.
[50] *Ibid.*
[51] P. SCHWARTZ, « Global Data Privacy : The EU Way », *New York University Law Review*, Vol. 94, 2019, p. 7.
[52] Article 46, RGPD.
[53] P. SCHWARTZ, *op. cit.*, p. 1.
[54] *Ibid.*, p. 7.

cible pour les entreprises internationales[55]. En raison de la valeur du marché européen dans l'équilibre international, peu d'entreprises – et surtout pas les plus grandes telles que Facebook, Amazon, Google, Microsoft ou Apple – peuvent se permettre de laisser de côté le marché européen[56]. En effet, le fait de devoir organiser leurs activités selon deux types de réglementations différents constituerait un fardeau extraordinaire pour les entreprises[57], que ce soit en raison du seuil de difficulté élevé pour classer géographiquement un marché numérique ou des coûts auxquels elles seraient confrontées si elles créaient des services séparés pour chaque marché sur lesquels elles exercent leur activité économique[58].

Le pouvoir de marché de l'UE lui permet donc d'imposer *de facto* et de façon unilatérale ses propres réglementations et ses propres standards en une forme de globalisation réglementaire unilatérale, ou «effet de Bruxelles»[59]. Il semble que l'UE soit en mesure d'extérioriser ses lois et réglementations au-delà de son territoire par le biais de son marché intégré, ce qui entraîne la mondialisation de ses normes[60] ; il est en effet beaucoup plus efficace pour les entreprises de mettre en œuvre mondialement les réglementations européennes plutôt que d'essayer d'aligner leur marché numérique aux différentes frontières nationales[61]. En conséquence, lorsque l'UE réglemente son propre marché, les multinationales sont fortement incitées – pour ne pas dire obligées - à suivre ces règles spécifiques et à normaliser leur propre production et leurs propres services en conséquence. Grâce à ce mécanisme, l'UE est en mesure d'étendre *de facto* la portée territoriale du RGPD, ce qui oblige les acteurs du marché étrangers à respecter les règles de l'UE en matière de vie privée, quelle que soit la nationalité de leurs consommateurs.

SECTION 2 : UNE FORME D'IMPERIALISME REGLEMENTAIRE ?

En outre, un autre phénomène qui favorise la diffusion des règles de l'UE en matière de vie privée réside dans le fait que les sociétés multinationales qui ont déployé des efforts considérables pour se conformer aux normes de l'UE finissent souvent par faire pression pour que le même type de normes soit adopté par leur État d'origine, ce qui leur conférerait

[55] *Ibid.*, p. 9.
[56] J. GOLDSMITH et T. WU, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006, p. 176.
[57] A. BENDIEK et M. RÖMER, « Externalizing Europe: the global effects of European data protection », *Digital Policy, Regulation and Governance*, Vol. 21 Issue: 1, 2019, p. 35.
[58] P. SCHWARTZ, *op. cit*., p. 7.
[59] A. BRADFORD, *op*. cit., p. 3.
[60] *Ibid*.
[61] A. BENDIEK et M. RÖMER, *op. cit*., p. 35.

un avantage concurrentiel par rapport à d'autres entreprises qui ne se sont pas adaptées et qui ne respectent pas les normes adéquates pour pénétrer sur le marché européen[62].

À titre d'exemple concret, de nombreuses entreprises aux États-Unis ont fini par se mettre en conformité avec le Règlement, car elles travaillaient avec des partenaires commerciaux déjà conformes au RGPD. Par la force des choses, ces partenaires commerciaux conformes ne sont donc plus en mesure d'accepter de recevoir ou de travailler avec des données non conformes aux critères du RGPD en raison du risque d'amende qu'ils encourent qui est trop élevé. Par conséquent, ces entreprises se voient contraintes de se conformer indirectement aux dispositions européennes, même si elles n'entrent pas explicitement dans le champ d'application du RGPD[63].

Nous pouvons donc également observer qu'il peut y avoir non seulement une application *de facto* mais aussi *de jure* des règles de l'UE, dont le respect est progressivement encouragé par toutes les entreprises d'Etats tiers qui s'adressent à leurs législateurs afin qu'ils agissent dans le sens d'une conformité généralisée aux normes européennes[64].

En conclusion, pour répondre à l'absence d'instruments internationaux qui permettraient une application globale et uniforme de standards à utiliser dans le domaine de la vie privée, l'UE a saisi l'opportunité de créer une forme d'impérialisme réglementaire par l'utilisation de lois omnibus[65] qui réglementent tant la sphère publique que privée par des règles générales et facilement applicable dans les différents systèmes nationaux. Le RGPD est le résultat de l'élaboration d'un modèle réglementaire de protection de la vie privée. Ce modèle fournit un cadre complet facilement accessible en dehors de l'UE[66], compte tenu en particulier de l'intérêt que représente le marché intérieur de l'UE pour d'autres juridictions internationales, les incitant de la sorte à adopter le modèle européen. La loi européenne sur la protection des données a également un potentiel de transposition élevé au niveau international. La loi

[62] A. BRADFORD, *op. cit.*, p. 5.
[63] C. BARRETT, « Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? », *Scitech Lawyer*, Vol. 15(3), 2019, p. 2.
[64] P. SCHWARTZ, *op. cit.*, p. 8.
[65] Le terme de loi omnibus est typiquement utilisé en distinction avec les lois dites sectorielles et couvre les loi qui comprennent un large champ d'application tant pour les entreprises et les personnes morales que pour les personnes privées.
[66] *Ibid.*, p. 29.

brésilienne le prouve; non seulement le Brésil a-t-il modélisé ses propres dispositions sur le RGPD, mais il a également donné le même nom à son propre règlement[67].

TITRE 2 : LES ELEMENTS DU RGPD QUI POUSSENT VERS UNE APPLICABILITE GLOBALE DU REGLEMENT

Le deuxième Titre isolera trois des principaux éléments du RGPD participant à la diffusion internationale du standard doré de l'UE en tant que modèle international facilement transposable et favorisant la conformité globale au modèle européen de confidentialité des données. Cette partie différenciera donc premièrement le champ d'application du RGPD (Chapitre 1) facilitant une application de facto à grande échelle du Règlement; deuxièmement, nous aborderons le principe d'adéquation (Chapitre 2), qui facilite les négociations bilatérales et permet à l'UE de faire des compromis afin de favoriser la mise en place de garanties adéquates et de normes harmonisées avec les États tiers. Enfin, nous conclurons cette seconde partie par une analyse des pouvoirs d'exécution conférés aux Autorités de Protections des Données (APD) (Chapitre 3) qui poussent les entreprises du monde entier vers une conformité au Règlement tant le risque de lourdes amendes est dissuasif.

CHAPITRE 1 : PORTEE DE LA PROTECTION DE LA VIE PRIVEE :

SECTION 1 : PORTEE MATERIELLE

Le champ d'application du RGPD est plus large que celui de la directive 95/46/CE. Dans le Règlement, le domaine matériel concerne tout traitement de données à caractère personnel par un processeur ou un contrôleur[68]. La définition du traitement n'a pas changé dans le RGPD et inclut toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, comprenant ainsi tout traitement allant de la collecte à la destruction de ces données[69].

Les données personnelles sont définies comme «toute information concernant une personne physique identifiée ou identifiable[70]», ce qui signifie qu'elles incluent toutes les informations, prises individuellement ou non, qui peuvent identifier des personnes directement ou

[67] *Ibid*., p. 30.
[68] Article 2, RGPD.
[69] Article 4 (2), RGPD.
[70] Article 4 (1), RGPD.

indirectement[71]. La définition comprend un ensemble d'exemples de ce qui peut constituer des données personnelles.

Pour conclure, deux critères sont essentiels pour identifier ce qui constitue une donnée à caractère personnel: premièrement cela ne concerne que les personnes physiques et les personnes physiques uniquement; deuxièmement cela permet d'identifier la personne physique concernée. Cette définition est très large et montre l'intention du régulateur européen de couvrir presque tous les types de données, à l'exception des données à caractère personnel collectées strictement dans le cadre d'une activité personnelle ou domestique[72].

SECTION 2 : PORTEE TERRITORIALE

En ce qui concerne le champ d'application territorial du RGPD, l'article 3 adopte volontairement de larges critères d'applicabilité. Selon la Commission européenne, deux critères principaux déterminent quelles entités entrent dans le RGPD. D'une part, toute entreprise ou entité qui traite des données à caractère personnel dans le cadre de l'activité de l'une de ses succursales établies dans l'UE, quel que soit le lieu où les données sont traitées[73]. D'autre part, le RGPD s'applique au traitement de données à caractère personnel de citoyens de l'UE, par une société établie en dehors de l'UE qui propose des biens ou des services dans l'Union – peu importe ici qu'un paiement soit exigé ou non pour ces biens et services - ou qui surveille et enregistre le comportement des citoyens européens, dans la mesure où ce comportement a lieu au sein de l'UE[74].

Pour déterminer si une entité offre des biens ou des services, les dispositions prévoient une évaluation au cas par cas[75]. Dans ce processus, il est déterminant d'évaluer si les responsables du traitement ou les sous-traitants ont l'intention de diriger leurs activités commerciales vers le marché européen[76]. En effet, le RGPD fonde son champ d'application territorial sur la

[71] Recital 26, RGPD.
[72] Article 2(c), RGPD.
[73] Article 3 (1), RGPD.
[74] Article 3 (2), RGPD.
[75] Recital 26, RGPD.
[76] O. KARADUMAN, *op. cit.*, p. 4.

destination de l'activité commerciale, en ce qu'il exige un lien entre l'action - en l'occurrence l'activité destinée au marché européen - et le territoire de l'UE[77].

Cette approche résout l'un des problèmes posés par les lois européennes antérieures en matière de protection des données, en donnant au RGPD la compétence nécessaire afin de couvrir le traitement des données des sujets de l'UE par un Etat tiers[78]. En ce sens, le champ d'application territorial du règlement est l'une des dispositions cruciales qui conduisent à la conformité mondiale, car il étend considérablement le champ d'application du RGPD à toutes les activités de traitement destinées à l'Union européenne.

CHAPITRE 2 : LE PRINCIPE DE PROTECTION ADEQUATE

L'applicabilité globale du RGPD peut être promue de manière unilatérale ou bilatérale. La portée matérielle et territoriale du RGPD permet son applicabilité internationale, en appliquant le droit de l'Union sur le territoire d'autres États souverains et en projetant la conception européenne de la protection de la vie privée de manière extraterritoriale.

Quand on en vient au transfert international de données, le champ d'application du RGPD doit être associé à un autre outil fondamental du règlement: le principe d'adéquation[79].

SECTION 1 : LES DECISIONS D'ADEQUATION

L'article 45, paragraphe 2, introduit ce principe dans le RGPD et énonce un ensemble de critères permettant d'évaluer le niveau de protection garanti par le régime juridique d'un pays tiers, afin de déterminer s'il est suffisant ou non pour permettre un échange de données de l'UE, en se basant sur une décision d'adéquation[80].

Pour contrôler le principe d'adéquation, les articles 45 et 46 du RGPD prévoient non seulement un seuil à utiliser lors de l'évaluation des transferts internationaux de données, mais

[77] P. DE HERT et M. CZERNIAWSKI, « Expanding the European data protection scope beyond territory: Article 3 of the General Data protection Regulation in its wider context », *International Data Privacy Law,* Vol. 6, No. 3, 2016, p. 1.
[78] *Ibid.*
[79] A. BENDIEK et M. RÖMER, *op. cit.*, p. 39.
[80] J. WAGNER, « The transfer of personal data to third countries under the GDPR : when does a recipient country provide an adequate level of protection ? », *International Data Privacy Law,* Vol 8, No 4, 2018, p. 5.

également une base légale permettant de bloquer tout échange de données européennes avec des pays qui ne respectent pas les normes européennes[81].

L'article 45 prévoit qu'un transfert de données vers un pays tiers peut avoir lieu lorsque la commission a décidé que le pays tiers assure un niveau de protection adéquat[82]. À titre d'exemple, la Commission européenne vient de rendre une décision d'adéquation avec le Japon[83], permettant un échange libre de données entre les deux zones économiques.

Plus important encore, les décisions d'adéquation constituent des instruments concrets permettant de renforcer davantage le phénomène de diffusion du modèle européen au niveau international. En effet, les décisions d'adéquation peuvent être négociées de manière bilatérale, sous la forme d'un contrat consensuel avec l'État destinataire et permettent à l'UE d'adapter et de renforcer le régime normatif de l'Etat tiers avec lequel elle traite, notamment en matière de protection de la vie privée. Lorsque le niveau de protection est finalement jugé adéquat, le pays tiers peut être inscrit sur « la liste blanche» via une décision d'adéquation du comité européen de la protection des données[84]. En fait, l'UE utilise le principe d'adéquation depuis la fin des années 70 pour créer des garanties pour les droits de ses citoyens[85] et, à présent, le RGPD lui confère une base juridique solide et même le renforce encore davantage[86].

Là où ce principe est particulièrement utile, c'est qu'il peut constituer un levier important dans les négociations internationales menées par l'Union. En effet, l'UE a la capacité non seulement de déterminer ce qui est adéquat, mais aussi de permettre à ses législateurs de bloquer tout transfert de données s'ils estiment que l'État tiers ne fournit pas de garanties suffisantes. En conséquence, la réglementation des transferts internationaux de données tend à s'appliquer catégoriquement de manière «noire ou blanche», ce qui peut entraîner une augmentation des oppositions entre le droit de l'UE et le droit de pays tiers[87].

---

[81] P. SCHWARTZ, *op. cit.*, p. 10.
[82] Article 45, RGPD.
[83] European Commission – Press release, (2019), *European commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows,* disponible sur http://europa.eu/rapid/press-release_IP-19-421_en.htm, , consulté le 2 Mai 2019.
[84] C. INGLEY et P. WELLS, *GDPR: Governance Implications for regimes outside the EU,* AUT University Press, Auckland, 2018, p. 107.
[85] P. SCHWARTZ, *op. cit.*, p. 10.
[86] *Ibid.*
[87] C. KUNER, « Extraterritoriality and regulation of international data transfers in EU data protection law », *International Data Privacy Law,* Vol. 5, No. 4, 2015, p. 2.

Sur la base de ce principe, l'UE peut également conclure des accords d'adéquation de bonne foi tout en exigeant un réexamen bilatéral a posteriori et par périodes régulières. À titre d'exemple, nous pouvons citer l'accord du « Privacy Shield »[88] – la dernière décision en matière d'adéquation conclue avec les Etats-Unis – qui est revue chaque année par la Commission européenne pour vérifier si les normes européennes sont suffisamment protégées et mises en œuvre tout en assurant une protection adéquate aux citoyens de l'UE[89].

SECTION 2 : LES SAUVEGARDES ADEQUATES

Dans le cas où la Commission n'a pas rendu de décision d'adéquation, l'article 46 dispose que l'échange de données n'est autorisé que si des «garanties adéquates» supplémentaires sont fournies sous la forme de «clauses types de protection des données» ou de «règles d'entreprise contraignantes»[90].

Les clauses types de protection des données peuvent être, soit des «clauses standards»[91], préalablement approuvées par la Commission, soit des clauses «ad hoc»[92] rédigées par les parties et devant être approuvées par l'autorité de protection des données locale[93].

Les règles d'entreprise contraignantes sont, comme leur nom l'indique, des règles juridiquement contraignantes adoptées par un groupe de sociétés qui créent des obligations envers les personnes physiques et qui se soumettent aux termes du RGPD si ces règles sont approuvées par une autorité de surveillance.

CHAPITRE 3 : MECANISMES D'EXECUTION

Si le RGPD harmonise le cadre de protection des données pour tous les États membres de l'UE, les autorités nationales – et indépendantes – de protection des données (APD) sont essentielles pour assurer sa mise en œuvre et garantir le respect de ses dispositions par le biais de mécanismes d'exécution[94].

---

[88] G29, « Opinion n°01/2016 on the EU-U.S. Privacy Shield draft adequacy decision», *WP238,* 13 avril 2016.
[89] European Commission – Press release, (2018)*, EU-US Privacy Shield: Second review shows improvements but a permanent Ombudsperson should be nominated by February 2019,* disponible sur http://europa.eu/rapid/press-release_IP-18-6818_en.htm , consulté le 2 Mai 2019.
[90] Article 46 (2 (b)), RGPD.
[91] Article 46 (2 (c)), RGPD.
[92] Article 46 (2 (d)), RGPD.
[93] Article 47, RGPD.
[94] A. BENDIEK et M. RÖMER, *op. cit.*, p. 39.

Les APD ont pour rôle central de traiter des plaintes, qu'elles soient individuelles ou introduites par des recours collectifs, ainsi que celui de surveiller le flux de données à caractère personnel et d'imposer des sanctions lorsque cela se révèle nécessaire.

SECTION 1 : LE PRINCIPE DU CHEF DE FILE

L'un des nouveaux principes du RGPD, appelé «principe du chef de file», introduit de nouveaux mécanismes de coopération qui désignent une autorité principale unique, chargée du traitement transfrontière effectué par un contrôleur ou un sous-traitant. Cette autorité principale de supervision est désignée au lieu de l'établissement principal du responsable du traitement ou du sous-traitant qui a effectué le traitement[95].

Le principe du guichet unique est un des éléments principaux participant à l'harmonisation globale du régime européen de protection des données. Dès l'origine, la Commission proposa ce principe afin d'assurer l'application cohérente et globale du Règlement, afin de réduire les frais administratifs pour les acteurs traitant de données personnelles, tels que les responsables de traitement et leurs sous-traitants qui exercent leurs activités économiques dans plusieurs Etats membres. De plus, ce principe permet de réduire la disparité du régime de protection des données en ce qu'il garantit aux entreprises la possibilité de ne devoir s'adresser qu'à un seul interlocuteur, plutôt qu'à 28 autorités nationales différentes[96].

Ce principe permet d'assurer de meilleurs moyens de recours non seulement aux entreprises mais également, et surtout, aux individus. En effet, le RGPD permet une amélioration des moyens de recours individuels quand on le compare à la Directive. Sous cette dernière, les APD étaient compétentes, en vertu de l'article 28(6), pour traiter de plaintes ou pour exercer leur pouvoir d'enquête dans les limites du territoire de leur Etat Membre. Toutefois, et sauf dans les cas où cette plainte concerne un responsable de traitement ou un sous traitant ayant son lieu d'établissement principal sur le territoire de cet État Membre, leurs pouvoirs d'exécution seraient en pratique limités à leur frontière nationale en ce que ce serait l'APD de l'Etat Membre sur lequel s'est déroulé le traitement en litige qui aurait pu poursuivre la plainte sur son propre territoire. Par conséquent, l'obligation d'appliquer la loi nationale d'un autre Etat membre sous la directive, couplée à l'impossibilité de poursuivre une enquête ou de prendre des sanctions dès qu'il n'y a pas de présence physique d'un responsable de traitement

[95] Article 56, RGPD.
[96] P. HUSTINX, *op. cit.*, p. 39.

ou d'un sous-traitant sur leur territoire rendait souvent les recours locaux des individus devant leur APD nationale quelque peu illusoires et certainement inefficaces[97].

Sous le Règlement, ce sont les articles 55, 56 et 60 qui permettent d'instaurer le mécanisme de l'autorité chef de file et qui permettent d'améliorer les moyens de recours individuels offerts aux citoyens. L'article 55 dispose que chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie sur le territoire de l'État Membre dont elle relève. L'article 56 stipule quant à lui qu'en cas de transfert de données transfrontalier, c'est l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant qui est compétente pour agir en tant qu'autorité de contrôle chef de file conformément à la procédure prévue par l'article 60.

Cela implique que les individus se voient octroyer le droit de déposer une plainte devant leur APD locale ou devant toute autre autorité afin d'obtenir réparation de leurs droits[98]. Le règlement garantit une exécution de ses dispositions par l'autorité chef de file avec, sous certaines conditions, l'éventuelle coopération de l'autorité locale lorsque c'est nécessaire. De plus, les citoyens ont toujours la possibilité de poursuivre une entreprise établie dans leur pays devant leur cour nationale pour une quelconque violation du règlement, en ce que le règlement est d'applicabilité directe.

Les mécanismes d'exécution du RGPD constituent certains des principaux facteurs qui poussent vers une convergence globale en matière de protection des données en ce que les entreprises préfèrent respecter les dispositions du Règlement à titre préventif plutôt que de risquer d'être passibles d'une sanction sous ces dispositions[99].

SECTION 2 : SANCTIONS ET AMENDES

En termes de sanctions, le RGPD innove en adoptant deux niveaux différents de sanctions, basés sur la fortune effective des individus ou des entreprises qu'elles visent[100]. Le but initial de ces nouveaux mécanismes de sanction étant de répondre aux préoccupations des individus face aux géants de l'information, en fournissant des mécanismes de sanctions qui soient efficaces, proportionnés et surtout dissuasifs[101] sous la forme d'amendes administratives. Pour

[97] *Ibid*., p. 40.
[98] *Ibid.*
[99] C. BARRETT, *op. cit.*, p. 5.
[100] M. RUSTAD et T. KOENIG, *op. cit.*, p. 371.
[101] *Ibid.,* p. 429.

ce faire, le RGPD stipule à ses articles 83 et 84 les critères qui doivent être pris en compte et les seuils que peuvent atteindre de telles sanctions. D'abord, l'article 83 reprends une liste de critères que l'autorité de contrôle chargée du dossier se doit de prendre en compte[102]. A titre d'exemple, on peut citer la nature de l'infraction, l'intention derrière la brèche, les mesures préventives mises en place ou encore la notification effective d'une telle brèche aux citoyens[103]. La prise en compte de ces critères sert à déterminer le montant de l'amende administrative qui sera imposée aux entreprises litigieuses. Le RGPD stipule que le montant maximal de l'amende ne peut excéder le montant pour l'infraction la plus grave, et distingue deux niveaux de seuils pour en déterminer le montant[104]. Le premier seuil dispose que les amendes administratives peuvent s'élever jusqu'à 10 000 000€ ou à 2% du chiffre d'affaire global de l'année précédant l'infraction. Le second seuil permet quant à lui d'imposer des sanctions pouvant monter jusqu'à 20 000 000€ ou à 4% du chiffre d'affaire global annuel de l'année précédant l'infraction, en fonction du montant le plus élevé.

SECTION 3 : ILLUSTRATION GOOGLE LLC VS CNIL

Récemment, l'APD française a utilisé pour la première fois les nouvelles armes fournies par le RGPD. Cette affaire est intéressante dans la mesure où elle illustre et met en pratique les nouvelles sanctions contenues dans le RGPD. Le 21 janvier, la Commission Nationale de l'Informatique et des Libertés (ci-après la CNIL) a infligé une amende de 57 millions d'euros à Google LLC sur le fondement du RGPD, pour violation des conditions de transparence, un manque d'information et une obtention illégale du consentement de ses utilisateurs quant à l'utilisation de publicités personnalisées et ciblées au sein des services Google[105]. Cette affaire est la plus récente à ce jour et montre les possibilités d'application du nouveau Règlement, ouvrant la voie à l'application future de ses articles 83 et 84.

D'un point de vue juridique, l'affaire met en lumière plusieurs principes énoncés dans le RGPD et pertinents pour son exécution. D'une part, cette affaire clarifie le principe du «principal établissement»; Google LLC affirmait que son principal établissement se trouvait

[102] Article 83,(2 (a-k)), RGPD.
[103] GDPR EU.org, *Fines and penalties,* disponible sur: https://www.gdpreu.org/compliance/fines-and-%20penalties/ consulté le 4 août 2019.
[104] Article 83 (3) et 83 (4), RGPD.
[105] Commission Nationale de l'Informatique et des Libertés, *Délibération de la formation restreinte n°SAN-2019-001 du 21 Janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.*, disponible sur : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1 , consulté le 25 Mai 2019.

en Irlande – via Google Ireland Limited -, ce qui aurait, selon les articles 56 et 60 du RGPD[106], désigné l'autorité irlandaise de la protection des données comme autorité de contrôle principale et compétente pour toutes les demandes d'indemnisation formulées contre Google en Europe.

Le RGPD prévoit que la qualification de l'établissement principal d'une entreprise doit être déterminée au moyen de critères objectifs[107]. En fait, il ressort du texte que les critères déterminants pour qualifier le principal établissement d'une entreprise en Europe sont caractérisés par le pouvoir décisionnel de cet établissement, concernant les moyens et les objectifs qui justifient les activités de traitement de cette entreprise[108]. La CNIL souligne que ces derniers doivent être apprécié *in concreto* et l'autorité française a rapidement démontré que Google Ireland Limited n'exerçait aucun contrôle ni aucun pouvoir de décision sur les activités de traitement de Google LLC et ne pouvait donc pas en être considérée comme le principal établissement. Comme Google Ireland Limited ne peut se prévaloir d'un pouvoir décisionnel, le principe du guichet unique n'est donc pas applicable et confirme la compétence de la CNIL en tant qu'autorité de surveillance en ce que l'autorité irlandaise ne disposait pas d'une compétence exclusive.

La CNIL a condamné Google pour deux violations du RGPD: premièrement, sur la base d'un manquement à la transparence et d'un manque d'informations suffisantes; deuxièmement, et après une analyse approfondie, au motif que les conditions de consentement des personnes étaient reçues de manière illégale, dans la mesure où elles n'étaient pas suffisamment claires, univoques et spécifiques[109].

Une violation de ces conditions de consentement, qui constitue un principe fondamental du traitement au sens du RGPD, permet à une autorité de contrôle d'imposer des amendes administratives allant jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel total de l'année précédente, en prenant en compte le chiffre qui se

[106] Article 56, Article 60, RGPD; Ces articles prévoient, d'une part, que l'autorité de contrôle du principal établissement du responsable du traitement est compétente pour superviser le traitement transfrontalier - également dénommé principe de guichet unique - et articule, d'autre part, la coopération entre l'autorité de surveillance principale et d'autres autorités de surveillance dans l'UE.
[107] Recital 36, RGPD.
[108] Article 4 (2), RGPD.
[109] Commission Nationale de l'Informatique et des Libertés, *op. cit.*, disponible sur : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1 , consulté le 25 Mai 2019.

trouve être le plus élevé[110]. La CNIL a tenu compte de la gravité de l'infraction pour déterminer le montant final de l'amende[111].

Une telle décision envoie un message clair aux entreprises du monde entier : il ne leur appartient pas de pouvoir choisir leur autorité de surveillance principale. Ce constat renforce d'avantage l'application uniforme du RGPD dans l'ensemble des Etats Membres et permet d'en assurer un peu mieux l'application globale à toute activité professionnelle qui se rapproche du marché européen. Avec cette affaire, la CNIL prouve et proclame que les autorités européennes de protection des données disposent à présent de dents acérées et qu'elles n'ont pas peur de s'en servir[112].

[110] Article 83 (5 (a)), RGPD.

[111] Article 83 (2 (a)), RGPD.

[112] A. O'DONOVAN, (2019), *CNIL vs Google : 10 lessons from the largest data protection fine ever issued,* disponible sur : https://www.passwordprotectedlaw.com/2019/01/cnil-vs-google-largest-fine/ , consulté le 30 avril 2019.

TITRE 3 : COMPARAISON ET INFLUENCE SUR D'AUTRES JURIDICTIONS

Le troisième titre traitera de certains des plus grands développements en matière de législation sur la confidentialité des données au niveau international et tentera d'évaluer le rôle que le RGPD a joué dans cette effervescence législative. Il est important de reconnaître le fait que de nombreux États ont déjà réglementé dans le domaine de la confidentialité des données, que ce soit dans une approche similaire à celle adoptée au niveau européen ou via des approches divergentes. Dans les années 90 – et pour donner une illustration chiffrée de ce phénomène d'expansion législative - environ 20 pays étaient dotés de lois sur la confidentialité des données; ils étaient plus de 100 en 2015[113]. Malgré l'effervescence croissante des réglementations en matière de confidentialité des données, l'Union européenne reste l'un des acteurs privilégiés dans le domaine et a toujours été un leader international en matière de confidentialité des données[114].

Au cours des dernières années et depuis l'adoption du RGPD, de nombreuses juridictions internationales ont adapté leurs propres lois afin d'adopter des normes et des dispositions plus semblables à celles du RGPD. Le Japon[115] et la Commission européenne ont récemment conclu un accord d'adéquation[116] réciproque de leurs législations respectives en matière de protection des données[117]. L'Inde est également en train d'adopter un projet de loi inspiré du RGPD, en ce que de plus en plus de parlementaires indiens préconisent l'adoption de normes européennes afin de garantir à l'Inde un accès au marché européen[118]. Des pays d'Amérique latine, tels que le Brésil[119], ont également élaboré des réglementations inspirées - voire

[113] E. DUROU, *Big Data, Mining a national resource,* 2015, disponible sur: https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/no-place-like-home/big-data.html# , consulté le 6 mai 2019.
[114] C. KUNER, « The European Union and the Search for an International Data Protection Framework », *op. cit.*, p. 60.
[115] Le Japon a récemment modifié sa loi sur la protection des informations personnelles, qui est entrée en vigueur le 30 mai 2017. L'UE la reconnaît comme un niveau de protection équivalent à celui du RGPD, créant ainsi la plus grande « safe-zone » au monde pour un libre-échange de données.
[116] European Commission – Press release, *European commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows.* , *op. cit.*
[117] D. SIMMONS, *5 countries with GDPR-like Data Privacy Laws,* 2019*,* disponible sur: *https://insights.comforte.com/5-countries-with-gdpr-like-data-privacy-laws*, consulté le 6 Mai 2019.
[118] En été 2018, l'Inde a adopté un nouveau projet de loi intitulé « Projet de loi sur la protection des données à caractère personnel » (ci-après PDPA, en anglais), qui contribue à l'émergence de nouveaux régime de protection des données dans le monde. Ce projet de loi a beaucoup en commun avec le RGPD et on promet déjà aux entreprises qui sont déjà conformes au RGPD auront peu ou pas d'efforts à fournir pour se conformer au PDPA.
[119] Le 18 août 2018, le Brésil a adopté sa loi générale sur la protection des données à caractère personnel (« Lei General de Proteçao de Dados Pessoais, ci-après LGPD). Ce règlement général brésilien sur la protection des

largement inspirées - du RGPD. En effet, le RGPD a déjà largement influencé les législations étrangères, en particulier dans les États où une réelle tradition de protection de la confidentialité des données n'existait pas ou, du moins, n'était pas souvent respectée[120]. Il semblerait que le RGPD soit en bonne voie pour réaliser son ambition de devenir le «standard doré» à travers le globe[121].

Nous avons choisi de porter notre analyse détaillée sur la Californie, le Japon et l'Inde pour multiples raisons. D'abord, parce que ces trois juridictions font parties des cinq plus grandes économies mondiales[122] et ont, par conséquent, un impact et un rôle crucial à jouer dans le domaine. Également, elles sont la preuve concrète d'une certaine influence européenne en ce que ces trois régimes avaient des approches très différentes du droit à la vie privée.

CHAPITRE 1 : LES ETATS-UNIS ET L'INFLUENCE EUROPEENNE EN CALIFORNIE

Pour l'Union européenne, la confidentialité des données est consacrée comme un droit fondamental et a été développée pour répondre à un problème interne, à savoir la volonté d'harmoniser les pratiques de traitement des données des États membres.

L'approche des États-Unis était singulièrement différente; il n'y a pas de droit équivalent ni de garantie sur la confidentialité des données dans la constitution, en ce que la pratique américaine libérale veut que les législateurs régissaient par le biais de lois sectorielles, leurs régimes juridiques étant dispersés entre les différents secteurs, selon une approche plus discrète et tentaculaire[123]. En outre, les données à caractère personnel sont considérées comme un atout économique pouvant être détenu par les entreprises, ce qui peut même inciter les consommateurs à se mettre d'accord sur la vente de leurs informations personnelles aux entreprises en échange de différents avantages ou services.

---

donnée reflète le RGPD dans ses principales dispositions, telles qu'une vaste application extraterritoriale, de lourdes sanctions et des bases légales de traitement déterminées, entre autres. Les entreprises ont jusqu'en 2020 pour se conformer à la LGPD.

[120] J. CLARK et J. HALPERT, « California's Consumer Privacy Act and the GDPR - where do they overlap », *Privacy and Data Protection,* 18 (7), 2018, p. 1.

[121] V. REDING., *A data protection compact for Europe.,* 2014, disponible sur: http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm , consulté le 27 Avril 2019.

[122] Journal du net, *Classement PIB: La liste des pays les plus riches du monde en 2019*, 16 Avril 2019, disponible sur: https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1209268-classement-pib/, consulté le 5 Août 2019.

[123] Paul Schwartz, *op. cit.*, p. 30.

SECTION 1 : LE « CALIFORNIAN CONSUMER PRIVACY ACT »

§1 : QU'EST CE QUE LE « CALIFORNIAN CONSUMER PRIVACY ACT » ?

Le « Californian Consumer Privacy Act »[124] (ci-après CCPA) a été adopté le 28 juin 2018. Dès son annonce, le monde entier commença à comparer ce projet de loi au RGPD[125] en ce qu'il s'agit de la première loi de ce type aux Etats-Unis. Le CCPA confère effectivement des droits individuels étendus aux consommateurs de l'Etat de Californie –et au-delà[126] -, afin de protéger leur vie privée.

Cette section tentera d'évaluer les principales raisons pour lesquelles cette loi, bien que rédigée à la hâte, est le candidat le plus direct pour une comparaison avec le RGPD, dans la mesure où elle transpose intentionnellement un grand nombre de ses dispositions[127].

S'il est déjà publié depuis le 28 juin 2018, le CCPA ne sera opérationnel qu'en janvier 2020. Similairement à ce qui s'est passé avec le RGPD entre 2016 et la date sacrée du 25 mai 2018, cette période de latence sera très probablement utilisée pour corriger certaines des erreurs de rédaction qui subsistent dans le texte[128]. Cette période de mise en œuvre permettra également aux entreprises de faire pression en faveur de certains amendements du texte[129], comme nous le verrons dans la dernière partie de cette section.

Néanmoins, cette loi est largement comparée au RGPD en ce que l'on affirme qu'elle aura une portée presque aussi large que le Règlement, garantira également la plupart des droits individuels et infligera des sanctions similaires en cas de non-respect de ses dispositions. Le CCPA dispose en effet d'une base solide pour offrir un régime axé sur le consommateur, qui peut être tout aussi strict que le RGPD, offrant des droits individuels spécifiques et ciblés dans un large éventail de domaines[130].

---

[124] Assembly Bill No. 375 : an act to add title 1.81.5 (commencing with section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy, *California Consumer Privacy Act,* June 28th, 2018.
[125] L. HAMILTON, C.-A. HELLEPUTE, S.TATA, O. YAROS, K.C. BURMAN, D. DE CICOO et E.M. WOOTEN., *Keeping it private : GDPR and developments in data privacy in 2019*, Mayer Brown, p. 2.
[126] BigID, *California Consumer Privacy Act vs GDPR : What you need to know,* 2019, disponible sur: https://bigid.com/wp-content/uploads/2018/07/California-Consumer-Privacy-Act-vs-GDPR-What-You-Need-To-Know.pdf , consulté le 27 Avril 2019.
[127] J. CLARK et J. HALPERT, *op. cit*., p. 1.
[128] *Ibid*.
[129] DuckduckGo, *24 Tech Companies Back CCPA Amendment to make it stronger : Privacy for All Act of 2019,* 2019, disponible sur*:* https://spreadprivacy.com/ccpa-privacy-for-all-act/ , consulté le 30 Avril 2019.
[130] J. CLARK et J. HALPERT, *op. cit.*, p. 4.

Pour bien saisir l'effet potentiel du CCPA à l'échelle mondiale, nous devons tout d'abord reconnaître l'importance du marché californien. Quand on regarde les chiffres, la Californie est actuellement l'État le plus peuplé des États-Unis - avec environ 39,5 millions d'habitants ; le CCPA représente donc la loi principale sur la protection des données de la cinquième économie mondiale, le marché californien ayant, selon le département américain du Commerce, dépassé le Royaume-Uni pour se placer juste derrière ceux des Etats-Unis, de la Chine, du Japon, et de l'Allemagne[131]. En outre, compte tenu en particulier de l'influence directe de la Silicon Valley dans le domaine de la protection des données - ou devrions-nous plutôt considérer l'impact qu'ont les lois traitant de la protection des données sur la Silicon Valley? -, il est clair que la Californie a déjà servi de modèle dans ce domaine de protection de la vie privée et parvient à le faire à nouveau avec l'adoption de ce projet de loi, en ce qu'il promeut le régime de protection de la vie privée le plus complet des États-Unis à ce jour[132].

De plus, le CCPA touchera, selon l'Association internationale des professionnels de la protection de la vie privée (IAPP), plus de 500 000 entreprises américaines[133]. Cela découle du fait que le nouveau projet de loi protégera non seulement tous les résidents de la Californie, mais élargira également son champ d'application à une grande partie des activités commerciales en Californie[134].

Gardant à l'esprit tous ces facteurs importants, nous pouvons mieux comprendre pourquoi le CCPA suscite actuellement le même type de brouhaha que celui connu lors de l'entrée en vigueur du RGPD. Cependant, il est important de se plonger dans les principales dispositions de ces deux textes afin de saisir exactement leur degré de similitude et d'expliquer leur effet futur sur les normes mondiales en matière de confidentialité des données.

---

[131] C. BARRETT, *op. cit.*, p. 5.
[132] *Ibid.*, p. 3.
[133] R. HEIMES et S. PFEIFLE, (2018) *New California Privacy Law to affect more than half a million US companies,* 2018, disponible sur: https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/, consulté le 5 Mai 2019.
[134] *Ibid.*

§2 : COMPARAISON CHOISIE AVEC LE RGPD

Le CCPA imite l'approche du RGPD dans un certain nombre de ses dispositions. Ce paragraphe fournira une approche comparative des éléments essentiels promus par les deux instruments. Le CCPA a en fait emprunté de nombreux principes fondamentaux du RGPD - parfois de manière timide, parfois de manière encore plus sévère pour les entreprises- en offrant une meilleure protection aux consommateurs en vertu de ses dispositions. Compte tenu de son champ d'application, des droits individuels accordés aux consommateurs sur leurs données à caractère personnel et des sanctions mises à disposition, nous examinerons l'influence européenne du RGPD sur le CCPA.

A. PORTEE MATERIELLE

La portée matérielle du CCPA est, tout comme le RGPD, volontairement large. Premièrement, la section 1798.140 (o) (1) du CCPA définit les «informations personnelles» comme suit: «les informations qui identifient, se rapportent à, décrivent, peuvent être associées à, ou peuvent être raisonnablement liées, directement ou indirectement, à un consommateur ou un ménage particulier[135] ». Cette définition des informations personnelles inclut délibérément les données anonymes, du moins dans la mesure où elles concernent ou peuvent être associées à un consommateur ou à un ménage particulier[136], et est par conséquent même plus large que celle du RGPD.

Deuxièmement, la notion de «traitement» des données, présente dans le RGPD, est remplacée par les définitions de «collecte» et de «vente» d'informations dans le CCPA[137]. En effet, la définition de «collection[138]» signifie «acheter, louer, collecter, obtenir, recevoir ou accéder à des informations personnelles relatives à un consommateur par quelque moyen que ce soit ; cela inclut la réception d'informations du consommateur, de manière active ou passive, ou en observant son comportement », ce qui est très similaire à la notion européenne du traitement[139], bien que plus restrictif puisque le RGPD inclut toute opération sur l'ensemble

[135] CAL. CIV. CODE § 1798.140.
[136] J. CLARK et J. HALPERT, *op. cit*., p. 2.
[137] CAL. CIV. CODE § 1798.140. (e).
[138] En anglais dans le texte.
[139] Article 4 (2), RGPD.

de données, telle que l'effacement, la modification ou la restriction de telles données et couvre bien plus que des opérations relatives à la simple collecte de donnée[140].

Une différence majeure entre les deux textes réside dans le fait que le RGPD inclut toutes les entreprises et organisations qui traitent des données en vertu de son article 2, tandis que le CCPA établit une distinction entre les entreprises à but non lucratif et les entreprises à but lucratif. En effet, la société californienne ne vise que les entreprises à but lucratif exerçant leurs activités dans l'État de Californie et s'applique à celles qui satisfont à l'un des seuils suivants: celles dont les revenus bruts annuels sont d'au moins 25 millions de dollars; celles qui achètent des informations personnelles sur plus de 50 000 consommateurs, ménages ou appareils; ou tirent 50% ou plus de leurs revenus annuels grâce à la vente des informations personnelles des consommateurs[141].

B. PORTEE TERRITORIALE

En ce qui concerne sa portée territoriale, le CCPA est similaire au RGPD en ce qu'il dispose d'une vaste portée et peut s'appliquer également aux entreprises situées en dehors des États-Unis. En effet, le fait qu'une entreprise n'ait pas d'établissement en Californie ne l'exempte pas de respecter le CCPA, à moins que l'activité commerciale de l'entreprise en ce qui concerne les données à caractère personnel du consommateur n'existe, dans son ensemble, que strictement à l'extérieur de la Californie[142]. En effet, le principal critère d'applicabilité du CCPA consiste à exercer une activité commerciale au sein même l'État de Californie. Le « California Franchise Tax Board » a clarifié la notion d'« exercer une activité commerciale en Californie»: elle consiste à «participer activement à toute transaction dans le but de réaliser un gain pécuniaire ou un profit financier[143]». L'effet extraterritorial du CCPA s'applique donc à toutes les entreprises qui reçoivent des données d'un résident californien lorsque ces résidents se trouvent dans l'État de Californie ou si ces informations sont traitées dans n'importe quelle partie de l'État[144]. L'établissement du responsable de traitement ou du sous-traitant en Californie n'est donc pas pertinent, et l'effet extraterritorial du CCPA s'étend bien au-delà du territoire californien.

---

[140] BigID, *California Consumer Privacy Act vs GDPR : What you need to know,* 2019, disponible sur: https://bigid.com/wp-content/uploads/2018/07/California-Consumer-Privacy-Act-vs-GDPR-What-You-Need-To-Know.pdf , consulté le 27 Avril 2019.
[141] CAL. CIV. CODE § 1798.140. (c).
[142] C. BARRETT, *op. cit.*, p. 3.
[143] Data Guidance, Future of Privacy Forum, *Comparing Privacy Laws: GDPR vs CCPA,* 2019, disponible sur: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf , consulté le 2 Mai 2019, p. 9.
[144] J. CLARK et J. HALPERT, *op. cit.*, p. 2.

C. DROITS INDIVIDUELS

En tant qu'instrument axé sur le consommateur, le CCPA prévoit de nombreux droits individuels. Les plus importants sont très semblables, bien que non-identiques, à ceux fournis par le RGPD[145]. Néanmoins, le CCPA vise également à redonner le pouvoir de décision sur leurs informations personnelles à tous ses consommateurs, en prévoyant des droits avec le même type d'objectifs que le règlement européen. Le droit à l'information, le droit à l'oubli, le droit d'accès à ses données personnelles et le droit de retirer son consentement ainsi que le droit d'opposition figurent tous dans le CCPA, avec quelques singularités qui témoignent des différences culturelles qui fondent les deux instruments[146].

Il est important de reconnaître que les deux textes ont été rédigés selon la même approche, le CCPA étant étroitement aligné sur le RGPD, dans la mesure où il reprend ses droits de transparence renforcés et des mécanismes individuels pour garantir la conservation sécurisée des données à caractère personnel.

Pour autant, les deux textes ne sont pas identiques. Une des différences fondamentales réside dans le droit d'opposition, qui a été adapté dans le CCPA en tant que droit de retrait, sous la forme d'un « opt-out ». Dans les deux instruments, le droit d'opposition confère aux particuliers la possibilité de demander la cessation du traitement et de la vente de leurs données personnelles. L'article 5 du RGPD autorise les personnes à retirer leur consentement préalablement au traitement; ce consentement doit être accordé en premier lieu de manière affirmative, transparente, et claire; cela nécessite, dans le RGPD, que les entreprises reçoivent le consentement des utilisateurs sous la forme d'un « opt-in »[147] qui se prouve par une indication non-ambiguë que les propriétaires des données fournissent afin de marquer leur accord au traitement de leur données personnelles. Les particuliers peuvent également exercer un droit général d'opposition au traitement de leurs données, que ce traitement ait lieu sur la base d'un intérêt légitime ou d'un intérêt public, ou à des fins de marketing direct. Lorsque le traitement est dû à des intérêts légitimes, les entreprises peuvent toujours tenter de surmonter cette objection s'ils parviennent à démontrer que le traitement est nécessaire pour des motifs légitimes impérieux, qui priment sur l'intérêt individuel du particulier[148]. Au contraire,

---

[145] C. BARRETT, *op. cit.*, p. 4.
[146] 451 Research Report Reprint, *The California Consumer Privacy Act : not just « America's GDPR »,* 2019, disponible sur: https://integris.io/wp-content/uploads/2019/03/451_Reprint_TheCaliforniaConsumerPrivacyAct.pdf, consulté le 2 Mai 2019, p. 4.
[147] Recital 32, GDPR.
[148] Article 21 (1), GDPR.

lorsque les données sont collectées à des fins de marketing direct, le droit d'opposition implique, lorsqu'il est exercé, que les données à caractère personnel ne peuvent plus être traitées à ces fins[149].

A l'article 1798.120 du CCPA, le droit de retrait se caractérise par le fait qu'il offre aux consommateurs la possibilité de refuser la vente de leurs données personnelles. Ce droit s'applique uniquement à la vente d'informations personnelles et non à d'autres formes de traitement. Là où le RGPD exige un consentement affirmatif et volontaire sous la forme d'un « opt-in », le CCPA demande uniquement aux entreprises de placer un lien indiquant «Ne pas vendre mes informations personnelles» sur leur page d'accueil, couplé à une obligation de notifier le consommateur lorsqu'une entreprise vend ses informations[150].

En résumé, si les deux instruments offrent un droit d'objection marqué par les mêmes objectifs, il n'est pour autant pas exactement identique sous les deux dispositions. Le RGPD offre la possibilité de s'opposer à tout type de traitement, mais les entreprises ont toujours la possibilité de passer outre une objection sous certaines conditions spécifiques et s'ils peuvent témoigner d'un intérêt légitime au traitement. De plus, le RGPD érige en principe fondamental le fait pour les entreprises d'obtenir le consentement des particuliers sous la forme d'un « opt-in »; le CCPA quant à lui n'offre la possibilité que de s'opposer à la vente de renseignements personnels sous la forme d'un opt-out, et ce droit de retrait est absolu en ce que les entreprises ne peuvent s'y opposer ou tenter de le contourner[151].

D. MECANISMES D'EXECUTION

En ce qui concerne les mécanismes d'exécution présents dans les deux instruments, le CCPA prévoit, tout comme le RGPD, des sanctions pécuniaires en cas de non-conformité. Néanmoins, le CCPA prévoit des sanctions civiles, ce qui signifie que l'amende est prononcée par un tribunal. En fonction de la violation, la peine peut aller jusqu'à 2500 USD pour chaque violation individuelle ou 7500 USD pour chaque violation intentionnelle. À titre de comparaison, et comme vu dans le Titre 2 de ce mémoire, le RGPD prévoit d'une part que la pénalité s'élève à 2% du chiffre d'affaires annuel global ou à 10 millions d'euros, selon le montant le plus élevé; ou d'autre part qu'elle s'élève jusqu'à 4% du chiffre d'affaires global

[149] Article 21 (3), GDPR.
[150] A. MARINI, A. KATEIFIDES, J. BATES, G. ZANFIR-FORTUNA, M. BAE, S. GRAY et G. SEN, *Comparing Privacy Laws : GDPR vs CCPA*, 2019, disponible sur: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf, consulté le 6 Mai 2019, p. 30.
[151] *Ibid.*

ou jusqu'à 20 millions d'euros, selon le montant le plus élevé, en fonction du type et de la gravité de l'infraction[152].

Le CCPA ne prévoit pas de montant maximum, ce qui implique que plusieurs pénalités peuvent être infligées pour chaque violation, à l'inverse du RGPD qui stipule que le montant maximal de l'amende sera équivalent à l'unique montant correspondant à l'infraction la plus grave[153]. Si, à première vue, le RGPD semblait avoir des outils plus tranchants en termes de sévérité de sanction, l'approche consécutive et non-plafonnée du CCPA pourrait bien constituer un concurrent tout aussi sérieux en matière de mécanismes d'exécution pour défendre la vie privée des consommateurs californiens[154].

Une autre différence est que toute violation de la CCPA est évaluée et intentée au civil par le procureur général de Californie. Le procureur général représente donc l'équivalent des autorités nationales de protection des données en Europe.

E. INFLUENCE ET EVOLUTION FUTURE

Grâce à sa conception différente du droit à la vie privée et à sa large applicabilité, le CCPA est en mesure de réduire quelque peu la différence culturelle entre les régimes européens et américains ; cet instrument est influencé par le RGPD et protège également la vie privée en tant que droit fondamental[155].

Un nouvel amendement au projet de loi a récemment été déposé le 22 février 2019 et remplacerait le titre du CCPA par le titre «Privacy for All 2019»[156]. Cet amendement vise à étendre les droits individuels du CCPA en incluant davantage de principes du RGPD, comme par exemple un droit de retrait valable pour tout type de traitement des données personnelles - pas seulement à la vente d'informations ; améliorer les voies de recours pour les consommateurs et créer un droit individuel d'action ou encore en introduisant une condition de consentement préalable, sous la forme d'un opt-in avant tout traitement[157]. Pour soutenir la

---

[152] Article 83 (2(a)),(5 (a))., RGPD.
[153] Article 83 (3), RGPD.
[154] 451 Research Report Reprint, *The California Consumer Privacy Act : not just « America's GDPR »,* 2019, disponible sur: https://integris.io/wp-content/uploads/2019/03/451_Reprint_TheCaliforniaConsumerPrivacyAct.pdf , consulté le 2 Mai 2019, p. 5.
[155] C. BARRETT, *op. cit.*, p. 6.
[156] California Legislature : Assembly Bill No. 1760 : *Privacy for All,* April 12th , 2019.
[157] H. TSUKAYAMA, *It's time for California to guarantee « Privacy for All »,* Electronic Frontier Foundation, 2019, disponible sur: https://www.eff.org/deeplinks/2019/02/its-time-california-guarantee-privacy-all, consulté le 1 Août 2019.

mise en œuvre de cet amendement, 23 grandes entreprises en technologie de la protection de la vie privée - avec DuckDuckGo[158], un méta moteur de recherche dont la politique est d'assurer le plus haut haut niveau de vie privée, en tant que leader - ont soutenu ce nouveau projet de loi en adressant une lettre ouverte à l'Assemblée de Californie. Un tel engouement pour l'évolution du texte du CCPA et le souhait qu'il soit encore plus semblable au RGPD montre bien l'influence de la norme européenne sur l'instrument californien et l'évolution future de ce projet de loi déterminera le taux de ressemblance entre les deux textes.

CHAPITRE 3 : LE JAPON

Le Japon constitue un exemple intéressant de l'influence européenne en matière de protection des données. Nous l'avons vu, le mécanisme de décision d'adéquation permet à l'Union européenne de négocier, souvent à la hausse, le respect de ses standards au niveau international. La première section mettra en valeur les implications et le processus de transformation que le Japon a entrepris pour finalement obtenir une reconnaissance mutuelle avec l'Union européenne. Ensuite, la deuxième section reprendra brièvement quel est l'état du texte Japonais et mettra en exergue les points sur lequel il s'est rapproché du RGPD. L'influence européenne se réalise donc ici en amont,

SECTION 1 : L'ACTE DE PROTECTION DES INFORMATIONS PERSONNELLES

L'Acte de Protection des Informations Personnelles (ci-après APIP) fut dès 2005 constitutif d'une sorte de révolution pour le Japon en ce qu'il constitue le premier texte général sur la protection des données personnelles au pays du soleil levant. Il est en effet le premier texte à couvrir la plupart des businesses Japonais et exige que les données personnelles soient traitées de façon sûre et sécurisée, et donne des droits individuels modernes aux citoyens tels que le droit d'accès, de suppression ou d'objection. Pour autant, l'Union ne se laissant pas facilement impressionner quand on touche aux données personnelles, refusait depuis lors de reconnaître le Japon comme un égal aux standards équivalent[159].

§1 DES AMENDEMENTS AU TEXTE ET L'INFLUENCE EUROPEENNE

[158] DuckDuckGo est un méta-moteur de recherche dont la politique est d'offrir le plus haut niveau de vie privée possible lors de l'expérience en ligne de ses utilisateurs et de ne stocker aucune de leurs données personnelles.
[159] G. GERENCSER, « Japan 's long road for adequacy under the GDPR », *International Association of Privacy Professionals*, 2018, disponible sur : https://iapp.org/news/a/japans-long-road-for-adequacy-under-the-gdpr/ , consulté le 30 juillet 2019.

En septembre 2015, suite à une série de brèches qui ont conduit à des fuites de nombreux profils de citoyens japonais, le texte fut réformé et de nombreux amendements vinrent moderniser ses dispositions[160]. Ces amendements ont surtout eu comme but de faciliter l'usage des données personnelles pour les citoyens japonais tout en renforçant les règles de protection de la vie privée pesant sur les entreprises du secteur privé[161]. Il est en effet important de souligner que l'APIP ne s'applique pas au secteur public[162]. Par ailleurs, le texte révisé est entré en vigueur en le 30 Mai 2017, soit un an avant l'entrée en vigueur du RGPD.

La première question qui nous vient à l'esprit dans le cadre de ce travail est d'évaluer quelle fut l'influence européenne dans cette révision du texte japonais. On peut en effet se poser la question en ce que les premières discussions officielles concernant une éventuelle décision d'adéquation émanant de la Commission européenne furent entreprises moins d'un an après la révision de l'APIP en 2016[163]. On pressent que le Japon a déjà entrepris ces révisions dans l'optique de se rapprocher des standards européens, portés par la directive à l'époque et poursuivis par le RGPD qui était alors en préparation. On souligne ici que cet effort de modernisation était nécessaire afin de ne fut-ce qu'espérer une décision favorable de la part de la Commission[164].

§2 : CHAMP D'APPLICATION DE LA PROTECTION DES DONNEES

A. PORTEE MATERIELLE : DEFINITION DES « INFORMATIONS PERSONNELLES »

Le nouvel APIP présente différentes définitions en rapport avec les données personnelles. Une première observation utile et terminologique est la suivante : le terme « donnée personnelles » que nous connaissons dans le RGPD et dans la plupart des autres législations similaires et actuelles a été remplacé par le terme « informations personnelles » dans

[160] A. COOS, « Data Protection in Japan : All you need to know about APPI », *Endpoint Protector,* 1er Février 2019, disponible sur : https://www.endpointprotector.com/blog/data-protection-in-japan-appi/ , consulté le 31 juillet 2019.
[161] The Japan Times, Amended *privacy protection law,* 1er Juin 2017, disponible sur : https://www.japantimes.co.jp/opinion/2017/06/01/editorials/amended-privacy-protection-law/#.XT63SpMzY_U , consulté le 31 juillet 2019.

[162] G. GREENLEAF, « Japan : EU adequacy discounted », *155 Privacy & Business International Report 8,* 2018, p. 1.
[163] G. GREENLEAF, « Questioning 'adequacy' (Pt 1) – Japan », *150 Privacy Laws & Business International Report,* 1, 6-11, 2017, p. 4.
[164] G. GREENLEAF, « Japan : Towards international standards – except for 'big data' », *Privacy Laws & Business International Reports, Issue 135,* Juin 2015, p. 1.

l'APIP[165]. Ces information personnelles sont définies comme celles qui peuvent, soit identifier des individus spécifiques ou soit, qui contiennent des « codes individuels d'identification »[166]. Ces codes sont un concept propre au régime japonais et se réfèrent à tout caractère, nombre, symbole dans lequel une caractéristique physique permettrait d'identifier un individu. On remarque également que l'APIP inclut aussi explicitement les données qui, une fois qu'elles sont rassemblées entre elles, permettent d'identifier un individu.

Ensuite, le terme « données personnelles » est utilisé dans l'APIP pour désigner les informations personnelles qui constituent une base de données d'informations personnelles[167].

Enfin, les amendements de l'APIP ont ajouté une définition de « données sensibles » qui est similaire à celle contenue dans le RGPD. Une telle définition n'était pas prévue dans l'ancien texte[168]. Celles-ci comprennent des informations sur l'origine, le clan, le statut social, le dossier médical, le dossier criminel, ou tout autre facteur qui pourrait créer une discrimination sociale[169].

B. PORTEE TERRITORIALE

La nouvelle portée territoriale de l'APIP est similaire à celle du RGPD en ce qu'elle s'applique à toutes les entreprises qui reçoivent des données de citoyens Japonais, même si elles ne sont pas établies au Japon. Le texte s'applique en effet si les données sont obtenues dans le cadre d'une activité commerciale dirigée vers des individus qui résident au Japon[170]. L'acte peut donc connaître de toute entreprise ou de tout responsable de traitement qui vient à traiter les données de citoyens japonais dans le cadre d'une activité économique dirigée vers le Japon et ses consommateurs[171].

§3 : OBLIGATIONS DES RESPONSABLES DE TRAITEMENT ET DROITS INDIVIDUELS

[165] Article 2(1), APIP.
[166] Article 2(2), APIP.
[167] *Ibid.*
[168] H. HAYASHI, « Japan : Data Protection 2019 », *The ICLG to : Data Protection Laws and Regulations,* 3 Juillet 2019, disponible sur https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan , consulté le 1er Août 2019.
[169] *Ibid.*
[170] Article 75, APIP.
[171] Y. AIHARA et H. NORIKO, « Data Privacy Protection of personal Information versus Usage of Big Data : Introduction of the recent amendment to the Act on the Protection of Personal Information (Japan) », *Defense Counsel Journal, vol. 84.,no. 4,* Octobre 2017, p. 13.

Premièrement, on peut citer les grands principes contenus dans l'APIP qui régulent les bases légales du traitement des données personnelles d'une part, et les obligations pesant sur les responsables de traitement d'autre part. L'obligation la plus importante est centrée sur l'obtention préalable du consentement du sujet. En ce qui concerne les bases légales d'un traitement légitime, l'APIP a une approche différente que le RGPD mais promeut *in fine* le même genre de protection. En effet, le texte prend une approche prohibitive qui s'agrémente d'une série d'exceptions[172]. Ces exceptions comprennent notamment le traitement sous l'autorité publique, le traitement nécessaire à la sauvegarde d'un intérêt supérieur ou à la sauvegarde d'un état de santé lorsqu'il est difficile d'obtenir le consentement du propriétaire des données. De plus, tout traitement se doit d'être transparent[173], limité selon son objectif[174], et les données se doivent d'être supprimées lorsque leur détention par le responsable de traitement n'est plus nécessaire aux objectifs caractérisant le traitement[175]. Pour autant, l'APIP va moins loin que le RGPD en ce qu'il n'existe pas d'obligation de proportionnalité de traitement ni de minimisation des données[176].

L'APIP octroie également des droits individuels aux consommateurs, bien que ceux-ci ne soient pas aussi étendus que sous le régime européen. Toutefois, nous verrons que lors de la décision d'adéquation, des règles supplémentaires ont été négociées par l'Union afin de lui assurer un niveau de protection adéquat[177]. Concernant les droits individuels garantis sous l'APIP, on peut citer le droit d'accès[178], de suspension et de correction des informations[179] en possession du responsable de traitement[180]. Pour autant, le droit à l'oubli n'est pas expressément repris dans le texte. Toutefois, la Commission de protection des informations personnelles (ci-après CPP) est actuellement en train de prévoir la possibilité d'inclure ce droit via la première révision du nouveau texte, qui aura lieu pour la première fois en 2020[181]. Ce mécanisme de révision sera ensuite exercé régulièrement, et ce tous les trois ans[182]. Les

[172] Article 17, APIP.
[173] Article 18, APIP.
[174] Article 15 et 16, APIP.
[175] Article 19, APIP.
[176] Article 5(c), RGPD.
[177] Supplementary Rules under the Act on the protection of personal information for the handling of Personal Data Transferred from the Eu based on an Adequacy Decision, Annex 1, disponible sur https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf, (consulté le 29 juillet 2019).
[178] Article 26, APIP.
[179] Article 29, APIP.
[180] A. COOS, *op. cit*.
[181] H. HAYASHI, *op. cit*.
[182] *Ibid.*

responsables de traitement se doivent d'obtenir le consentement des individus avant de procéder à tout traitement et doivent, s'il en est fait la demande par ces derniers, révéler dans quel but un tel traitement est effectué[183].

§4 : DES MECANISMES D'EXECUTIONS LIMITES :

Avec les amendements de 2017, le Japon a fait un grand pas en avant en matière de protection des données en ce qu'il s'est enfin muni d'une autorité de protection des données indépendante et centrale[184] . Ce faisant, le Japon s'est rapproché du rôle moderne attendu des autorités de protection des données. La CPP endosse donc la fonction de planifier et d'adopter les différentes législations en la matière, supervise et contrôle le flux des informations personnelles sur le territoire Japonais, d'une part, et vers leurs partenaires commerciaux d'autre part, et agit comme l'acteur unique pour connaître des plaintes concernant l'usage des données personnelles par tous les acteurs privés qui tombe sous le champ d'application de l'acte quand ils conduisent une activité économique vers le marché japonais[185]. Un élément intéressant en ce qui concerne la CPP est sa capacité à nommer des entités qui seront également aptes à connaître des plaintes concernant le traitement par les responsables de traitement[186]. En 2018, près de 43 entités de ce type avaient été désignée par la CPP, renforçant de la sorte l'effectivité du nouveau texte. Leur rôle principal est de connaître des requêtes des responsables de traitements et de les conseiller sur les pratiques à adopter afin de rester dans les limites des dispositions sur la protection des données[187].

En termes de sanctions, et comparées aux sanctions contenues dans le RGPD à l'article 84, le texte de l'APIP est fondamentalement différent. D'abord, en ce que le texte ne permet pas à l'autorité de protection des données de prendre des sanctions civiles et administratives, mais uniquement criminelles[188]. Ensuite, parce que le montant de celles-ci est beaucoup plus réduit. Le montant maximal prévu dans le texte est en effet inférieur à une dizaine de milliers d'euros[189], ce qui contraste largement avec les juridictions européennes, californiennes ou encore indiennes qui ont toutes adopté des sanctions aussi élevées que dissuasives. On

[183] *Ibid.*
[184] A. CARSON, « Israel, Japan, Canada talk keeping up with the GDPR », *International Association of Privacy Professionals,* disponible sur: https://iapp.org/news/a/israel-japan-and-canada-talk-keeping-up-with-the-gdpr-2/ , consulté le 1er Août 2019.
[185] *Ibid.*
[186] Article 47, APIP.
[187] *Ibid.*
[188] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », 154 Privacy Laws & Business International Report ; *UNSW Law Research Paper No. 18-53*, 2018, p. 9.
[189] *Ibid.*, p. 10.

rappelle ici qu'avec cette décision d'adéquation, de nombreux acteurs européens auront accès aux données des citoyens japonais et ce contraste sème le doute sur une défense effective des droits des citoyens par la CPP. En effet, les armes à sa disposition pour ce faire semblent nettement moins tranchantes que celles de ses homologues étrangers.

SECTION 2. LA DECISION D'ADEQUATION

Sous les dispositions du RGPD, une décision d'adéquation représente, comme nous l'avons vu dans le Titre 2, un des outils qui permettent d'assurer un flux de données sécurisé envers les Etats tiers. L'intérêt de la décision d'adéquation avec le Japon est multiple. D'abord, il permet de voir comment, dans cette ère numérique où l'utilisation des données dans une économie digitale est croissante, l'Europe parvient à négocier à la hausse ses partenariats et à imposer de la sorte ses standards supérieurs sur la scène internationale. Ensuite, cette décision étant la première à être délivrée sous le RGPD, elle occupe un rôle clé en ce qu'elle pose les bases de ce que signifie une protection "essentiellement équivalente" au régime européen.

En 2015, la Cour de Justice de l'Union européenne a rendu un arrêt de principe avec l'affaire *Schrems*[190], dans laquelle elle a établit différent critères qui doivent être pris en compte lors de l'examen d'un régime juridique en vue d'une décision d'adéquation. Parmi ceux-ci, la cour a dégagé la nécessité d'examiner le niveau de protection d'un régime en prenant en compte les sauvegardes mises en places pour l'ingérence de l'autorité publique dans les données personnelles de ses citoyens[191]. Également, la possibilité pour les individus de défendre leur droits par des recours accessibles et efficaces ou encore l'indépendance des autorités de protection des données sont des facteurs déterminants[192]. Au regard de ces éclaircissements, nous allons tenter d'approcher la décision d'adéquation avec le Japon et évaluer si elle répond correctement à ces critères et, si ce n'est pas le cas, quelles implications cela peut avoir sur les futurs applications d'un tel mécanisme.

§1 OBJECTIFS DE LA DECISION D'ADEQUATION

Le 23 janvier 2019, l'Europe a finalement adopté sa décision d'adéquation concernant le Japon. De façon quelque peu inusuelle, le Japon a également adopté, dans un effort de réciprocité, une décision similaire en ce que cette décision d'adéquation est caractérisée par

[190] Arrêt Maximillian Schrems, Data Protection Commissioner, C-362/14, EU:C:2015:650.
[191] Y. MIDAZVETSKAYA, « What are the pros and cons of the Adequacy decision on Japan », *Centre for IT & IP Law Blog,* disponible sur: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/ , consulté le 3 août.
[192] *Ibid.*

un effort mutuel de reconnaissance des régimes des deux pays, là où auparavant, l'Europe adoptait ce type de décisions de façon unilatérale[193]. Ces mots de la commissaire européenne à la Justice, aux consommateurs et à l'égalité des genres[194] témoignent bien des objectifs européens qui résident derrière le processus d'une décision d'adéquation: « Cette décision d'adéquation crée la plus grande zone de libre échange au monde. Les données des européens vont bénéficier de hauts standards de protection lors de leur transfert au Japon. Nos entreprises bénéficieront également d'un accès privilégié à un marché de 127 millions de consommateurs. Car investir dans la vie privée est très utile ; cet arrangement servira d'exemple pour nos futures collaborations dans le secteur et participera à la promotion d'un standard global de protection de la vie privée.[195] »

Premièrement, et comme cela a toujours été l'objectif européen depuis l'entrée en vigueur de la directive en 1995[196], l'Europe veut assurer un niveau de standard de protection élevé à ses citoyens lors de tout transfert international de leurs données. Pour cela, et après plusieurs années de négociation entre les deux parties, l'Europe et le Japon sont tombés d'accord et ont adopté un nombre de règles complémentaires[197] qui devront être introduites dans le régime japonais afin d'en améliorer les dispositions légales et réduire l'écart du niveau de protection offert par les deux textes[198]. Ces règles comprennent, entre autres, des garanties quant à la protection des données sensibles, des détails précis quant au transfert de donnés européennes vers une tierce partie ou encore sur les droits individuels offerts aux citoyens. Dans la même idée, les règles assurent que l'autorité de protection des données Japonaise, la Commission de protection des Informations personnelles, soit compétente pour exécuter ces règles et offre les recours nécessaires pour en assurer le respect, en ce que toutes ces règles supplémentaires seront bien évidemment obligatoire pour les entreprises japonaises[199].

---

[193] G. GREENLEAF, « Questioning 'adequacy' (Pt 1) – Japan », *op. cit.*, p. 1.

[194] Vera Jourovà, occupe encore ce post actuellement.

[195] Communiqué de presse de la Commission Européenne, « La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde », Bruxelles, 23 Janvier 2019, disponible sur: https://europa.eu/rapid/press-release_IP-19-421_fr.htm, consulté le 2 Août 2019.

[196] M. RUSTAD et T. KOENIG, *op. cit.*, p. 371.

[197] Supplementary Rules under the Act on the protection of personal information for the handling of Personal Data Transferred from the Eu based on an Adequacy Decision, Annex 1, disponible sur https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf, (consulté le 29 juillet 2019).

[198] R. HEALEY, « How the Japan APPI compares to the GDPR, are you compliant ? », *GDPR 24/7 Privacy by Design*, 13 Mars 2019, disponible sur : https://relentlessdataprivacy.com/japanappi-v-eu-gdpr/, consulté le 29 juillet 2019.

[199] *Ibid.*

Deuxièmement, cette décision d'adéquation crée la plus grande zone de libre échange de données au monde et permet à l'Europe d'avoir un accès privilégié à un marché de consommateurs de près de 127 millions de personnes. On s'en souvient, la Directive, et le RGPD à sa suite, ont également avancé comme but intrinsèque celui d'assurer une zone de libre échange à travers l'Union européenne et de parfaire le transfert de données entre les Etats membres[200]. De plus, cette harmonisation du transfert de données s'est vue agrémentée d'une volonté européenne d'étendre cet échange de données à tous les acteurs préparés à fournir une protection équivalente aux standards européens. On remarque que dans cette campagne pour assurer une vaste zone sécurisée de libre échange, les décisions d'adéquation constituent le fer de lance de la conquête européenne. C'est en effet via cet instrument que l'Europe a toujours étendu son pouvoir sur le marché numérique et a pu étendre ses standards aux quatre coins du globe[201].

Le Japon est donc désormais le premier pays à bénéficier d'une telle décision depuis l'entrée en vigueur du RGPD[202] et accède de la sorte à la « liste blanche » établie au fil des ans par l'Union européenne[203]. Dans un effort de réciprocité - ou simplement dans une optique de se montrer le plus équivalent possible - le japon a également adopté ce système de « liste blanche » et cette reconnaissance mutuelle placera l'Union comme la première juridiction sur la liste japonaise[204].

Troisièmement, on voit bien là une autre trace de cette volonté très présente au sein de l'Union de constituer un standard global et international qui soit, au minimum, équivalent aux standards européens[205]. Pour cela, il semble que jusqu'ici l'Union ait toujours réussi à négocier afin que le pays tiers améliore son propre régime et qu'il adopte une approche européanisée, plutôt qu'un phénomène inverse. Pour le Japon, cela s'est concrétisé par les amendements de 2017 qui furent largement inspirés par le RGPD – voire contraints, vu l'objectif final de s'y plier.

---

[200] P. HUSTINX, *op. cit.*, p. 9.

[201] B-A. SAFARI, « Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection », *47 Seton Hall L. Rev. 809*, 2017, p. 810.

[202] G. GERENCSER, « Japan 's long road for adequacy under the GDPR », *op. cit.*

[203] K. TAKASE, « GDPR matchup : Japan's Act on the protection of personal information », *International Association of Privacy Professionals*, 2017, disponible sur : https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/, consulté le 30 juillet 2019.

[204] *Ibid*.

[205] Communiqué de presse de la Commission Européenne, « Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World, Questions and Answers » 10 janvier 2017, disponible sur : http://europa.eu/rapid/press-release_MEMO-17-15_en.htm , consulté le 30 juillet 2019.

§2: EVALUATION DE LA DECISION D'ADEQUATION

La décision d'adéquation sera, tout comme nombre des autres décisions d'adéquation rendues par la Commission européenne[206], soumise à une évaluation et à un contrôle régulier afin de d'assurer qu'elle soit toujours valable en l'état. Pour autant, la décision d'adéquation réciproque entre l'Europe et le Japon joue un rôle tout particulier en ce qu'elle constitue la première de ce genre rendue depuis l'entrée en vigueur du RGPD et constitue dès lors la première pierre à l'édifice de ce que représente un régime essentiellement équivalent au RGPD[207]. Dans un exercice d'évaluation d'une décision d'adéquation, il importe surtout de voir comment un régime tiers s'est aligné sur les principes européens et les a justement intégré à son propre régime. Une réplicabilité stricte n'est donc pas nécessaire, mais c'est là qu'il nous faut établir dans quelle mesure les standards européens ont été effectivement transposés dans la juridiction tierce[208].

A. DES ELEMENTS QUI FAVORISENT LES STANDARDS EUROPEENS CONTENUS DANS LE RGPD

D'abord, et depuis 2017, le Japon a également reconnu le droit à la vie privée - comprenant la protection des données personnelles - comme étant un droit fondamental et constitutionnel[209]. De plus, et afin de répondre plus avant aux critères établis dans l'affaire *Schrems,* l'établissement d'une autorité de protection des données indépendante fut une avancée majeure. Par ailleurs, la CPP a reçu la compétence d'édicter des règles juridiques qui dépassent la portée du cadre juridique domestique japonais[210]. En effet, une des étapes cruciales dans la balance de la décision d'adéquation fut l'adoption par la CPP de règles supplémentaires qui ont érigé un régime sur mesure en faveur de l'Union[211]. En effet, ces règles supplémentaires ne sont d'application qu'en ce qui concerne les données obtenues à l'origine de l'Union européenne[212]. Elles concernent principalement les données sensibles, le stockage des données personnelles, la délimitation des objectifs de traitements, le traitement

[206] Voyez par exemple les révisions annuelles du Privacy Shield, qui donnent lieu chaque année à des communiqués de presse et à des rapports de la part de la Commission Européenne, disponible sur : https://europa.eu/rapid/press-release_IP-18-6818_en.htm, consulté le 30 Juillet 2019.
[207] G. GREENLEAF, « Japan : EU adequacy discounted », *op. cit.*, p. 1.
[208] Y. MIDAZVETSKAYA, « What are the pros and cons of the Adequacy decision on Japa n», *Centre for IT & IP Law Blog,* disponible sur: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/ , consulté le 3 août.
[209] *Ibid.*
[210] *Ibid.*
[211] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 5.
[212] *Ibid.*

de donnés anonyme et leur processus de transformation, ainsi que l'impossibilité de transférer les données personnelles avec des Etats tiers à l'Europe et au Japon[213]. Ces règles supplémentaires seront obligatoires pour toutes les entreprises japonaises qui importent des données européennes et seront sous la compétence de la CPP[214].

Ensuite, la version amendée de l'APIP reprend nombres des droits individuels portés par le RGPD, comme nous avons pu l'évoquer dans la Section 1 de ce titre. Toutefois, et nous le rappelons, une des faiblesses du texte réside dans l'applicabilité strictement privée du texte. Pour y pallier, les règles supplémentaires reprennent que tout accès par le gouvernement aux données personnelles pour des raisons de poursuites judiciaires ou de sécurité nationale sera limité et proportionnel à son objectif de traitement. Par ailleurs, cet accès sera également sujet à des recours individuels devant la CPP qui en assurera le contrôle[215]. Ce mécanisme de recours pour les plaintes des utilisateurs européens leurs permettra d'assurer une défense similaire à celle qui leur est offerte sous le RGPD[216].

B. CRITIQUES ET INTERPRETATION

Par ailleurs, il nous faut souligner que l'existence de ces règles supplémentaires - uniquement applicables aux données européennes - prouve bien l'influence du modèle européen. Pour autant, on peut s'interroger quant au sens réel d'une décision d'adéquation quand on remarque que la protection offerte aux citoyens européens est, dans les faits, supérieure à celle offerte aux citoyens japonais par leurs propres dispositions nationales[217].

En effet, ces règles spéciales ne bénéficient qu'aux sujets dont les données sont perçues depuis l'Europe, et ne concernent pas celles qui sont perçues au Japon ou en provenance de toute autre juridiction[218]. De plus, ces règles plus strictes ne s'appliquent qu'au traitement exercé dans le cadre de la décision d'adéquation, selon l'article 45 du RGPD, et non pas, par exemple, à celles en provenance du territoire européen dans le cadre de garanties adéquates

---

[213] Y. MIDAZVETSKAYA, *op. cit.*

[214] T. DAVIES, « European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows », *PrivSec Report,* 24 Janvier 2019, disponible sur: https://gdpr.report/news/2019/01/24/european-commission-adopts-adequacy-decision-on-japan-creating-the-worlds-largest-area-of-safe-data-flows/, consulté le 3 Août 2019.

[215] *Ibid.*

[216] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 7.

[217] Y. MIDAZVETSKAYA, *op. cit.*

[218] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.,* p. 7.

contenues à l'article 46 du RGPD, telles que les clauses contractuelles standard ou encore les règles d'entreprise contraignantes. On ne peut donc qu'encourager une modification du texte de l'APIP en tant que tel, afin de palier à la différence de standard de protection qui existe entre un transfert sur base des règles supplémentaires et celui basé sur les dispositions de l'APIP. Il ne faudrait pas transformer les garanties adéquates de l'Article 46 de RGPD en un outil inutile parce qu'elles ne permettrait pas une protection jugée satisfaisante, au contraire de ce qui est admis pour le transfert de données sous la décision d'adéquation et de l'article 45 du RGPD à strictement parler[219].

De plus, une analyse approfondie des mécanismes d'exécution actuellement présents dans l'APIP pose question quant à la nécessité de fournir des recours effectifs aux individus pour défendre leurs droits et celle de doter l'autorité de protection des données des compétences nécessaires pour en assurer le respect[220] . En effet, l'historique actuel de la CPP à ce propos ne permet pas de vérifier que ce soit bien le cas en l'espèce[221]. Certes, le texte reprend des mécanismes de sanction mais ces derniers sont particulièrement peu élevés en comparaison de ceux présents dans le RGPD. Surtout, on ne relève actuellement aucune affaire permettant de démontrer l'utilisation concrète de ces mécanismes ou de toute forme de compensation qu'ils aient déjà pu offrir aux individus[222].

Enfin, les transferts ultérieurs de données[223] constituent également une zone d'ombre de cette décision d'adéquation. En effet, il existe une crainte que des transferts ultérieurs soient possibles avec les données européennes via une sorte de "porte de secours"[224] qui permettrait un transfert de données vers des pays tiers ne bénéficiant pas du régime d'adéquation avec l'Union[225]. En fait, et en tant que membre de la Coopération Économique Asie-Pacifique (ci-après CEAP)[226], le Japon reconnaît les règles transfrontières de vie privée de la CEAP comme constituant un système de protection adéquat. En ce qu'elles sont reconnues comme telles, ces règles permettent un transfert de données du Japon vers les membres de la CEAP selon les

[219] *Ibid.*
[220] Article 45 (2)(b), RGPD.
[221] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 9.
[222] G. GREENLEAF, « Japan : EU adequacy discounted », *op. cit.*, p. 1.
[223] Article 44, RGPD.
[224] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.* , p. 9.
[225] Y. MIDAZVETSKAYA, *op. cit*.
[226] La CEAP compte actuellement 21 membres: Australie; Brunei Darussalam; Canada; Chili; Chine; Hong Kong; Indonésie; Japon; Corée du Sud; Malaisie; Mexique; Nouvelle-Zélande; Nouvelle Guinée Papouasie; Pérou; Philippines; Russie; Singapour; Taipei chinois; Thaïlande; Etats-Unis d'Amérique et Vietnam.

dispositions de l'APIP[227]. Toutefois, il est clair que les standards fournis par les règles de la CEAP pour un tel transfert sont largement inférieurs à ceux requis sous l'Article 44 du RGPD[228]. La solution qui fut trouvée par la CPP pour empêcher un transfert ultérieur des données européennes et acceptée par la Commission est d'inclure dans les règles supplémentaires à la décision que le consentement des sujets européens est requis avant tout transfert ultérieur[229]. On peut toutefois critiquer cette solution centrée sur le consentement à différents égards: d'abord, tant l'information accompagnant ce consentement risque d'être trop vague pour être significative; ensuite, parce que lorsque qu'un citoyen consent à un tel transfert, on voit mal comment il serait encore en mesure d'exercer des recours efficaces et accessibles dans la juridiction tierce; enfin, une telle solution consacre le consentement individuel comme étant une base légale propice à un transfert international de données[230]. Cela n'est pas prévu dans le texte du RGPD aux articles 44 à 50 sauf à titre exceptionnel et lorsqu'il n'existe justement pas de décision d'adéquation ou de garantie appropriées[231]. Or dans le cas d'espèce, l'exception deviendrait la règle[232].

Au vu de ces différentes considérations, on se rend compte que malgré une hausse du niveau de protection des standards japonais, qui s'accompagne d'un régime juridique presque sur mesure pour intégrer les dispositions européennes, le Japon a encore et toujours certaines lacunes en matière de protection des données. Cela précise les contours de ce que représente également un régime adéquat selon le RGPD et nous verrons comment cela se développe sur le long terme lors des premières évaluations de cette nouvelle zone internationale d'échange de données. Jusqu'ici toutefois, il semble que le Japon s'en soit tiré avec un régime tout au plus suffisant pour passer à travers les mailles de la Commission, et nous verrons quelles implications cela peut avoir lors des futures décisions.

[227] Article 24, APIP.
[228] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 11.
[229] *Ibid.*
[230] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 12.
[231] Article 49(1), RGPD
[232] G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », *op. cit.*, p. 12.

CHAPITRE 4 : L'INDE: EN QUETE D'UNE APPROCHE INDEPENDANTE ?

SECTION 1 : LE DROIT A LA VIE PRIVEE COMME DROIT FONDAMENTAL

Le régime juridique de l'Inde fut longtemps basé sur deux instruments en matière de protection des données ; le Information Technology Act[233], qui date de 2000, d'une part, et le Information Technology Rules[234], de 2011, d'autre part. Ce dernier régule les règles de protection des données.

Il semble que l'entrée en vigueur de ces deux actes était déjà marquée par une volonté du gouvernement Indien de se garantir l'accès au marché européen, en ce qu'une économie comme celle de l'Inde ne voulait pas risquer de perdre ses activités économiques transfrontalières avec l'Europe. L'Union avait en effet souligné que l'Inde ne remplissait pas les standards européens en matière de protection des données, portés à l'époque par la Directive 95/46/EC[235]. Pour cette raison, l'Union européenne a, à deux reprises déjà, refusé de prendre une décision d'adéquation envers le régime indien car l'Inde ne remplissait pas les critères de protection équivalente et n'était pas en mesure de fournir des sauvegardes adéquates sous son ancien régime[236] .

Du fait des implications du procès *Puttaswamy vs Union of India*[237], dans lequel la Cour suprême indienne a reconnu le droit à la vie privée comme un droit fondamental, l'Inde s'est retrouvée confrontée à un régime qui présentait des incohérences et des lacunes incompatibles avec les standards européens. En outre, l'ancien régime ne permettait pas de répondre aux attentes de la Cour suprême quant à la fonctionnalité que devrait remplir un régime moderne de protection de la vie privée, à savoir que «le droit de la vie privée est destiné à protéger les informations privées des individus et leur permettre d'exercer leur droit fondamental à la vie

[233] Information Technology Act, 2000, disponible sur https://indiankanoon.org/doc/1965344/ , consulté le 20 Juillet 2019.
[234] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, disponible sur http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf , consulté le 20 Juillet 2019.
[235] S-K. PRASAD, "(Draft) Paper on Information Technology Act, 2000 and the Data Protection Rules", C*entre for Communication Governance at National Law University,* Delhi, 30 Décembre 2017, p. 4.
[236] G. GREENLEAF,, « India's « Fourth Way » : GDPR-lite with chinese characteristics ? », *UNSW Law Research Paper No. 18-83.*, 20 septembre 2018, p. 7.
[237] Puttaswamy v. Union of India, Writ petition (civil) no 494 of 2012, (2017)6MLJ26 .

privée »[238] . On remarque ici un parallèle entre cette interprétation de la Cour suprême indienne et l'approche européenne de la protection de la vie privée.

Le ministère de l'électronique et des technologies de l'information (ci-après MEITY) nomma donc un comité d'experts, mené par le juge suprême Srikrishna (ci-après le Comité Srikrishna[239]), afin qu'il crée un nouveau régime de protection des données censé garantir à l'Inde un cadre suffisant pour assumer sa place de leader économique sur le marché des technologies de communication, tout en respectant l'interprétation nouvelle du droit fondamental à la vie privée dégagée lors de l'affaire *Puttaswamy*. Le Comité Srikrishna rédigea le nouveau texte de loi, appelé le « Personal Data protection Bill 2018 » (ci-après PDPB) et également un rapport explicatif du nouveau projet de loi, appelé « Rapport pour une économie numérique libre et juste, garantissant la protection de la vie privée et l'autonomisation des Indiens »[240](ci-après le Rapport Srikrishna ou encore le Rapport). Si le texte de loi doit toujours être officiellement validé par le MEITY avant son entrée en vigueur, on peut déjà connaître de ses éléments principaux et tirer certaines conclusions quant au nouveau régime de protection qu'il introduira d'ici 2020[241].

SECTION 2 : ANALYSE DU PERSONAL DATA PROTECTION BILL 2018

§1 : TERMINOLOGIE ET DEFINITION DES DONNEES PERSONNELLES

Dans ce nouveau projet de loi, l'Inde emprunte beaucoup de la terminologie proposée par le RGPD : le texte reprend notamment la notion de « sous-traitant » mais remplace la notion de « responsable de traitement » par la notion de « fiduciaire de données »[242]. Également, le texte remplace la notion de « personne concernée » par le traitement - « data subject » en anglais - par le terme de « data principal »[243]. Fondamentalement, cette différence terminologique renvoie aux mêmes concepts, en ce que les fiduciaires sont responsables de leurs propres

[238] Paragraph 185, J. Chandrachud's opinion, Puttaswamy v. Union of India, Writ petition (civil) no 494 of 2012, 6MLJ267 , 2017.
[239] S. AGARWAL, « Justice BN Srikrishna to head Committee for data protection framework », *The Economic Times*, 1er Août 2017, disppnible sur: https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection- framework/articleshow/59866006.cms , consulté le 25 Juillet 2019.
[240] Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the the Chairmanship of Justice B.N.
Srikrishna, 2018 ; Une copie du Rapport est disponible sur le site du MEITY :
https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report- comp.pdf
[241] L. DETERMANN et C. GUPTA, « Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law », *UC Berkeley Public Law Research Paper*,18 septembre 2018, p. 7.
[242] Personal Data Protection Act, Section 11.
[243] *Ibid.,* p. 11.

activités de traitement ainsi que de celles de leurs sous-traitant, tout comme les responsables de traitement dans le RGPD[244].

Ensuite, et si le droit à la confidentialité des données fait partie intégrante du droit fondamental à la vie privée[245], il est important d'analyser la définition des données personnelles protégées par le nouveau texte. Le Comité Srikrishna a exprimé que pour assurer une protection adéquate aux citoyens, le texte se doit de protéger toutes les données personnelles qui sont en rapport avec tout type d'information qui identifie ou est capable d'identifier une personne[246]. En adoptant une définition aussi large, le PDPB se base sur la définition des données personnelles du RGPD[247] et s'engage à respecter le standard européen qui veut que tout type d'informations capable d'identifier une personne soit comprise dans le régime de protection, couvrant de la sorte non seulement les informations d'identification traditionnelles telles que le nom, l'adresse ou le numéro de téléphone d'un individu mais également toutes les informations agrégées ou anonymes qui, lorsqu'elles sont groupées et combinées permettent également d'identifier un individu[248].

§2 CHAMP D'APPLICATION DU PERSONAL DATA PROTECTION BILL 2018

Concernant le champ d'application de ce nouveau texte, le comité a pris en compte deux éléments qui permettent d'en préciser l'étendue et les influences.

Tout d'abord, il y eu lieu de répondre à la question d'adopter une loi sectorielle plutôt qu'une loi générale, dite loi omnibus. Dans les anciens instruments indiens, le législateur indien avait choisi d'opérer par le biais d'une combinaison d'une loi générale[249] s'appliquant à plusieurs secteurs déterminés, et de lois spécifiques à chaque industrie, où les règles se recoupent par secteur d'activité, comme par exemple dans le secteur financier[250]. Cette division constituant l'un des facteurs d'inefficacité de l'ancien régime, le Comité Srikrishna a encouragé l'adoption d'une loi générale, applicable horizontalement et sans égards à la spécificité des

[244] Article 4, RGPD.
[245] Puttaswamy v. Union of India, Writ petition (civil) no 494 of 2012, (2017)6MLJ267.
[246] Rule 2(1) (i) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[247] Article 4(1), RGPD.
[248] S-K. PRASAD, « Back to the Basics: Framing a New Data Protection Law for India », *op. cit.*, p. 3.
[249] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, disponible sur: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf , consulté le 26 Juillet 2019.
[250] S-K. PRASAD, « Back to the Basics: Framing a New Data Protection Law for India », *op. cit.*, p. 3.

différents secteurs. Ce faisant, l'Inde semble s'aligner encore davantage sur l'approche européenne.

Ensuite, le Personal Data protection Bill s'appliquera tant aux organes publics qu'aux entreprises privées. En effet, le juge suprême A. P. Shah a encouragé le Comité Srikrishna à adopter une loi qui s'appliquerait tant au secteur public que privé, citant encore une fois l'approche européenne[251]. Cette caractéristique est singulière en ce que de façon traditionnelle, les droits fondamentaux ne créent de recours pour les citoyens indiens que lorsqu'ils agissent contre l'Etat ou une autorité publique. Lors du procès *Puttaswamy*, la Cour suprême a en effet reconnu qu'une violation des informations personnelles pouvait résulter aussi bien d'une exaction de l'Etat que d'acteurs privés. Elle a par conséquent demandé aux législateurs de garantir un droit d'action aux individus même envers des acteurs privés, afin d'offrir un régime de protection complet composé de droits individuels ouverts à tous, et contre tous[252].

Toutefois, il est important de souligner que le PDPB contient de larges exceptions quant à la discrétion laissée à l'Etat pour ordonner le traitement de données personnelles en marge du régime de protection. En effet, les sections 42 à 45 du PDPB contiennent des exceptions pour le traitement de données autorisé par ou en accord avec la loi, pour le traitement qui touche à la mise en application de la loi ou encore pour celui effectué dans le cadre de poursuites judiciaires[253].

§3 L'INCORPORATION DE STANDARDS EUROPEENS ET INTERNATIONAUX

Nous l'avons vu, la deuxième et la troisième génération de standards européens, respectivement représentés par la Directive et le Règlement, ont été, du moins pour ceux promus par la Directive, largement incorporé dans des juridictions étrangères[254]. Le Comité Srikrishna a, pour la construction du PDPB, choisi de mettre en avant 9 standards formant les grands principes du droit européen de la vie privée.

---

[251] Report of the Group of Experts on Privacy, 2018, disponible sur: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf , consulté le 30 Juillet 2019.

[252] Paragraph 5 of Conclusions, J. Chandrachud's opinion, Puttaswamy v. Union of India, Writ petition (civil) no 494 of 2012,6MLJ26, 2017.

[253] G. GREENLEAF,, « India's « Fourth Way » : GDPR-lite with chinese characteristics ? », *op. cit.*, p. 12.

[254] G. GREENLEAF, « European' Data Privacy Standards Implemented in Laws Outside Europe », *149 Privacy Laws & Business International Report 21-23; UNSW Law Research Paper No. 2.*, 3 Septembre 2017, p. 4.

Premièrement, le principe de notification, qui veut que chaque responsable de traitement communique, de façon claire et concise, ses pratiques de traitement aux individus avant de pratiquer un quelconque traitement sur leurs données personnelles[255].

Deuxièmement, le principe de libre choix et de consentement, selon lequel un responsable de traitement se doit de donner le choix aux individus de transmettre leurs données personnelles, sous la forme d'un opt-in ou d'un opt-out ; le responsable ne peut légalement procéder aux traitement ou à la communication de ces données à une tierce partie qu'après avoir reçu le consentement de l'individu, sauf dans les cas où le traitement est exécuté par une agence publique spécialement autorisée par la loi[256]. Selon le Rapport, ce principe du consentement est lié au droit de retrait des individus, qui peuvent retirer leur consentement à tout moment. Toutefois, il existe des cas exceptionnels où l'obtention préalable du consentement de l'individu n'est pas requise lorsque le service exécuté par le responsable de traitement n'est pas conciliable avec l'obtention préalable du consentement[257].

Troisièmement, le principe de limitation de traitement[258] : bien connu en Europe sous le RGPD, ce principe implique qu'un responsable de traitement ne peut collecter des données personnelles que dans la mesure où c'est strictement nécessaire pour les objectifs dudit traitement.

Quatrièmement, le principe de limitation de la finalité[259] selon lequel un responsable de traitement n'est en droit de collecter des données personnelles que dans les limites de la notification préalable faite à l'individu quant au dit traitement, de façon adéquate et cohérente. Ce principe constitue le cadre dans lequel un responsable de traitement peut utiliser les données personnelles récoltées.

Cinquièmement, le principe d'accès et de rectification[260] qui stipule que les individus ont le droit d'avoir accès aux informations personnelles qui leur sont propres et qui sont détenues par un responsable de traitement, et d'en demander la correction, la mise à jour ou la suppression si elles se trouvent être erronées. Ce droit s'accompagne du devoir pour le

[255] Government of India, Planning Commission, *Report on the group of experts on Privacy,* 2012, p. 22.
[256] *Ibid.*
[257] *Ibid.*
[258] *Ibid.,* p. 23.
[259] *Ibid.*, p. 24.
[260] *Ibid.,* p. 25.

responsable de traitement de révéler toutes les informations individuelles qu'il détient à l'égard de celui qui en fait la demande et celui d'en délivrer une copie.

Sixièmement, le principe de non-divulgation des informations[261] dispose que le responsable de traitement ne peut divulguer des informations personnelles qu'après en avoir notifié l'individu et après obtention de son consentement à cette divulgation.

Septièmement, le principe de sécurité[262] implique que les responsables de traitement sont dans l'obligation de sécuriser par des sauvegardes adéquates les informations personnelles qu'ils ont en leur possession envers tout accès non-autorisé ou envers leur destruction, leur usage, leur traitement, leur stockage, leur modification, leur divulgation ou tout autre risque prévisible.

Huitièmement, le principe de transparence[263] – d'ouverture dans le texte – dispose que le responsable du traitement se doit de prendre toutes les mesures nécessaires pour mettre en œuvre les pratiques, procédures, politiques et autres systèmes de manière proportionnée par rapport à l'ampleur, à la portée et à la sensibilité des données qu'ils collectent, afin de garantir le respect des principes de protection de la vie privée. Ces informations doivent être délivrées aux individus sous une forme intelligible, en utilisant un langage clair et simple, et accessible à tous.

Neuvièmement, le principe de responsabilité[264] veut que le responsable de traitement soit responsable du respect de toutes les mesures mises en place afin de respecter les principes de protection de la vie privée des individus.

SECTION 3 : CRITIQUE DU PDPB ET RAISONNEMENT SUR UNE POTENTIELLE DECISION D'ADEQUATION DE LA COMMISSION EUROPEENNE

Malgré l'incorporation des ces neuf principes, il est utile de tenter d'évaluer l'issue d'une potentielle décision d'adéquation de la Commission européenne au regard du PDBP en l'état. De plus, au regard de l'interprétation faite lors de l'examen du régime Japonais, on peut tenter d'isoler certains éléments qui pourraient représenter un obstacle à une interprétation favorable de la Commission.

[261] *Ibid.*
[262] *Ibid.,* p. 26.
[263] *Ibid.*
[264] *Ibid.,* p 27.

La dernière demande de décision d'adéquation date de 2013 et l'Inde a, depuis, élaboré le PDPB. L'obtention d'une telle décision représente encore et toujours l'un des objectifs de la modernisation du régime indien. Si l'on tente de prévoir l'issue probable d'une décision d'adéquation à l'heure actuelle, on remarque des faiblesses qui devraient être rectifiées par le Gouvernement et le comité Srikrishna, en ce qu'elles représentent encore des lacunes quant aux standards supérieurs mis en avant par le RGPD et risquent d'en compromettre l'issue. En effet, ces faiblesses concernent certains motifs de la légalité de traitement, le pouvoir discrétionnaire accordé au gouvernement, l'indépendance fictive de l'autorité indienne de protection des données (ci-après AIPD), la localisation des données, ainsi que certains droits individuels qui ont été omis lors de la rédaction du texte. Nous allons dès lors procéder à une critique constructive du PDPB afin de mettre en exergue certains points qu'il serait bon que le Comité Srikrishna améliore d'ici son entrée en vigueur.

§1: MOTIFS POUR LA LEGALITE DE TRAITEMENT

En l'état, le PDPB reconnaît le consentement au traitement des données personnelles comme étant l'élément central, nécessaire et préalable à tout traitement légal, tout comme le RGPD en son article 6. De plus, il reconnaît également nombre de bases légales à un traitement non-consensuel, pour lequel le consentement du propriétaire des données n'est pas requis. En effet, les sections 13-21 disposent de différents motifs, également repris dans le RGPD, tels que : le traitement pour une mission d'intérêt publique ; le traitement dans le cadre d'une obligation légale ou judiciaire ; le traitement dans le cadre d'un contrat de travail.

Toutefois, le PDPB intègre une base supplémentaire en sa section 17, à savoir le traitement pour un « objectif raisonnable ». Dans son Rapport, le Comité Srikrishna explicite ce que veut dire cette notion et dispose que : « L'objectif raisonnable est une base résiduelle pour le traitement qui n'est pas couvert par les autres bases légales telles que le consentement, l'obligation légale, l'urgence, ou la fonction publique mais qui sert malgré tout l'intérêt général. L'appréciation de cette disposition sera limitée aux objectifs reconnus comme valides par l'AIPD pour guider les responsables de traitement »[265].

Cette base légale garantit à l'AIPD un vaste pouvoir d'appréciation en ce que c'est cet organe qui déterminera ce qui peut être « utile à la société ». Certes, le texte présente certains facteurs à prendre en compte, mais ne reprend pas expressément de limites à ce pouvoir

[265] Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the Chairmanship of Justice B.N. Srikrishna, 2018, p. 180.

d'appréciation. On pourrait donc encourager le Comité Srikrishna à définir ce que représente effectivement un objectif raisonnable, et d'y intégrer des contre-mesures similaires à celles présentes à l'article 6 du RGPD qui seraient spécifiques et déterminées quant à chaque objectif poursuivi par le traitement et la collecte de données. A titre d'exemple concret, on pourrait citer la nécessité de prendre en compte les intérêts légitimes du propriétaire des données à ce que ses données personnelles ne subissent pas de traitement, et ce afin de procéder à une balance d'intérêts malgré l'existence d'un objectif raisonnable[266].

§2: LE POUVOIR DISCRETIONNAIRE DU GOUVERNEMENT EN MATIERE DE TRAITEMENT POUR LA SECURITE DE L'ETAT

Un autre problème à prendre en considération se trouve dans les larges exceptions dont bénéficie le gouvernement lorsqu'il veut procéder à un traitement dans l'intérêt de la sécurité de l'Etat ou dans le cadre d'infractions criminelles – bien que la section 43 (1) stipule « dans l'intérêt de la poursuite de tout crime ou toute autre infraction à la loi », ce qui peut même inclure des éléments non criminalisés[267].

Premièrement, c'est sous le titre IX du PDPB, intitulé « Exceptions », que le bât blesse. En effet, la sous-section 2 de la Section 42, et la sous-section 2 de la section 43 stipulent que tout traitement prenant forme sous l'autorité d'une loi et dans un objectif de sécurité de l'Etat ou de poursuites judiciaires ne se verra pas appliquer, à peu de chose près, les huit premiers chapitres du projet de loi. Si le texte tente de conditionner ces exceptions à des garanties et aux critères de nécessité, de proportionnalité et de légalité de traitement – ce dernier n'étant présent qu'implicitement en ce qu'on requiert que le traitement ait lieu sous l'autorité d'une loi[268] - on ne peut que souligner que le texte ne les définit en aucune façon et que, en rapport avec les larges exceptions qu'ils permettent, ces garanties sont dangereusement vagues[269].

Deuxièmement, de telles exceptions posent problème en ce qu'elles octroient un vaste pouvoir discrétionnaire à l'Etat pour interférer dans la vie privée de ses citoyens, sans leur donner les garanties procédurales nécessaires pour pouvoir contrôler si les critères de nécessité, proportionnalité et légalité sont bel et bien remplis en l'espèce[270]. De plus, la charge

[266] G. GREENLEAF, « GDPR-lite and requiring strengthening – submission on the Draft Personal Data Protection Bill to the ministry of electronics and information technology », *University of New South Wales Research Series,* 2018, p. 3.
[267] *Ibid.*
[268] Section 42 (1), PDPB.
[269] G. GREENLEAF, « GDPR-lite and requiring strengthening – submission on the Draft Personal Data Protection Bill to the ministry of electronics and information technology », *op. cit.*, p. 3.
[270] *Ibid*. p. 4.

de la preuve repose sur les propriétaires de données, ce qui complique encore la possibilité pour les citoyens d'éviter une ingérence de l'Etat.

§3: L'INDEPENDANCE FICTIVE DE L'AUTORITE INDIENNE DE PROTECTION DES DONNEES

Une troisième critique que l'on peut adresser au PDPB touche à l'Autorité Indienne de protection des données et met en cause le pouvoir discrétionnaire de l'Etat quant au traitement des données de ses propres citoyens. On remarque, suite à une analyse des pouvoirs et des compétences accordées à l'AIPD, que cette dernière ne bénéficie en fait que d'une indépendance factice. Pourtant, on peut lire dans le Rapport Srikrishna que « Le PDPB va mettre en place une autorité de protection des données qui sera un organe réglementaire indépendant, responsable de la mise en application et de l'exécution de la loi »[271]. De plus, le Rapport continue et explique que l'AIPD est chargé notamment des pouvoirs de poursuite judiciaire, du pouvoir de prendre des sanctions et que c'est sa cour d'arbitrage qui sera chargée de traiter de toutes les plaintes entre les individus et les responsables de traitements[272]. Toutefois, on ne peut qu'émettre des réserves quant à la réelle indépendance de l'AIPD.

D'une part, en effet, en ce que les sections 98 et suivantes disposent que le gouvernement est compétent pour émettre des directives dans « certaines circonstances ». Plus concrètement, cela implique que l'AIPD sera tenue par des directives écrites prisent par le gouvernement central lorsque celui-ci estime que cela défend un intérêt de l'Etat. Enfin, la section 98(4) stipule explicitement que, malgré une maigre possibilité pour l'AIPD d'exprimer son avis sur les directives du gouvernement, il appartiendra à ce dernier - et à ce dernier seulement - de trancher si une question touche aux intérêts de l'état. Cela prouve que ces décisions gouvernementales ne seront pas soumises à une révision judiciaire ou administrative, et participe davantage à la mise à mal de l'indépendance réelle de l'AIPD[273].

D'autre part, on remarque que la composition de l'AIPD sera déterminée par le gouvernement – ou du moins en partie - en ce que le Directeur du comité de l'AIPD sera nommé par le gouvernement central et ce pour une période de 5 ans[274]. De plus, la cour d'arbitrage sera composée d'officiers d'arbitrage qui seront choisis et nommés par le gouvernement central,

[271] Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the the Chairmanship of Justice B.N., p. 176.
[272] Section 68, PDPB.
[273] G. GREENLEAF, « India's « Fourth Way » : GDPR-lite with chinese characteristics ? », *op. cit.*, p. 11.
[274] Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the the Chairmanship of Justice B.N., p. 152.

qui pourra également en déterminer le nombre[275]. Plus particulièrement, le gouvernement aura, toujours sous le couvert assez vague « d'assurer une ségrégation opérationnelle, indépendante, et neutre »,[276] le pouvoir de déterminer la juridiction des Officiers d'arbitrage, la procédure selon laquelle ils peuvent conduire un arbitrage selon le texte, ou « tout autre exigence, selon les besoins du gouvernement »[277].

On ne peut donc que conclure à une zone obscure quant à cette prétendue indépendance de l'AIPD, là où la plupart des régimes internationaux, avec l'Union européenne en tête, prescrivent une indépendance absolue de leurs Autorité de protection des données[278]. Certes, le texte reprend bien le terme d' « indépendance », mais, lorsque l'on constate son utilisation vague et la forte implication du gouvernement, tant dans la composition de l'AIPD que dans ses compétences exécutives, on ne peut qu'émettre de sérieux doutes quant à la véracité de cette indépendance en l'espèce.

§4: L'OBLIGATION DE LOCALISATION DES DONNEES SUR LE TERRITOIRE INDIEN

Une quatrième critique que l'on peut apporter touche au transfert international de données personnelles. En effet, la section 40 du PDPB présente des restrictions au transfert international de données. Cette section indique que les entreprises ont l'obligation de stocker sur le territoire Indien toutes les données personnelles qui tombent dans le large champ d'application du texte[279]. Si le RGPD, on l'a vu, contient également des restrictions au transfert international de données[280], cette obligation rappelle plutôt le modèle chinois qui a intégré des obligations de localisations similaires dans son propre instrument de cyber-sécurité[281]. Il est bon de souligner que ni le modèle Européen, ni le modèle Californien n'ont opté pour des conditions de localisations sur leur territoire[282] et que, lorsque l'Allemagne a tenté d'en ébaucher sur son propre territoire, elles avaient été jugées contraire au droit européen[283]. Il semble donc qu'avec cette obligation générale de localisation des données,

[275] *Ibid*., p. 158.
[276] Section 68(2), PDPB.
[277] *Ibid.*
[278] G. GREENLEAF, « GDPR-lite and requiring strengthening – submission on the Draft Personal Data Protection Bill to the ministry of electronics and information technology », *op. cit.*, p. 7.
[279] Section 41, PDPB : « Tout responsable de traitement devra assurer le stockage, sur un serveur ou dans un centre de données localisés en Inde, d'au moins une copie effective des données personnelles auxquelles l'Acte s'applique ».
[280] Articles 44 et suivants, RGPD.
[281] L. DETERMANN et C. GUPTA, *op. cit*., p. 24.
[282] *Ibid*.
[283] *Ibid*., p. 25.

l'Inde s'écarte quelque peu du modèle européen et s'aventure là où l'Europe a récemment refusé de conduire son propre régime.

De plus, l'arrêt *Puttaswamy v. Union of India* avait établi que pour respecter le droit à la vie privée des citoyens, toutes mesures qui vont à l'encontre de l'autonomie et de la maîtrise des citoyens sur leurs données se doivent d'être justes, raisonnables, légitimes et proportionnées. Le Rapport Srikrishna explique cette nouvelle obligation de localisation qui pèse sur les entreprises par une volonté de diminuer les risques de brèches lors des transferts de données internationaux.

Si on ne peut que saluer ce principe, on voit mal comment l'Etat indien pourrait justifier que d'autres mesures, telles que la soumission des transferts internationaux à un test d'adéquation ou encore à des obligations contractuelles pour les entreprises, n'aurait pas fourni une approche plus proportionnée qu'une obligation générale et obligatoire de localiser les données[284].

De plus, cette explication est discutable quand on tente de faire le bilan entre, d'une part, la protection effective qu'une mesure de ce type permet et, d'autre part, la possibilité pour l'Etat Indien d'augmenter son ingérence et son accès aux données personnelles. Effectivement, on ne voit pas dans le texte de sauvegardes adéquates qui permettraient de contrer les risques d'une surveillance accrue de l'état, que ce soit en termes de procédure ou de recours offerts au citoyens[285]. En effet, les sections 13[286] et 19[287] du PDPB permettent à l'Etat de traiter les données des individus pour certaines « fonctions de l'Etat ».

Enfin, et comme dit plus haut, les sections 42 et 43 permettent des exceptions pour toutes les actions prisent dans l'intérêt de l'Etat ou pour des poursuites judiciaires. Ces deux éléments renforcent donc les risques d'excès de la part de l'Etat en ce qui concerne la surveillance de masse des citoyens[288]. En conséquence, nous ne sommes pas certains que le fait d'exiger la localisation des données personnelles en Inde permettra donc de renforcer la protection des

[284]R. BAILEY et S. PARSHEERA, « Data Localisation in India: Questioning the Means and Ends », NIPFP *Working Paper No. 24*2, 2018, p. 6.
[285] *Ibid.* , p. 21.
[286] Concerne les données personnelles dites « non-sensibles » qui peuvent être traitées pour toute fonction de l'État autorisée par la loi. Autant dire que cette mesure est très vaste.
[287] Concerne les données sensibles, qui peuvent être traitées pour une fonction de l'Etat quand cela s'avère être nécessaire. Ces données sensibles incluent : les mots de passes, les informations financières, les informations de soin de santé, l'orientation sexuelle, les données biométriques, religieuses ou politiques tel qu'indiqué par la section 3(35) du PDPB.
[288] R. BAILEY et S. PARSHEERA, *op. cit.* p. 21.

données personnelles et d'en diminuer le risque de brèche, en ce qu'il est fort probable que de telles brèches proviennent à l'avenir d'un excès de pouvoir du gouvernement.

§5: L'OMISSION VOLONTAIRE DE CERTAINS DROITS INDIVIDUELS

Cette dernière critique permet de mettre en exergue un autre aspect du PDPB. Si le Comité Srikrishna a pris le RGPD en modèle, il a toutefois choisi de ne pas intégrer l'entièreté de ses principes[289].

Le texte indien reprend le principe de « protection des données dès la conception », encourageant ainsi les entreprises à adapter leur structures internes pour se conformer par avance aux nouvelles dispositions du PDPB. Le texte de loi est pourtant lacunaire en ce qu'il ne reprend pas un principe sous-jacent au premier, à savoir le principe de « protection des données par défaut». Ce dernier consacre le droit pour les citoyens d'avoir accès par défaut à la plus grande protection possible de leur vie privée. Si l'on reprend le RGPD[290], on remarque qu'il incombe au responsable de traitement d'assurer que, par défaut, seules les données qui sont strictement nécessaires pour tous les objectifs de traitement seront traitées. Cette obligation implique que c'est le propriétaire des données qui peut choisir, sous la forme d'un opt-out, de lever ce droit à la vie privée par défaut et de consentir au traitement de ses données. A l'inverse, le PDPB promeut la protection dès la conception[291] mais ne spécifie pas que les citoyens ont accès au seuil le plus élevée de protection par défaut ; à l'inverse on remarque que les individus doivent réaliser un opt-in pour y avoir accès[292], ce qui affaiblit la protection de leurs données personnelles en ce que cela laisse une plus grande marge de manœuvre aux entreprises pour récolter les données des citoyens même lorsqu'elles ne sont pas conditionnées à la nécessité des objectifs de traitement.

SECTION 4: UN QUATRIEME MODELE DE PROTECTION DES DONNEES ?

Suite à la promotion de ces neufs principes, qui reprennent dans les grandes lignes nombre des dispositions misent en avant par le RGPD, le Rapport Srikrishna a annoncé que l'Inde disposerait, dès l'entrée en vigueur du PDPB, d'une quatrième approche permettant une protection complète et générale de la vie privée de ses citoyens. Cette nouvelle approche

[289] G. GREENLEAF, « GDPR-lite and requiring strengthening – submission on the Draft Personal Data Protection Bill to the ministry of electronics and information technology », *op. cit.,* p. 12.
[290] Article 25, RGPD.
[291] Section 29, PDPB.
[292] G . GREENLEAF, « India's « Fourth Way » : GDPR-lite with chinese characteristics ? », *op. cit.,* p. 11.

devrait également permettre l'autonomie et l'indépendance de l'Inde sur le plan des régimes de protection des données[293]. Il est clair qu'il est dans l'intention du gouvernement indien de se distinguer du modèle européen, américain ou même chinois. Pour autant, on remarque une influence marquée du régime européen pour l'approche fondamentale du droit à la vie privée, pour le champ d'application du PDPB ou encore pour les droits individuels qu'il promeut, et du régime chinois pour le pouvoir discrétionnaire que le texte permet encore au gouvernement de par ses larges exceptions au principe de légalité de traitement et quant à l'indépendance factice de l'AIPD[294].

Toutefois, et s'il faut reconnaître que le Comité Srikrishna a proposé un texte bien pensé et très complet sur le plan intellectuel[295], le PDPB présente encore des zones d'ombre qui laissent planer le doute sur l'issue d'une potentielle décision d'adéquation par l'Union européenne qui serait déterminante afin que ce projet de loi soit reconnu à sa « juste » valeur. En effet, cela fait bientôt deux décennies que l'Inde promet un régime moderne et global qui aurait un impact positif pour les citoyens indiens mais également une influence déterminante sur le monde économique en ce que les entreprises internationales ne seraient plus en mesure de bafouer davantage les droits à la vie privée issus du territoire indien[296].

En conclusion, nous pouvons revenir sur certains éléments pour déterminer si le PDPB est effectivement un candidat sérieux à devenir un modèle de protection des données indépendant.

Premièrement, il semble que le Comité Srikrishna avait clairement à l'esprit la globalisation des standards de protection de la vie privée lors de la rédaction de son projet de loi, en ce que le Rapport reprend explicitement comme objectif celui de devenir un modèle international et de s'élever comme une quatrième approche, indépendante de ses propres influences. En effet, le Rapport annonce, quant à la juridiction souhaitée pour le PDPB, que, d'une part, le texte devrait permettre de protéger les données personnelles des résidents indiens, et, d'autre part, « établir un modèle qui peut être répliqué à son tour par d'autres juridictions »[297]. Pour autant, il est important de souligner qu'en l'état, certaines dispositions présentes dans le texte

[293] *Ibid*., p. 14.
[294] *Ibid.*
[295] *Ibid.*
[296] L'inde avait en effet été outragée suite au scandale Facebook- Cambridge Analytica, où les données de millions de citoyens indiens avaient également été dévoilées. Voyez également : https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html
[297] Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the the Chairmanship of Justice B.N., p. 16.

risquent encore de tenir à distance les acteurs européens et américains ; plus spécifiquement, l'obligation de localisation physique des données ainsi que l'indépendance partielle de l'autorité de protection des données indienne rappelle le modèle chinois, ce qui risque d'empêcher une réelle reconnaissance de la part de ces derniers.

Deuxièmement, il est clair que le texte est basé sur les principes du RGPD. Il reprend en effet l'approche européenne, à savoir une approche prohibitive qui tente de faire passer une loi générale couvrant l'entièreté du secteur, ce qui distingue le PDPB du régime Indien actuel[298]. Tout comme le RGPD, le PDPB tente de trouver un équilibre entre innovation et sauvegarde du droit à la vie privée. Toutefois, certains de ces principes ne sont repris que de façon partielle et lacunaire, notamment en ce que l'Etat conserve encore un vaste pouvoir sur les données des citoyens, là où le RGPD s'évertue à garantir aux citoyens un contrôle sur leurs données qui soit le plus étendu possible. Le nouveau régime Indien n'est donc pas une quatrième approche à part entière, mais plutôt une version alternative et moins poussée des standards européens. Cependant, une telle approche pourra sans doute être bien reçue dans certains pays qui cherchent à améliorer leur régime de protection des données personnelles par un modèle modérément consistant avec les standards supérieurs du RGPD[299].

CONCLUSION : LE RGPD, UN MODELE INTERNATIONAL EN DROIT DE LA PROTECTION DES DONNEES PERSONNELLES ?

Lorsque l'on étudie le phénomène de convergence réglementaire au niveau international, certains auteurs[300] – et particulièrement chez nos voisins de l'autre côté de l'Atlantique – semblent avancer la thèse intéressante selon laquelle lorsque deux régimes souverains ont une vision politique commune, il en résulterait un consensus réglementaire efficace qui permettrait une harmonisation globale. A l'inverse, lorsque ces puissances sont en désaccord et ne partagent pas la même vision, il en résulterait une divergence menant droit à un bras de fer politique pour imposer ses propres standards « par la force » jusqu'à ce que le moins tenace disparaisse au gré du vainqueur. Or, il est clair qu'en matière de protection des données, il n'est pas encore possible de trouver de consensus politique quant à une approche

[298] J. RITU,« India 's digital data debated at town hall », Indica News, 29 Août 2018, disponible sur https://indicanews.com/2018/08/29/indias-digital-data-debated-at-town-hall/ , consulté le 1 Août 2019.
[299] G. GREENLEAF, « India's « Fourth Way » : GDPR-lite with chinese characteristics ? », *op. cit.*, p.13..
[300] A. BRADFORD, *op. cit.*, p. 3.

adéquate et commune à adopter. D'abord, parce qu'il existe encore au niveau international des différences trop flagrantes entre les Etats dits développés et les pays en voie de développement. Ensuite, et nous l'avons vu, parce que les grandes économies mondiales n'ont pas – ou pas toujours du moins - la même approche lorsqu'il s'agit de protéger les donnés personnelles de leurs citoyens. Il existe des craintes qu'avec l'entrée en vigueur du RGPD, les différents systèmes mondiaux de protection des données personnelles s'affrontent et provoquent une scission de l'Internet et de l'économie numérique; pourtant, nous maintenons la thèse que malgré ces divergences de conceptions politiques ou réglementaires, le RGPD permet une convergence vers un standard global de la protection des données.

Premièrement, une question sous-jacente à notre problématique consiste à déterminer si l'Union européenne a ou non la capacité d'imposer ses propres standards de façon extraterritoriale et de stimuler le secteur de protection de la vie privée vers une convergence globale. Notre étude nous permet de répondre par l'affirmative et d'isoler certains des mécanismes permettant ce phénomène.

D'abord, nous soulignons que l'importance économique du marché européen est un facteur clé favorisant cette convergence globale. En tant que partie prenante du plus grand marché de consommateurs au monde, le modèle européen s'impose finalement à tous les producteurs étrangers, qui ne peuvent accéder au marché intérieur qu'en modifiant leurs propres standards. Le principe est limpide: au plus strict le marché importateur, au plus les pays exportateurs seront forcés de se plier à ses exigences. Ensuite, la capacité réglementaire européenne lui permet d'harmoniser d'une traite l'ensemble du droit des Etats membres par des instruments tels que le Règlement, et d'en assurer le respect par des mécanismes de sanctions uniformisés. Enfin, les règles strictes du RGPD, applicables extraterritorialement, ainsi que ses garanties pour les transferts internationaux, lui permettent d'assurer un standard de protection supérieur. Ces trois éléments participent *de facto* à la diffusion des standards européens.

Deuxièmement, si l'on affirme que l'Union européenne a, grâce au RGPD, la capacité d'augmenter la convergence globale vers ses propres standards, il nous faut évaluer de façon similaire si, dans les faits, cela porte ses fruits.

Quant à cette question de l'influence européenne au niveau international, il est bon de rappeler que lorsque nous nous sommes lancés sur la piste d'un modèle international à

vocation universelle, nous trouvâmes sans grande surprise que le premier traité sur la protection de la vie privée à être contraignant pour ses signataires reposait déjà dans les bras du Conseil de l'Europe avec la Convention 108. Cela témoigne d'emblée, à notre sens, d'une volonté européenne d'atteindre un standard universel pour la protection des données personnelles. On remarque par ailleurs que dès la deuxième génération, les standards européens virent le jour dans un esprit qui comportait déjà le souhait d'engendrer des standards supérieurs qui soient repris globalement, ce qui était explicitement repris dans la Directive. A l'avènement de la troisième génération de standards européens, cristallisés au sein du Règlement, nous affirmons que le RGPD a déjà eu un impact important autour du globe.

La partie comparative de ce travail s'est attardée sur certaines des plus grandes économies mondiales afin de tenter d'y déceler l'influence européenne.

D'abord, nous avons pu établir que l'influence du RGPD en Californie sert de terreau fertile à une approche européenne au sein des Etats-Unis, qui se sont toujours illustrés par une approche réglementaire fondamentalement différente. En outre, et puisque ses dispositions s'appliqueront à 500 000 entreprises[301] et protégeront près de 40 millions de résidents californiens[302] grâce à sa large applicabilité, le CCPA est en bonne voie pour constituer le nouveau standard de référence aux États-Unis. Combiné au RGPD, qui protège environ 500 millions de citoyens européens, le nouveau cadre de protection des données de ces deux instruments constitue, en fait, un standard mondial, car des milliers d'entreprises devront se conformer à l'un ou à l'autre en fonction de leurs activités de marché[303].

Ensuite, il ressort de la décision d'adéquation entre le Japon et l'Union européenne que ce dernier a modernisé son texte de loi afin qu'il s'aligne majoritairement sur le RGPD. Bien que l'APIP présente encore des lacunes, notamment au niveau de ses mécanismes de sanctions et des droits individuels qu'il octroie, on ne peut nier l'influence européenne sur le régime japonais si l'on prend en compte, d'une part, le régime sur mesure qui fut édicté afin d'obtenir une décision positive de la Commission et, d'autre part, l'amélioration, selon les critères

[301] R. HEIMES, et S. PFEIFLE, *op. cit.*
[302] C. BARRETT, *op. cit.* , p. 6.
[303] *Ibid.*, p. 7.

européens, des standards de protection de la vie privée présents dans la version amendée de l'APIP.

En outre, l'analyse du PDPB Indien nous permet de prendre une position plus contrastée. Certes, l'Inde a reconnu dès l'origine de son travail réglementaire qu'ils avaient le RGPD à l'esprit dans la construction de leur régime de protection des données. Pour autant, en laissant un tel pouvoir discrétionnaire à son gouvernement, et en incluant une obligation physique de localisation des données sur leur territoire, l'Inde s'est éloignée de la conception européenne afin de prétendre à une nouvelle approche indépendante.

Enfin, au niveau mondial, on remarque aujourd'hui une influence du RGPD sur la plupart des continents. Sur le continent africain, on observe que les pays qui présentent déjà une loi sur la protection des données tels que l'Afrique du Sud, le Ghana ou l'Angola ont des régimes qui protègent les données personnelles de façon similaire au RGPD[304]. En Asie, et suite à l'analyse de l'Inde et du Japon, nous pouvons ajouter les Philippines et la Corée du Sud[305] à la liste des pays qui sont en phase d'inclusion des standards européens. En Amérique du Sud, nous avons déjà cité le Brésil et nous pouvons également citer le Mexique en Amérique centrale, qui avait dors et déjà ratifié la Convention 108 et qui est en phase de modernisation pour inclure les standards supérieurs du RGPD[306].

Pour conclure, il semble que l'Europe soit en bonne voie de réussir son pari de l'externalisation de ses standards sur la scène internationale. Il faut reconnaître que les standards particulièrement stricts du RGPD peuvent représenter un effort titanesque pour les acteurs économiques qui tentent d'accéder au marché européen, et qu'il n'est pas exempt de critiques ou de défauts. Pour autant, nous réalisons que le RGPD représente aussi et surtout une réponse nécessaire au cri de plus en plus prononcé des citoyens du monde lorsqu'ils clament qu'ils sont excédés de voir leurs données personnelles bafouées à leur insu, à l'ère du

---

[304] Notamment pour la définition des données personnelles ou pour le transfert de données, bien que des divergences fonctionnelles subsistent, tels que des moyens de recours inefficaces. Voyez pour plus d'informations : M. RUSTAD et T. KOENIG, *op. cit.*, p. 433.

[305] La Corée du Sud est actuellement dans l'attente d'une décision d'adéquation de la part Commission européenne, voyez : D. MEYER., « South Korea's EU adequacy decision rests on new legislative proposals », *International Association of Privacy Professionals,* 27 Novembre 2018, disponible sur : https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/, consulté le 7 Août 2019.

[306] M. RUSTAD et T. KOENIG, *op. cit.*, p. 435.

numérique moderne et en plein essor qui est la nôtre. Ne dit-on pas qu'il vaut mieux obtenir un diamant brut qu'une turquoise polie ? Le RGPD, en tant que modèle international, est peu à peu reconnu comme le Joyaux de la couronne du droit de la protection des données et, ce faisant, rassemble de plus en plus de sujets sous ses dispositions.

BIBLIOGRAPHIE :

I. LEGISLATION

1. UNION EUROPEENNE

- Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C 364 du 18 décembre 2000, Article 8.

- 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, *JOCE*, L 281/3, 23 novembre 1995, p. 31.

- 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, *J.O.U.E.*, L 119/1, 4 mai 2016, p. 1.

2. CONSEIL DE L'EUROPE

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et Protocole additionnel, signé à Paris le 20 mars 1952, approuvés par la loi du 13 mai 1955, *M.B.,* 19 août 1955, p. 5028 (ci-après "CEDH"), Article 8.

- Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n°108), faite à Strasbourg le 28 janvier 1981.

- Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 mai 2018.

3. ETATS-UNIS

- Assembly Bill No. 375: an act to add title 1.81.5 (commencing with section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy, *California Consumer Privacy Act,* June 28th, 2018.

- California Legislature: Assembly Bill No. 1760 : *Privacy for All,* April 12th , 2019.

4. JAPON

- Act on the protection of personal information for the handling of Personal Data, 2017.

5. INDE

- Information Technology Act, 2000.

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

- Information Technology - Reasonable security practices and procedures and sensitive personal data or information Rules, 2011.

II. DÉCISIONS, AVIS, COMMUNICATIONS, COMMUNIQUÉS ET PROPOSITIONS, RAPPORTS

1. COMMISSION

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions - *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, 2012, disponible sur : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52012DC0009, consulté 5 Juillet 2019.

- European Commission – Press release, *EU-US Privacy Shield: Second review shows improvements but a permanent Ombudsperson should be nominated by February 2019,* 2018, disponible sur http://europa.eu/rapid/press-release_IP-18-6818_en.htm , consulté le 2 Mai 2019.

- Communiqué de presse de la Commission Européenne, « La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde », Bruxelles, 23 Janvier 2019, disponible sur: https://europa.eu/rapid/press-release_IP-19-421_fr.htm, consulté le 2 Août 2019.

- Communiqué de presse de la Commission Européenne, « Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World, Questions and Answers » 10 janvier 2017, disponible sur : http://europa.eu/rapid/press-release_MEMO-17-15_en.htm , consulté le 30 juillet 2019.

- Supplementary Rules under the Act on the protection of personal information for the handling of Personal Data Transferred from the Eu based on an Adequacy Decision, Annex 1, disponible sur https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf, (consulté le 29 juillet 2019).

2. CONSEIL

- Rapport explicatif de la Convention 108 telle que modifiée par le Protocole d'amendement, série des traités du Conseil de l'Europe n°223, 2018.

3. GROUPE DE TRAVAIL

- G29, « Opinion n°01/2016 on the EU-U.S. Privacy Shield draft adequacy decision», *WP238,* 13 avril 2016.

4. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

- Commission Nationale de l'Informatique et des Libertés, *Délibération de la formation restreinte n°SAN-2019-001 du 21 Janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.*, disponible sur : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1 , consulté le 25 Mai 2019.

5. COUR SUPREME ET GOUVERNEMENT INDIEN

- Government of India, Planning Commission, *Report on the group of experts on Privacy,* 2012.
- J. Chandrachud's opinion, *Puttaswamy v. Union of India*, Paragraph 185, Writ petition (civil) no 494 of 2012, 6MLJ267 , 2017.
- Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the the Chairmanship of Justice B.N. Srikrishna, 2018, disponible sur: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report- comp.pdf , consulté le 25 Juillet 2019.
- Report of the Group of Experts on Privacy, 2018, disponible sur: http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf, consulté le 30 Juillet 2019.
- Data Protection Committee Report, « A free and Fair Digital Economy, Protecting Privacy, Empowering Indians » Committee of experts under the Chairmanship of Justice B.N. Srikrishna, 2018.

III. JURISPRUDENCE

1. COUR DE JUSTICE

- Arrêt *Maximillian Schrems/Data Protection Commissioner,* C-362/14, EU:C:2015:650.

2. CONSEIL DE L'EUROPE

- Cour eur. DH, arrêt *Copland c. Royaume-Uni* du 25 juin 1997, *Rec. Cour eur. D.H.*, 1997-III.
- Cour eur. DH, arrêt *Amann c. Suisse* du 16 février 2000, *Rec. Cour eur. D.H.*, 2000-II, point 65.
- Cour eur. DH, arrêt *Rotaru c. Roumani*e du 4 mai 2000, *Rec. Cour eur. D.H.*, 2000-V.

3. COUR SUPREME INDIENNE

- Puttaswamy v. Union of India, Writ petition (civil) no 494 of 2012, 6MLJ26, 2017.

IV. DOCTRINE

1. MONOGRAPHIES

- GONZALEZ FUSTER, G., *The emergence of Personal Data Protection as a Fundamental Right of the EU*, Etats-Unis, Springer International, 2014.

2. CONTRIBUTIONS DANS UN OUVRAGE COLLECTIF

- GOLDSMITH, J. et WU, T., Who *Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006.

- HAMILTON, L., HELLEPUTE, C.-A., TATA, S., YAROS, O., BURMAN, K.C., DE CICOO, D.et WOOTEN, E.M.., *Keeping it private : GDPR and developments in data privacy in 2019*, Mayer Brown, 2018.

- HUSTINX, P., « EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation » *in New technologies and EU Law,* M. CREMONA (dir.), Oxford Scholarship online, 2017.

- DETERMANN, L., et GUPTA, C., « Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law », *UC Berkeley Public Law Research Paper*, 18 septembre 2018.

3. ARTICLES DE REVUE :

- AIHARA, Y., et NORIKO, H., « Data Privacy Protection of personal Information versus Usage of Big Data: Introduction of the recent amendment to the Act on the Protection of Personal Information (Japan) », *Defense Counsel Journal, vol. 84, no. 4,* Octobre 2017.

- ALBRECHT, P., « How the GDPR will change the world », *European Data Protection Law*, 2016.

- BARRETT, C., « Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? », *Scitech Lawyer*, Vol. 15(3), 2019.

- BENDIEK, A., et RÖMER, M., « Externalizing Europe: the global effects of European data protection », *Digital Policy, Regulation and Governance*, Vol. 21 Issue: 1, 2019.

- BRADFORD, A., « The Brussels Effect », *107 Nw. U.L. Rev. 1*, 2015.

- BAILEY, R. et PARSHEERA, S., « Data Localisation in India: Questioning the Means and Ends », NIPFP *Working Paper No. 24*2, 2018.

- CLARK, J., et HALPERT, J., « California's Consumer Privacy Act and the GDPR - where do they overlap », *Privacy and Data Protection,* 18 (7), 2018.

- DE HERT, P., et CZERNIAWSKI, M., « Expanding the European data protection scope beyond territory: Article 3 of the General Data protection Regulation in its wider context », *International Data Privacy Law,* Vol. 6, No. 3, 2016.

- GLON, C., « Data Protection in the European Union: a closer look at the current patchwork of Data Protection Laws and the proposed reform that could replace them all », *International Journal of Legal Information,* vol. 42.3*,* 2015.

- GREENLEAF, G., « The influence of European data privacy standards outside Europe: Implications for globalization of convention 108 », *International Data Privacy Law*, Vol. 2, 2012.

- GREENLEAF, G., « Japan: Towards international standards – except for 'big data' », *Privacy Laws & Business International Reports, Issue 135,* Juin 2015.

- GREENLEAF, G., « European' Data Privacy Standards Implemented in Laws Outside Europe », *149 Privacy Laws & Business International Report 21-23; UNSW Law Research Paper No. 2.*, 3 Septembre 2017, p. 4.

- GREENLEAF, G., « Global Data Privacy Laws », *145 Privacy Laws and Business International Report*, 2017.

- GREENLEAF, G., « Questioning 'adequacy' (Pt 1) – Japan », *150 Privacy Laws & Business International Report,* 1, 6-11, 2017.

- GREENLEAF, G., « Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018 », *UNSW Law Research Paper No. 18-56*, 24 Mai 2018.

- GREENLEAF, G., « India's « Fourth Way »: GDPR-lite with Chinese characteristics? », *UNSW Law Research Paper No. 18-83.*, 20 Septembre 2018.

- G. GREENLEAF, « GDPR-lite and requiring strengthening – submission on the Draft Personal Data Protection Bill to the ministry of electronics and information technology », *University of New South Wales Research Series,* 2018.

- G. GREENLEAF, « Japan proposed EU Adequacy Assessment - Substantive issues and procedural hurdles », 154 Privacy Laws & Business International Report; *UNSW Law Research Paper No. 18-53*, 2018, p. 9.

- GREENLEAF, G., « Japan: EU adequacy discounted », *155 Privacy & Business International Report 8,* 2018.

- INGLEY, C., et WELLS, P., *GDPR: Governance Implications for regimes outside the EU,* AUT University Press, Auckland, 2018.

- KARADUMAN, O., "The General Data Protection Regulation: Achieving compliance for EU and non-EU companies", *Business Law International*, Volume 18, Issue 3, 2017.

- KUNER, C., « The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law », *Bloomberg BNA Privacy and Security Law Report*, 11 PVLR 215, 2 Juin 2012.

- KUNER, C., « The European Union and the Search for an International Data Protection Framework », *Groningen Journal of International Law*, 2014.

- KUNER, C., « Extraterritoriality and regulation of international data transfers in EU data protection law », *International Data Privacy Law,* Vol. 5, No. 4, 2015.

- LANGHEINRICH, M., « The Golden Age of Privacy ? », *IEEE Pervasive Computing,* 2018.

- PRASAD, S-K., "(Draft) Paper on Information Technology Act, 2000 and the Data Protection Rules", C*entre for Communication Governance at National Law University,* Delhi, 30 Décembre 2017.

- PRASAD, S-K., « Back to the Basics: Framing a New Data Protection Law for India », 30 Janvier 2018.

- RUSTAD, M. et KOENIG, T., « Towards a Global Data Privacy Standard », *Florida Law Review,* vol. 71, no. 2, March 2019.

- SAFARI, B-A., « Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection », *47 Seton Hall L. Rev. 809*, 2017.

- SCHWARTZ, P., « Global Data Privacy: The EU Way », *New York University Law Review*, Vol. 94, 2019.

- WAGNER, J., « The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? », *International Data Privacy Law,* Vol 8, No 4, 2018.

V. DIVERS

1. SOURCES ELECRTONIQUES

- AGARWAL, S., « Justice BN Srikrishna to head Committee for data protection framework », *The Economic Times*, 1er Août 2017, disppnible sur: https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection- framework/articleshow/59866006.cms, consulté le 25 Juillet 2019.

- CARSON, A., « Israel, Japan, Canada talk keeping up with the GDPR », *International Association of Privacy Professionals,* disponible sur: https://iapp.org/news/a/israel-japan-and-canada-talk-keeping-up-with-the-gdpr-2/, consulté le 1er Août 2019.

- COOS, A., « Data Protection in Japan: All you need to know about APPI », *Endpoint Protector,* 1er Février 2019, disponible sur : https://www.endpointprotector.com/blog/data-protection-in-japan-appi/ , consulté le 31 juillet 2019.

- DAVIES, T., « European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows », *PrivSec Report,* 24 Janvier 2019, disponible

sur:https://gdpr.report/news/2019/01/24/european-commission-adopts-adequacy-decision-on-japan-creating-the-worlds-largest-area-of-safe-data-flows/, consulté le 3 Août 2019.

- DUROU, E., *Big Data, Mining a national resource,* 2015, disponible sur: https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/no-place-like-home/big-data.html# , consulté le 6 mai 2019.

- GERENCSER, G., « Japan 's long road for adequacy under the GDPR », *International Association of Privacy Professionals*, 2018, disponible sur : https://iapp.org/news/a/japans-long-road-for-adequacy-under-the-gdpr/ , consulté le 30 juillet 2019.

- H. HAYASHI, « Japan : Data Protection 2019 », *The ICLG to : Data Protection Laws and Regulations,* 3 Juillet 2019, disponible sur https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan , consulté le 1er Août 2019.

- R. HEALEY, « How the Japan APPI compares to the GDPR, are you compliant? », *GDPR 24/7 Privacy by Design*, 13 Mars 2019, disponible sur : https://relentlessdataprivacy.com/japanappi-v-eu-gdpr/, consulté le 29 juillet 2019.

- HEIMES, R.et PFEIFLE, S., *New California Privacy Law to affect more than half a million US companies,* 2018, disponible sur: https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/, consulté le 5 Mai 2019.

- MARINI, A., KATEIFIDES, A., BATES, J., ZANFIR-FORTUNA, G., BAE, M., GRAY, S., et SEN, G., *Comparing Privacy Laws : GDPR vs CCPA*, 2019, disponible sur: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf, consulté le 6 Mai 2019, p. 30.

- MEYER, D., « South Korea's EU adequacy decision rests on new legislative proposals », *International Association of Privacy Professionals,* 27 Novembre 2018, disponible sur : https://iapp.org/news/a/south-koreas-eu-adequacy-decision-rests-on-new-legislative-proposals/, consulté le 7 Août 2019.

- MIDAZVETSKAYA, Y., « What are the pros and cons of the Adequacy decision on Japan », *Centre for IT & IP Law Blog,* disponible sur: https://www.law.kuleuven.be/citip/blog/what-are-the-pros-and-cons-of-the-adequacy-decision-on-japan/ , consulté le 3 août.

- O'DONOVAN, A., *CNIL vs Google : 10 lessons from the largest data protection fine ever issued,* 2019, disponible sur : https://www.passwordprotectedlaw.com/2019/01/cnil-vs-google-largest-fine/, consulté le 30 avril 2019.

- REDING, V., *A data protection compact for Europe.,* 2014, disponible sur: http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm , consulté le 27 Avril 2019.

- RITU, J., « India 's digital data debated at town hall », Indica News, 29 Août 2018, disponible sur https://indicanews.com/2018/08/29/indias-digital-data-debated-at-town-hall/ , consulté le 1 Août 2019.

- SIMMONS, D., *5 countries with GDPR-like Data Privacy Laws,* 2019, disponible sur: *https://insights.comforte.com/5-countries-with-gdpr-like-data-privacy-laws*, consulté le 6 Mai 2019.

- TAKASE, K., « GDPR matchup : Japan's Act on the protection of personal information », *International Association of Privacy Professionals*, 2017, disponible sur :

https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/, consulté le 30 juillet 2019.

- TSUKAYAMA, H., *It's time for California to guarantee « Privacy for All »,* Electronic Frontier Foundation, 2019, disponible sur: https://www.eff.org/deeplinks/2019/02/its-time-california-guarantee-privacy-all, consulté le 1 Août 2019.

- OECD, *30 years after the OECD Privacy Guidelines*, 2011, disponble sur: http://www.oecd.org/sti/ieconomy/49710223.pdf , consulté le 30 Mai 2019.

- OECD*, OECD Privacy Guidelines* 2013, disponible sur: http://www.oecd.org/sti/ieconomy/oecd- privacy-framework.pdf., consulté le 30 Mai 2019.

- The Japan Times, *Amended privacy protection law* , 1er Juin 2017, disponible sur : https://www.japantimes.co.jp/opinion/2017/06/01/editorials/amended-privacy-protection-law/#.XT63SpMzY_U, consulté le 31 juillet 2019.

- GDPR EU.org, *Fines and penalties,* 2017*,* disponible sur: https://www.gdpreu.org/compliance/fines-and-%20penalties/ consulté le 4 août 2019.

- BigID, *California Consumer Privacy Act vs GDPR: What you need to know,* 2019, disponible sur: https://bigid.com/wp-content/uploads/2018/07/California-Consumer-Privacy-Act-vs-GDPR-What-You-Need-To-Know.pdf , consulté le 27 Avril 2019.

- Data Guidance, Future of Privacy Forum, *Comparing Privacy Laws: GDPR vs CCPA,* 2019, disponible sur: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf , consulté le 2 Mai 2019, p. 9.

- DuckduckGo, *24 Tech Companies Back CCPA Amendment to make it stronger: Privacy for All Act of 2019,* 2019, disponible sur*:* https://spreadprivacy.com/ccpa-privacy-for-all-act/ , consulté le 30 Avril 2019.

- 451 Research Report Reprint, *The California Consumer Privacy Act : not just « America's GDPR »,* 2019, disponible sur: https://integris.io/wp-content/uploads/2019/03/451_Reprint_TheCaliforniaConsumerPrivacyAct.pdf, consulté le 2 Mai 2019, p. 4.

2. ROMANS

- A. MAALOUF, « Les identités meurtrières », Grasset, 1998.

.