Année académique 2018-2019

ETUDE DE LA GEOPOLITIQUE ET SOUVERAINETE DE LA DONNEE : REGLEMENTATIONS ETATIQUES, CLASSIFICATION DES DONNEES ET QUESTIONS DE PROPRIETE DE LA DONNEE

MEMOIRE

MBA Risques Sûreté Internationale et Cybersécurité

Franz JIOFACK TANGOUTSOP

PRINCIPAUX SIGLES ET ACRONYMES

AFAPDP	Association Francophone des Autorités de Protection des Données Personnelles
APEC	Asia Pacific Economic Cooperation
BATX	Baidu, Alibaba, Tencent et Xiaomi
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CBPR	Cross-Border Privacy Rules System
GAFAM	Google, Apple, Facebook, Amazon et Microsoft
IRIS	Institut de Relations Internationales et Stratégiques
NATU	Netflix, Airbnb, Tesla et Uber
RDPG	Règlement Européen sur la Protection des Données

SOMMAIRE

INTRODUCTION

L'idée selon laquelle l'espace géographique détermine la politique des peuples et des nations est ancienne. A ce titre, comme le relève Pascal Boniface, fondateur et directeur de l'Institut de Relations Internationales et Stratégiques (IRIS), Aristote déjà à son époque *« (…) estimait que l'environnement naturel avait un impact sur le caractère humain des citoyens et sur les nécessités militaires et économiques d'un Etat idéal*[1] *»*. Avec donc l'avènement des premiers Etats au Proche Orient et en Egypte antique, trois mille ans avant notre ère, l'environnement géographique acquière une dimension géopolitique. Pour Alexandre Defay, professeur au centre de géostratégie de l'ENS, à partir de cet instant, *« (…) l'espace n'est plus seulement façonné et cloisonné par la diversité du milieu naturel et par celle du peuplement, mais aussi par l'exercice de souverainetés étatiques concurrentes* [2] *»*.

Si au départ le milieu géographique était essentiellement constitué de l'espace terrestre, maritime, aérien ou de l'espace extra-atmosphérique, plus récemment un nouvel espace s'est ajouté, à savoir le cyberespace encore appelé l'espace numérique[3]. Né à la suite de l'arrivée du Web ou *World Wide Web*[4] à la fin du XXème siècle, le cyberespace est considéré pour beaucoup comme le 6e continent bien que n'étant pas palpable. Celui-ci se définit en effet comme un *« espace immatériel produit par l'ensemble des relations sociales qui s'établissent via des réseaux de télécommunications informatiques interconnectés (Internet)*[5] *»*. Aujourd'hui, le cyberespace fait l'objet de convoitise - comme l'ont été les autres auparavant - de la part des Etats qui entendent chacun à leur façon y exerce leur souveraineté.

En effet, malgré sa singularité, cet espace n'apparaît pas fondamentalement différent des autres et les principes de base de la stratégie peuvent s'y appliquer sans trop de difficultés[6]. Ainsi, l'espace numérique constituerait alors un enjeu légitime de puissance tout à fait déterminant dans les rapports de force. Selon Grégoire Germain et Paul Massart *« les acteurs étatiques et industriels*

---

[1] Pascal Boniface, *La géopolitique*, Éditions Eyrolles : 6e Ed, 2019, p.8

[2] Alexandre Defay, *La géopolitique*, Que sais-je ? 4e éd. 2018, p. 4

[3] Cet espace stratégique n'a en effet pas plus d'une cinquantaine d'années.

[4] Pour le grand public, l'Internet et web tendent souvent à être confondus. Dans la réalité, le web n'est qu'une sphère avec les Gopher, Ftp, Wais et Newsgroup qui compose Internet (interface de communication prenant en charge plusieurs types de fichiers différents). On peut dès lors définir le web comme *« (…) une immense ''toile d'araignée'' mondiale qui relie des milliers d'ordinateurs et qui permet surtout un accès très convivial aux informations grâce au principe d'hypertexte et au caractère multimédia de chaque document publié ».* Carlo Revelli, *intelligence stratégique sur internet,* 1998, pp.24-27

[5] Pascal Gauchon, Jean-Marc Huissoud, *Les 100 mots de la géopolitique*, Que sais-je ? 5e éd. 2019, p.104

[6] Paul Massart, *Faut-il créer une nouvelle stratégie pour le cyberespace ?* Revue de la Défense nationale, n°757, février 2013, pp.116-120.

qui en maîtrisent les ressorts conserveront l'initiative et l'indépendance et ils pourront préserver leur invulnérabilité. Inversement, ceux qui perdront le contrôle de certains compartiments de ce ''terrain'' seront réduits à agir en réaction, à dépendre d'autres acteurs hégémoniques et à subir les conséquences de leur vulnérabilité[7] ». Dans cet ordre d'esprit, Anne Grély affirme qu' *« il faut pouvoir planter son drapeau dans le cyberespace … [et de poursuivre] les Etats ont d'ailleurs reconnu en 2013 à l'ONU que leur souveraineté s'appliquait sur la couche physique c'est-à-dire sur les infrastructures situées sur le territoire, en revanche pour tout ce qui est la couche logicielle, ce qui concerne les données, là il n'y a pas de consensus et on ne sait pas exactement à qui appartiennent les données*[8] ». C'est dire ici que les infrastructures, les applications et surtout les données constituent le cœur de l'enjeu de la souveraineté numérique[9].

En s'appuyant sur une grille de lecture reposant sur la géopolitique, il sera question pour nous ici d'analyser ce désir de contrôle des Etats sur l'espace numérique et plus particulièrement sur une de ses composantes que sont les données[10]. Cette analyse nous permettra *in fine* de positionner chaque nation dans l'espace numérique et d'évaluer leur souveraineté sur la donnée.

A l'image de nombreuses disciplines scientifiques, la pratique de la géopolitique a précédé la création du concept introduit pour la première fois par le professeur suédois de science politique Rudolf Kjellén en 1905[11]. Ce dernier définissait la géopolitique comme « *la science de l'Etat en tant qu'organisme géographique, tel qu'il se manifeste dans l'espace*[12] ». Cependant, cette discipline a été diabolisée par la suite ; parce qu'assimilée à l'expansionnisme nazies qui a conduit à la seconde guerre mondiale[13]. C'est que vers la fin du siècle dernier que la géopolitique retrouve ses lettres de noblesse dans le monde scientifique et politique. En France en particulier, la

[7] Germain Grégoire, Paul Massart (2017), op.cit. p. 49

[8] Isabelle Guibert, Frédéric Jeannin, *Les nouvelles frontières numériques : RGPD et politiques de protection des données*, VA éditions, 2018, p.9

[9] Bien que primordiaux pour une souveraineté numérique, il conviendrait d'y ajouter pour être plus complet, l'ensemble des servitudes dont elles dépendent telle notamment l'alimentation électrique. Germain Grégoire, Paul Massart (2017), op.cit. pp.50-53. Dans le même ordre d'idée, Thierry Berthier et Olivier Kempf énumèrent les différents éléments qui caractérisent la puissance data-numérique d'une nation. On y retrouve ainsi cinq grandes capacités que sont : sa capacité en data-infrastructures, sa capacité de data-traitement, sa capacité d'attractivité auprès des grands acteurs internationaux de la donnée, sa capacité à former des *data scientist* et, enfin, sa capacité de priorisation d'une politique de la donnée. Thierry Berthier, Olivier Kempf, *Vers une géopolitique de la donnée*, Annales des Mines - Réalités industrielles, vol. août 2016, no. 3, 2016, pp.15-17 *(annexe 1 p.30)*

[10] Au côté des données, on a également d'un point de vue macroscopique, les applications qui permettent leurs traitements et les réseaux qui permettent les échanges. Germain Grégoire, Paul Massart*, Souveraineté numérique*, Études, vol. octobre, no. 10, 2017, p.50

[11] Alexandre Defay (2018), *op.cit.* p.9

[12] Rudolf Kjellen, *L'État comme forme de vie*, 1916

[13] Alexandre Defay, *ibid.* pp.23-30. Cette vision allemande de la géopolitique a notamment été prônée par des penseurs comme Freidrich Ratzel et Karl Haushofer. Pascal Gauchon, Jean-Marc Huissoud (2019), op.cit. pp.3-11

discipline fut réhabilitée grâce à Yves Lacoste dans le années 1970, qui va en faire une science permettant de comprendre le monde et non une justification politique d'oppression par certains peuples[14]. Pour le français, la géopolitique est *« l'étude des différents types de rivalités de pouvoir sur les territoires, (…) la puissance se mesurant en fonction de potentialité territoriale interne et de la capacité à se projeter à l'extérieur de ce territoire et à des distances de plus en plus grande*[15] ». L'espace géographique devient ainsi tout simplement un espace de manifestation de la puissance[16]. Depuis, la discipline a évolué et s'est renouvelée du fait de la raréfaction des grands conflits territoriaux, la dématérialisation, la mondialisation des échanges et des communications[17], et s'étend maintenant à d'autres affrontent dans l'espace numérique.

En nous appesantissant uniquement sur la donnée, il s'agit de ce que certains qualifient de « matière première » de l'espace numérique. A cet égard, une donnée pour la Commission ministérielle de terminologie de l'informatique (qui n'existe plus aujourd'hui) est *« (…) la représentation d'une information sous forme conventionnelle destinée à faciliter son traitement*[18] *»*. Celle-ci acquière sa valeur grâce à son volume et le traitement qui en ait fait pour en faire un renseignement pertinent. Ce volume de données *(big data)*[19], est généré par l'accumulation des connaissances qui circulent sur le Web et qui proviennent d'activités humaines, industrielles, commerciales, etc.[20] Comme le relève si bien Thierry Berthier et Olivier Kempf, *« en 2015, l'humanité a produit, en une seule minute, 200 millions de méls, 15 millions de SMS, 350 000 tweets, 250 gigaoctets de données sur Facebook et plus de 1 740 000 gigaoctets d'informations numériques au niveau mondial. Google a traité quotidiennement plus de 24*

[14] Pascal Boniface (2019), op.cit. p. 30

[15] A travers cette définition faite par Yves Lacoste, l'on pourrait s'interroger la distinction entre la géopolitique et la géographie politique. Or comme le relève si bien Ladis K.D. Kristol, *« la géographie politique se concentre sur les phénomènes géographiques et leur donne une interprétation politique. La géopolitique se concentre sur les phénomènes politiques pour en donner une interprétation géographique et étudie les aspects géographiques de ces phénomènes »*. Pascal Boniface (2019), *ibid.* pp.13-14

[16] Cette nouvelle réalité s'est manifestée à travers la guerre qui opposa l'Iran à l'Irak entre 1980 et 1988. Pascal Boniface (2019), ibid. p. 43

[17] Pascal Gauchon, Jean-Marc Huissoud (2019), *ibid.* p.4

[18] Pour cette défunte commission, *« une information est un élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué »*. Olivier de Maison Rouge, *Les cyberisques : la gestion juridique des risques à l'ère immatérielle*, LexisNexis, 2018, p.71.

[19] Selon les archives de la bibliothèque numérique de l'Association for Computing Machinery, ce terme est apparu pour la première fois en octobre 1997. Concrètement, le *Big Data* renvoi à *« (…) un ensemble très volumineux de données qu'aucun outil classique de gestion de base de données ou de gestion de l'information ne peut vraiment travailler »*. Pour être encore plus pertinent, les données doivent être non seulement volumineuses, mais également variées et avoir une vitesse de création, de partage et de collecte rapide ; d'où les trois V du *big data* que sont le volume, la variété et la vitesse. Éric Peres – Rapporteur, « Les Données numériques : un enjeu d'éducation et de citoyenneté », Les Avis du Conseil économique, social et environnemental, janvier 2015, p.16

[20] A ce propos, cf. le rapport *« Digital, social media, mobile et e-commerce en 2018 »* publié par We Are Social et Hootsuite

pétaoctets de données (soit 24 millions de milliards d'octets)[21] ». Au cours de la même année, la part des produits et services numériques dans l'activité mondiale a représenté près d'un sixième du total de l'économie des biens et services traditionnels[22]. Dès lors, la souveraineté de la donnée revoit à une situation où celle-ci est soumise aux lois du pays où elle se trouve[23].

On le voit bien, la donnée est devenue un enjeu évident de puissance, car elles donnent des pouvoirs à celui qui sait la collecter et l'exploiter. Dès lors, si cet enjeu est d'abord commercial pour les acteurs privés à l'instar des géants du numérique[24], du côté des Etats l'enjeu est de contrôler et par ricochet protéger juridiquement la donnée (I) contre les accès frauduleux, les altérations, les suppressions, les modifications, les divulgations, les usurpations, les pertes et les fuites[25]. Pour ce faire, une classification de celle-ci est nécessaire tout en levant l'équivoque sur sa propriété effective (II).

[21] Berthier Thierry, Olivier Kempf, ibid. p. 13
[22] Éric Peres – Rapporteur, *« Les Données numériques : un enjeu d'éducation et de citoyenneté »*, Les Avis du Conseil économique, social et environnemental, janvier 2015
[23] Leslie Saladin, *La souveraineté des données, pourquoi est-ce essentiel ?* Journal du net, 27 juin 2018
[24] GAFAM (Google, Amazon, Facebook, Apple et Microsoft) et des NATU (Netflix, Air BnB, Telsa et Uber) aux Etats-Unis ou BATX (Baidu, Alibaba, Tencent et Xiaomi) en Chine.
[25] Isabelle Guibert, Frédéric Jeannin (2018), op.cit. p.1

I. REGLEMENTATIONS ETATIQUES SUR LE CONTROLE DE LA DONNEE

A l'ère de l'économie numérique, la donnée est plus que jamais un enjeu stratégique économique, politique et sociétal. A cet égard, les Etats entendent y étendre leur souveraineté par le droit. Dans les faits, il s'agit pour chaque entité étatique d'assurer la pleine applicabilité de son droit dès lors que les données appartiennent à son ressortissant. Dès lors, il convient à présent de s'interroger sur les réglementations étatiques en Europe (A) et dans le reste du monde (B).

A. LA SITUATION EN EUROPE

Dans un souci d'assurer une meilleure protection des données des citoyens européens[26] et à la suite des révélations Snowden en 2013[27], l'Union Européenne (UE) a adopté le 27 avril 2016 le règlement n°2016/679 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. Couramment appelé règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), ce texte est entré en vigueur le 25 mai 2016, et est applicable directement au sein des pays membres de l'union depuis le 25 mai 2018. Pour le législateur européen, l'objectif affiché s'articule autour de trois piliers, comme le relève si bien l'avocat et docteur en droit Olivier de Maison Rouge, à savoir : *« la consolidation des droits des personnes ; le renforcement de la coopération entre les autorités de protection des données ; et la responsabilisation des entités traitant des données à caractère personnel »*. Par ailleurs, pour ce dernier, ce nouvel instrument juridique est également *« (…) très clairement diriger contre les géants de l'économie numérique[28] »*. En filigrane, il faut notamment voir ici les GAFAM, qui ont accès toujours selon juriste, *« (…) à près de 90 % des données collectées dans le monde[29] »*.

Ayant donc vocation à harmoniser les règles de protection des données au sein de l'UE, il convient à chaque Etat membre d'adapter ces nouvelles dispositions dans leur ordre interne. Avant

[26] *« En matière de protection des données, comme dans beaucoup d'autres domaines, le niveau européen constitue un niveau d'intégration à la fois efficace et pertinent. A l'ère numérique, l'enjeu est d'assurer un contrôle territorialisé d'un phénomène par nature déterritorialisé ».* Alain Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*, Larcier, 2014, p.21

[27] T.d.L, *Tout comprendre à l'affaire Snowden*, Le Parisien, 5 novembre 2017

[28] Olivier de Maison Rouge (2018), pp. 5-76

[29] *Ibid*. p.3

de présenter la transposition du RDPG en droit local (2), une présentation du régime de protection dudit règlement s'impose (1).

1. Régime général de protection des données instauré par le RGPD

Seront abordés ici la question du champ d'application territorial du RGPD, le traitement des données, leurs transferts hors de l'UE, ainsi que les exigences de sécurité et de responsabilité des opérateurs.

Concernant la question du champ d'application territoriale du RGPD celui -ci a une emprise non seulement sur l'ensemble du territoire de l'UE, mais aussi sur le public ciblé par le traitement[30]. Dans ce sens, de l'article 3 du règlement dispose que :

1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :*

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

3. *Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.*

En d'autres termes, l'application du RGPD dépasse les frontières, dans la mesure où, il pourra s'appliquer à l'égard de sociétés basées dans des pays tiers. En ce sens, il s'agit alors d'une « loi »

[30] En effet, *« (…) si une société américaine, qui n'a aucun établissement en Union européenne, effectue du traitement de données personnelles sur des personnes situées en France ou dans un pays de l'UE, alors elle devra respecter les obligations du RGPD ».* SVP, *RDPG : Les dispositions particulières à l'international*, 2 avril 2019, p.4

extraterritoriale[31] qui traduit la volonté de l'UE de s'assurer une souveraineté par le droit des données personnelles de ses citoyens.

S'agissant à présent du traitement des données, il ressort de l'article 2.1 que *« le règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »*[32]. L'article 4.1 va plus loin en définissant les données à caractère personnel comme : *« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »*[33].

l'alinéa 2 du même article définit quant à lui le traitement comme : *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».*

A noter qu'en amont dudit traitement, une exigence du consentement (article 4 du RDPG)[34] des personnes concernées est nécessaire, aussi bien pour les personnes majeurs que pour les mineurs de seize ans (article 8 du RGPD).

Pour ce qui est du transfert des données hors de l'UE, le principe est qu'il est interdit de transférer des données personnelles à destination d'Etats non membre de l'Union européenne. Cependant, ce principe souffre de trois exceptions[35] :

---

[31] L'extraterritorialité est *« l'application du droit national d'un Etat en dehors de son territoire et réciproquement c'est, pour un pays, laisser s'exercer l'autorité d'un État étranger sur une partie de son territoire ».* Glossaire international sur la définition de l'extraterritorialité.

[32] Cf. les alinéas 2 et 3 pour les limites du Champ d'application matériel.

[33] A signaler que l'article 9 du règlement énonce un certain nombre de données à caractère personnel qui ne peuvent faire l'objet de traitement.

[34] Le consentement de la personne concernée est défini comme : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».*

[35] SVP, op.cit. p.6

- *Le transfert sera possible si le pays tiers bénéficie d'un niveau de protection adéquat [36] ;*
- *Le transfert sera possible s'il est effectué avec des garanties appropriées.*
- *Enfin, certaines situations particulières permettent de déroger à l'interdiction de principe : en effet, si la personne concernée a donné son consentement de manière explicite (par exemple, un salarié muté à l'étranger), ou encore si le transfert est nécessaire à la sauvegarde de la vie de cette personne, à la sauvegarde de l'intérêt public etc. Dans ces cas précis, le transfert de données dans un pays hors UE sera possible.*

En ce qui concerne enfin les exigences de sécurité des données et des sanctions en cas de manquement de la part des entreprises, le RGPD est beaucoup plus ferme par rapport à la directive 95/46/CE qu'elle abroge. Ainsi, le règlement impose que la sécurité soit assurée aussi bien par le responsable du traitement que par le sous-traitant (article 26). En ce sens, il introduit une nouvelle exigence qu'est la « résilience constante des systèmes et des services de traitement ». A cet effet, ces derniers doivent assurer une protection des données dès la conception et une protection des données par défaut (article 25). Selon Olivier de Maison Rouge, l'obligation de protection dès la conception *(privacy by design) « fait peser sur les fabricants de produits, les prestataires de services et les producteurs d'application l'obligation de prendre en compte la protection des données à caractère personnel et l'exigence de sécurité dès l'élaboration, la conception, la sélection et l'utilisation de produits, de services et d'applications impliquant le traitement de données »*. Et de poursuivre, *« le principe du Privacy by default [protection des données par défaut] implique du responsable du traitement la mise en place de mesures techniques et organisationnelles dont l'objectif est de garantir, par défaut et sans l'intervention de la personne concernée, la limitation de l'accessibilité des données à caractère personnel à un nombre déterminé de personnes »*[37]. De plus, le règlement impose également aux responsables de traitement et aux sous-traitants à notifier à l'autorité de contrôle et à la personne concernée toute violation de données à caractère personnel (article 33 et 34).

Relativement aux sanctions, celles-ci sont fortement renforcées en cas de non-conformité. Pour les manquements les plus graves, l'amende peut monter jusqu'à 4 % du chiffre d'affaires mondial s'agissant des entreprises ou 20 millions d'euros (article 83).

Quid à présent de la transposition du RGPD en droit local ?

[36] Cette adéquation peut être le fait soit d'une décision adoptée la Commission Européenne ou par une autorité de contrôle nationale. A ce jour, 12 pays dans le monde bénéficient parmi lesquels : Andorre, Argentine, Canada, îles Féroé, Guernesey, Israël, île de Man, Jersey, Nouvelle-Zélande, Suisse, Uruguay et États-Unis.
[37] Olivier de Maison Rouge (2018), op.cit. pp. 84-86

2. La transposition du RGPD en droit local

En ce qu'il modifie substantiellement les règles applicables en matière de protection des données et des droits des personnes concernées, l'ensemble des pays membres de l'UE ont dû adapter leur législation interne pour se conformer au RGPD[38].

Seront donc successivement présentés ici et de manière succincte le corpus législatif encadrant les données personnelles dans quelques pays en Europe (la France, l'Allemagne, la Belgique, le Royaume-Uni et la Suisse) ainsi que leurs organes de régulation.

En France

Dans l'Hexagone le règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 a été transposé au travers de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles afin de modifier la loi « Informatique et libertés » de 1978.

L'autorité de contrôle est la Commission Nationale de l'Informatique et des Libertés (CNIL)[39], dont la mission est de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.

En Allemagne

L'Allemagne a été le premier pays à adapter sa législation nationale sur la protection des données à caractère personnel à travers la nouvelle loi fédérale allemande sur la protection des données, promulguée le 5 juillet 2017 et est entrée en vigueur le 25 mai 2018, soit à la même date que l'entrée en vigueur du RGPD.

L'équivalent de la CNIL française en Allemagne est la Bundesdatenschutzgesetz qui joue quasiment le même rôle outre-Rhin.

[38] A noter ici que la transposition dans les droits nationaux n'est pas nécessaire ; puisque le règlement s'applique directement en leur sein et que chaque Etat est libre de faire ou non. Néanmoins les Etats le font pour calibrer le texte à leur contexte socioéconomique ; ce qui n'est pas sans poser quelques spécificités locales. SVP (2019) op.cit. p.7

[39] La CNIL a été créée par la loi Informatique et Libertés du 6 janvier 1978.

En Belgique

Le texte adaptant localement le RGPD en Belgique est la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 30 juillet 2018 et publiée le 5 septembre 2018 au Moniteur Belge.

L'organe de contrôle chargé de veiller au respect des principes fondamentaux de la protection des données à caractère personnel dans le pays est l'Autorité de protection des données[40].

Au Royaume-Uni

Le cas du Royaume-Uni est particulier, car le pays a entamé en 23 juin 2016 à la suite d'un référendum sa sortie de l'UE. Néanmoins, le pays n'est pas en reste sur la transposition du RDPG à travers la Data Protection Act 2018 du 23 mai 2018 est entré en vigueur le 25 mai 2018.

L'organe responsable du contrôle outre-Atlantique est l'Information Commissioner's Office**.** Son principal rôle est notamment de pour promouvoir l'accès aux informations officielles et protéger les données personnelles.

En Suisse

En Suisse, la principale loi sur la protection des données est la loi fédérale sur la protection des données de 1992. Cependant, en vertu de l'accord Schengen, le pays s'est vu dans l'obligation d'arrimer sa législation sur la protection des données par rapport au règlement (UE) n°2016/679 et la directive (UE) n°2016/680 relative à la protection des données dans le cadre des poursuites pénales. La nouvelle mouture devrait entrer en vigueur courant 2020[41]. Pour certains, derrière cette conformité, la suisse entend bénéficier de *« (…) la portée extraterritoriale du Règlement d'une part et de la question du statut de pays équivalent »*[42].

L'organe national en charge de faire respecter la protection des données dans le pays est le Conseil Fédéral Suisse.

[40] Depuis l'entrée en vigueur du RDPG soit le 25 mai 2018, l'APD à remplacer la Commission de la protection de la vie privée.
[41] Isabelle Guibert, Frédéric Jeannin (2018), *op.cit.* p. 31
[42] *Ibid.*

En somme, si les pays européens semblent bien équipés en matière de protection des données ; ce qui leur permet de revendiquer une souveraineté par le droit sur ces derniers, fort est de constater qu'ailleurs dans le monde excepter quelques pays, ce n'est pas le cas.

B. LA SITUATION DANS LE RESTE DU MONDE

Selon la CNUCED, 58 % des pays hors UE ont une loi sur la protection des données à l'image du RDPG, contre 10 % en cours de rédaction d'un projet de loi. Les 32 % restant n'ont aucune loi[43]. De son côté la CNIL dresse une carte actualisée permettant de visualiser les différents niveaux de protection des données des pays dans le monde *(annexe 2 p.31).* Dans ce contexte, nous présenterons dans un premier temps le *Cross-Border Privacy Rules System* (CBPR) applicable au sein de certains Etats membres de l'*Asia Pacific Economic Cooperation* (APEC)[44] (1), avant de nous attarder sur le cadre réglementaire aux Etats-Unis, en Chine, en Russie, au Brésil ainsi que de manière générale de l'Afrique et de l'Océanie (2).

1. Le Cross-Border Privacy Rules System

Le CBPR de l'APEC est *« une certification de confidentialité des données garantie par le gouvernement, à laquelle les entreprises peuvent adhérer pour démontrer leur conformité aux mesures de protection des données reconnues à l'échelle internationale »*[45]. Pour l'APEC, il s'agit de veiller à ce que les différences de réglementation ne nuisent pas à la capacité des entreprises de fournir des produits et des services innovants. En cela donc, le système CBPR permet aux entreprises et aux gouvernements qui travaillent ensemble de s'assurer que, lorsque des renseignements personnels traversent les frontières, qu'ils soient protégés conformément aux normes prescrites par les exigences du programme du système et qu'ils sont exécutoires dans toutes les juridictions participantes. En d'autres termes, il s'agit d'une passerelle de protection de données personnelles au sein des pays membres l'APEC. Pour intégrer ce système, un Etat membre de l'APEC doit démontrer qu'il peut faire respecter les exigences du système CBPR. A ce jour, huit

[43] Lauriane Hauchard, *Protection de données personnelles : bilan de l'année écoulée et perspective pour l'année 2019*, Le Petit Juriste, 17 avril 219

[44] L'APEC est un forum économique intergouvernemental visant à faciliter la croissance économique, la coopération, les échanges et l'investissement de la région Asie Pacifique.

[45] APEC, *What is the Cross-Border Privacy Rules System?*

(Canada, les États-Unis, le Japon, la République de Corée, le Mexique et Singapour, l'Australie et Taiwan) des 21 pays que compte l'APEC sont membres de ce système de protection.

Pour certains, *« si le CBPR reste encore embryonnaire, il conviendra de suivre de près ses travaux, car une adoption active par la Chine pourrait impliquer un déplacement du centre de gravité de la doctrine de protection des données vers l'Asie »*[46].

2. Panorama des législations nationales sur la protection des données dans le monde

Nous verrons ici successivement le cas des Etats-Unis, de la Chine, de la Russie, du Brésil, de l'Afrique et de l'Océanie.

Les Etats-Unis

Aux Etats-Unis, pays des GAFAM, plusieurs textes législatifs encadrent la collecte et le traitement des données des citoyens[47]. De manière non exhaustive on peut mentionner, le *Priacy Act* de 1974, l'*Electronic Communication Privacy Act* de 1986, *USA Freedom Act* de 2015, *Email Privacy Act de 2017,* et dans une certaine mesure le *Privacy Shield* de 2016[48] et plus récemment le *Clarifying Lawful Overseas Use of Data Act* dit *CLOUD Act* de 2018.

Parmi ces lois, celle qui marque vraiment la volonté des américains à contrôler les données au-delà de ses frontières est le *CLOUD Act*, qui permet aux autorités judiciaires d'ordonner la communication de données dans le cadre d'enquêtes criminelles même si celles-ci sont stockées à l'étranger. Selon Winston Maxwell, Associé chez Hogan Lovells *« La nouvelle loi précise que la localisation physique des données n'est pas un critère pertinent dans la délivrance des réquisitions*[49] *»*. Concrètement donc, il s'agit d'une loi extraterritoriale à l'image du RDPG dont elle n'est pas forcément en contradiction[50].

[46] Isabelle Guibert, Frédéric Jeannin (2018), *op.cit.* p.20
[47] Ibid. p.115 - 116
[48] La particularité du *Privacy Shield* applicable depuis le 1er août 2016, est qu'il s'agit *« d'un système bilatéral de protection de la vie privée entre l'Union européenne et les Etats-Unis d'une part, la Suisse et les Etats-Unis d'autre part (…) pour fournir aux entreprises des deux côtés de l'Atlantique un mécanisme de conformité en matière de protection lors du transfert de données personnelles ».* Isabelle Guibert, Frédéric Jeannin (2018), *op.cit.* p. 17
[49] Maxwell Winston, *Le cloud act américain ne permet pas d'espionner les entreprises européennes*, Eurocloud
[50] Maxwell Winston ibid.

Prospectivement, il convient de signaler que le sénateur américain Marco Rubio a déposé un projet de loi pour la création d'un règlement fédéral sur la collecte de données au début de l'année 2019. Intitulé *American Data Dissemination Act*, il remplacerait les réglementations en vigueur dans les États.

Enfin, contrairement à ce que l'on pourrait croire, les Etats-Unis sont étonnement dépourvus de régulateur au niveau fédéral. Cependant, la quasi-totalité des Etats requièrent une déclaration d'incident.

La Chine

D'après Lauriane Hauchard, *« (...) l'administration de Xi Jinping souhaite devenir un « Cyber superpower » en développant des standards juridiques made in China destinés à s'exporter à l'étranger*[51] *»*. C'est donc en toute logique qu'est entrée vigueur en mai 2018 le *Personal Information Security Specification* concomitamment que le RGPD dans l'UE. En effet, cette loi vient actualiser la *Cyber Security Law*, en mettant en exergue l'obligation d'une spécification des catégories de données personnelles collectées. Dès lors, pour assurer un contrôle ou mieux la souveraineté des données de ses 829 millions d'internautes[52], la loi stipule que *« les informations personnelles et les données importantes des citoyens chinois doivent être stockées sur des serveurs au sein du pays*[53] *»*.

La Russie

En Russie, la protection des données personnelles est notamment régie par la loi fédérale ("N 242-FZ") portant sur la protection des données personnelles des citoyens russes. Adopté en juillet 2014, ce texte oblige les entreprises étrangères à localiser sur le territoire national le stockage et le traitement des données personnelles appartenant aux ressortissants russes. Pour la fédération de Russie, l'objectif affiché est similaire à celui de la Chine dans la mesure où l'enjeu est de garantir sa souveraineté sur les données de ses citoyens.

[51] Lauriane Hauchard (2019), *op.cit*
[52] Selon un rapport publié le 28 février par le Centre d'information du réseau Internet de Chine (CNNIC), le nombre d'internautes chinois s'élevait à 829 millions, dont 871 millions en téléphonie mobile, soit 98,6% du nombre total d'internautes.
[53] Isabelle Guibert, Frédéric Jeannin, i*bid* p.128

L'équivalent CNIL en Russie est le Service fédéral de supervision des communications, des technologies de l'information et des médias de masse (Roskomnadzor).

Le Brésil

Le « RGPD brésilien » est la loi n° 13.709 du 14 août 2018 sur la protection des données, qui sera applicable en février 2020. Cette loi vise à réguler le traitement des données personnelles, contrôler et responsabiliser les acteurs qui traitent des données personnelles, et protéger la vie privée des individus. Elle prévoit également une autorité de contrôle dédiée (Autorité Nationale de Protection des Données) qui aura des missions similaires à celles de la CNIL française[54].

Le point en Afrique

En Afrique, la protection des données constitue également un grand enjeu, puisque les pays africains abritent 435 millions d'utilisateurs d'Internet, pour 191 millions utilisateurs des réseaux sociaux, selon le Digital Report 2018 de We Are Social et Hootsuite.

A ce jour, seul 23 pays africains sur 54 disposent une législation nationale sur la protection des données. A titre d'exemple, on peut citer le Bénin, le Burkina Faso, la Côte d'Ivoire, le Gabon, le Mali, le Maroc, la Tunisie, l'Algérie et l'Egypte[55].

A ces réglementations nationales, il faudrait également rajouter l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) créée en 2007 à Montréal pour coordonner la réglementation applicable dans les pays francophones. Cette démarche interrégionale traduit à l'évidence la volonté des certains pays africains d'harmoniser leur réglementation afin de mieux marquer leur souveraineté sur les données.

[54] Hélène Legras, *La loi brésilienne 13.709 du 14 août 2018 sur la protection des données (LGPD) applicable en Février 2020*, Association Data Protection Officers, 20 novembre 2018
[55] Lauriane Hauchard (2019), *op.cit.*

Le point en Océanie

Dans cette région du monde, la judiciarisation des données personnelles comme moyen de protection et contrôle est également mise en place, notamment en Australie et en Nouvelle-Zélande depuis respectivement les années 80 et 90.

Comme le souligne Lauriane Hauchard à propos de l'Australie, *« en sus des lois gouvernementales de ses Etats, possède une loi fédérale datant de 1989, modifiée à deux reprises, un régime obligatoire de notification des atteintes à la vie privée a été introduit par un projet de loi fédérale de 2017, entré en vigueur depuis février 2018*[56] *»*. Par ailleurs, le pays n'est pas reconnu comme adéquat par l'UE, bien qu'il dispose d'une autorité nationale de protection des données[57] reconnue elle par la conférence internationale des commissaires à la protection de la vie privée et des données personnelles.

Du côté de la Nouvelle-Zélande, la protection des données repose essentiellement sur le Privacy Act 1993 en cours d'actualisation depuis le dépôt d'un projet de loi au Parlement en 2018. Contrairement à l'Australie, le pays bénéficie d'une décision d'adéquation de la Commission européenne ; ce qui signifie que le transfert de données personnelles vers la Nouvelle-Zélande ne nécessite pas d'encadrement par les outils de transfert. L'autorité nationale de protection des données est l'*Office of the Privacy Commissioner*.

II. CLASSIFATION ET PRORIETE DE LA DONNEE

À l'heure de la collecte massive des données tout azimut sur le *Web*, il convient de s'interroger sur la propriété réelle de celles-ci (B). Mais avant, quelle est le contenu de la donnée ? Mieux, comment classifie-t-on les données ? (A).

A. CLASSIFICATION DES DONNES

Compte tenu de l'intérêt que suscitent aujourd'hui les données pour les Etats, ceux-ci à travers leurs différentes réglementations ont classifié les données afin de pouvoir mieux les appréhender

[56] Lauriane Hauchard (2019), *op.cit.*
[57] Il s'agit de l'*Office of the Austranlian Information Commissionner*

et les protéger. Dans cet esprit et en nous appuyant sur l'approche française, on peut classer les données dans huit catégories en fonction de leur famille juridique, selon Olivier de Maison Rouge [58]. Ainsi, on a :

- Les données de nature militaire ;
- Les données personnelles ;
- Les données médicales relatives au patient ;
- Les données de recherche, données stratégiques et techniques ;
- Les secrets d'affaires, savoir-faire, données confidentielles ;
- Les données stratégiques sur support numérique ;
- Les données numériques essentielles ;
- Et les informations autres que personnelles.

A travers cette classification, fort est de constater que les données sur lesquelles les Etats veulent absolument avoir le contrôle par le droit sont les données à caractère personnel. Les autres types de données étant ici déjà de facto sous l'emprise de chaque nation ou des entreprises privées.

Par conséquent, ce que l'on qualifie souvent d'or noir du XXI^{e} siècle sont avant tout les données à caractère personnel (1) et dans une certaine mesure les données publiques (2).

1. Les données à caractère personnel

Quand on parle de données à caractère personnel *(annexe 3 p.32)*, il s'agit laconiquement de toutes données permettant d'identifier directement ou indirectement une personne, même dans le cadre de sa vie professionnelle[59].

Identification directe

Selon que les données permettent d'identifier directement une personne sur une base de données ou un document papier, c'est-à-dire des données contenant toutes les informations

[58] Olivier de Maison Rouge (2018), *op.cit.* p. 73-74
[59] Cabinet Koc, *RGPD : Les données professionnelles sont-elles des données personnelles ?* LinkedIn, 28 septembre 2018

précises d'identification, il peut s'agir par exemple : d'une fiche client ; d'une fiche de paye, d'un relevé d'identité bancaire, d'un dossier médical, d'un CV, d'une facture ou un devis.

Identification indirecte

Quant aux données qui permettent d'identifier indirectement un individu, il peut s'agir soit des données nécessitant un croisement avec d'autres sources de données pour arriver à cette fin, soit alors des données comportementales rattachées à un profil d'utilisateur.

Dans le premier cas, on peut citer[60] :

- Un numéro de téléphone parce qu'il permet de *« retrouver le nom et l'adresse d'un citoyen, par le biais d'un annuaire téléphonique » ;*
- Une plaque d'immatriculation parce qu'elle permet de *« trouver le nom et l'adresse d'un citoyen, par le biais du fichier des cartes grises » ;*
- Un numéro de sécurité sociale parce qu'il permet de *« retrouver les coordonnées et le dossier médical du citoyen par le biais du fichier de la sécurité sociale » ;*
- Une adresse mail parce qu'elle *« peut être utilisée sur un simple moteur de recherche pour retrouver la personne concernée » ;*
- Une adresse IP parce qu'elle peut *« permet de remonter jusqu'à l'adresse de l'utilisateur en passant par le fichier de l'opérateur ».*

Parmi cette liste non exhaustive de données personnelles, il convient de préciser que certaines plus que d'autres ont un caractère « privé » parce que tenant au respect de la vie privée. Rentre notamment dans cette catégorie, les données concernant la santé[61] comme les données génétiques[62] ; et les données biométriques[63].

En ce qui concerne le second cas, en l'occurrence les données comportementales qui sont rattachées à un profil d'utilisateur, il s'agit bien souvent des informations au sujet de l'activité

[60] Thomas-Jérôme Bouche, Qu'est-ce qu'une donnée à caractère personnel – donnée personnelle ?

[61] Selon l'article 3.14 du RDPG, on attend par données concernant la santé, *« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».*

[62] D'après l'article 3.12 du RDPG, les données génétiques sont des *« données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ».*

[63] Il ressort de l'article 3.13 du RDPG que les données biométriques sont des *« données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».*

de ce dernier dans l'espace numérique. Dans la pratique, celles-ci sont collectées via de multiples démarches[64]. En effet, dès lors qu'une personne crée un profil sur le *Web*, s'y rattache indirectement à son profil toutes ses activités. Sur un site de vente en ligne par exemple, ses activités peuvent être la fréquence de connexion, le type de vêtements achetés ou encore le navigateur utilisé. Sur un réseau social, on aurait en plus de ceux précédemment cités, notre cercle d'ami, les personnes ou les pages que l'on suit, les *likes*¸ etc. En résumé, les données à caractère personnel *« (…) s'appliquent également aux informations susceptibles d'avoir une influence manifeste sur la manière dont une personne physique est traitée ou évaluée »*[65]. A ce propos, l'entreprise de Mark Zuckerberg a récemment lancé sur sa plateforme, « *Off-Facebook Activity* », une fonctionnalité qui permet de déconnecter votre activité Facebook de votre navigation sur des sites tiers[66].

2. Les données publiques

La notion de « donnée publique » renvoie à l'ensemble des informations accessibles au public et qui sont produites ou collectées par un État, une collectivité territoriale, un organe parapublic, dans le cadre de leurs activités de service public[67]. Or comme le relève à juste titre Maximilien Lanna, Doctorant à l'Université de Paris II Panthéon-Assas (CERSA), chercheur assistant de la chaire Mutations de l'action publique et du droit public, Sciences-Po, ces données publiques *« (…) peuvent ainsi être amenées à contenir des données personnelles. La frontière entre les différentes catégories de données, publiques ou personnelles, anonymes ou identifiantes,*

[64] Léger Lucas, Landreau Isabelle, Peliks Gérard, Binctin Nicolas, Pez-Pérard Virginie (2018), *Mes data sont à moi : Pour une patrimonialité des données personnelles*, Mailedit, janvier 2018, pp.28-34

[65] Groupe de travail « artiCle 29 » sur la proteCtion des données, 20 juin 2007, Avis 4/2007 *sur le concept de données à caractère personnel*. *In* Arnaud Anciaux, Joëlle Farchy, Cécile Méadel. *L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable*, Revue d'économie industrielle, vol. 158, no. 2, 2017, pp.12

[66] Marion Simon-Rainaud, *Comment Facebook veut vous « redonner le contrôle » avec son nouvel outil de gestion des données*, O1net, 21 août 2019. Selon l'auteur, *« L'objectif est d'être totalement transparent sur comment les entreprises utilisent les informations des utilisateurs grâce aux outils professionnels du réseau mis à leur disposition (pixel Facebook ou Facebook Log par exemple) ».*

[67] En France, la loi n° 78-753 du 17 juillet 1978 relative au droit d'accès aux documents administratifs, les définit en son article 1er : *« (…) quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes-rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions. (…) ».*

n'étant pas toujours clairement établie (…) »[68]. Ainsi, pour donc protéger les individus contre les risques de divulgation d'informations nominatives dans certaines situations, des mesures comme l'anonymisation, sont souvent prises à cet effet.

Ainsi identifiées et classées, fort est de reconnaitre que les données représentent un enjeu économique certain de la part des entreprises du numérique. A partir de ce constat, à qui appartiennent-elles réellement ? Derrière cette question, se soulève la question de la propriété de la donnée.

B. PROPRIETE DE LA DONNEE

Se poser la question de la propriété de la donnée, c'est en réalité s'interroger sur le droit qu'à une personne sur ses données. En d'autres termes, un individu peut-il en disposer comme il l'entend à l'instar d'un bien classique ?

En effet, c'est face d'une part à la surveillance massive et parfois abusive des Etats au prétexte de garantir la sécurité de leurs citoyens et d'autre part à la marchandisation des données personnelles par les entreprises du numérique, que l'idée de patrimonialisation trouve son origine. Si la plupart des lois définissent et encadrent la problématique de la surveillance des citoyens par les Etats, il n'en va pas de même de la marchandisation qui découlerait d'un droit de propriété pour la personne en amont. Dès lors l'enjeu de titularité de la donnée tient aux nombreux revenus qui peuvent en être tirés.

En droit français par exemple et comme dans beaucoup d'autres Etats, le droit[69] autour des données personnelles s'est avant tout construit autour *« (…) d'une volonté de protection des personnes, de leurs droits fondamentaux et de leur vie privée, et non dans une logique patrimoniale. [Parce que] créé dans un contexte où il s'agissait surtout de protéger les citoyens de la collecte de données par les administrations et de leur fichage, [il doit aujourd'hui s'adapter] à l'essor de pratiques marchandes et à la volonté des acteurs qui souhaitent construire tout ou partie de leur activité économique autour de l'exploitation de ces données personnelles »*[70].

[68] Lanna, Maximilien, *Données publiques et protection des données personnelles : le cadre européen*, Revue française d'administration publique, vol. 167, no. 3, 2018, pp.502
[69] La loi dite informatique et libertés de 1978
[70] Anciaux, Arnaud, Joëlle Farchy, Cécile Méadel (2017), op.cit. p 10.

Avec donc l'essor commercial lié à l'exploitation des données personnelles à la fin des années 1990, l'idée d'un droit de propriété a émergé permettant à toute personne d'être propriétaire des droits d'exploitation commerciale des renseignements le concernant[71]. Or dans les faits, l'internaute fournit généralement sans contrepartie financière - via les conditions générales d'utilisation[72] *(annexe 4 p.33)* - aux plateformes numériques leurs données aux fin de traitement, d'exploitation, voire de vente à des partenaires cherchant à toucher les consommateurs par des publicités. De plus, ces données sont aussi indispensables à ces plateformes dans la mesure où, elles améliorent leurs services et participent à conserver leur position sur les marchés[73]. Bien que parfois, les utilisateurs en tirent directement des bénéfices monétaires via notamment les cartes de fidélité, cette rétribution reste encore très faible par rapport aux gains considérables qu'engrangent les plateformes numériques.

A ce propos, plusieurs modèles de rétribution du citoyen sur ses données personnelles ont vu le jour. Ceux-ci partent du postulat qu'il est communément admis qu'une donnée personnelle est un bien meuble incorporel[74], et en tant que tel, confère à son titulaire le droit d'user (usus), de profiter (fructus) et de disposer (abusus) de la manière la plus absolue[75]. A titre d'exemple on peut citer ici, le contrat de licence de marque et le droit de suite cher au droit d'auteur[76].

C'est donc en tenant compte de ces débats doctrinaux autour de la titularisation des données personnelles que s'est construit et continue d'évoluer les réglementations étatiques en la matière. Aux Etats-Unis par exemple, l'idée de droit de propriété sur les données personnelles trouve un écho plus favorable contrairement à l'Europe.

---

[71] Nathalie Mallet-Poujol, Appropriation *de l'information : l'éternelle chimère*, *Recueil Dalloz*, 1997, p. 330

[72] Les conditions générales d'utilisation que l'on accepte avant d'utiliser un service sue Web, constituent pour le moment l'acte juridique qui permet aux entreprises du numérique de jouir des données personnelles. Pour beaucoup, il s'agit d'un contrat léonin, qui ne permet pas un consentement éclairé.

[73] En effet, outre à la logique mercantile, les entreprises peuvent utiliser ces données pour *« (…) conserver les produits mis au panier lors d'une précédente visite par exemple, ou recommander des produits en fonction du profil du consommateur ou de ses achats précédents. Elles peuvent ainsi proposer aux utilisateurs des expériences fluides, simples et pratiques. De fait, même s'ils n'en sont pas toujours conscients, les consommateurs retirent de l'utilisation de leurs informations personnelles des bénéfices fonctionnels (gain de temps, confort, bénéfices de commodité) »*. Lucas Léger, Isabelle Landreau, Gérard Peliks, Nicolas Binctin, Virginie Pez-Pérard (2018), op.cit. p. 27

[74] Fabrice Mattatia et Morgane Yaïche, *Etre propriétaire de ses données personnelles : peut-on recourir au régime traditionnel de propriété ? Revue Lamy de droit immatériel*, 2015/114, pp60-63

[75] *« La donnée appartient à celui qui la fournit (conception classique) et le business model doit se fonder sur le premier fournisseur de donnée : le citoyen, qui sera rétribué sur la plus-value produite par la donnée, qu'elle soit première, générée ou agrégée »*. Lucas Léger, Isabelle Landreau, Gérard Peliks, Nicolas Binctin, Virginie Pez-Pérard (2018), ibid. pp.87

[76] Lucas Léger, Isabelle Landreau, Gérard Peliks, Nicolas Binctin, Virginie Pez-Pérard (2018) *ibid.* pp. 89-91

Outre Atlantique les données personnelles sont en effet davantage considérées comme appartenant à son propriétaire et donc pouvant être cédées par celui-ci à une plateforme numérique moyennant son consentement[77]. C'est dans ce sens que se multiplient les *databrokers* (les courtiers de données) tels qu'ACXIOM ou BLUEKAI qui se positionnent comme intermédiaires afin de proposer aux internautes de monétiser leurs données. Pour aller encore plus loin, certains sénateurs américains tentent d'en fixer le prix à travers un projet de loi[78].

Au sein de l'UE, la position actuelle est contenue dans le RDPG qui, présente une alternative au droit de propriété à savoir une autodétermination informationnelle couplée à une logique de responsabilisation *(accountability) et* sanction des plateformes. En cela, l'autodétermination informationnelle est considérée comme « *permettant d'offrir une véritable protection des données personnelles, en prolongeant une protection construite autour de l'individu, en dehors de toute appropriation patrimoniale*[79] ». Par ailleurs, ces données conservent leur statut de biens aliénables pour la valeur qu'elle représente ainsi que pour leur circulation[80] au profit des plateformes numériques.

Dans le reste du monde, et à quelques exceptions près, l'approche choisit actuellement se rapproche plus de la position européenne qui, sans accordé la patrimonialisation des données personnelles aux citoyens, renforce d'une part leurs droits, responsabilise et sanctionne le cas échant les entreprises et d'autre part encadre leur exploitation par les entreprises.

[77] Anciaux Arnaud, Joëlle Farchy, Cécile Méadel (2017), op.cit. p. 18

[78] A ce sujet voir: Alyssa Newcomb, *How Much Is Your Data Worth to Facebook and Google ? A New Senate Bill Aims to Find Out*, 25 juin 2019

[79] Anciaux, Arnaud, Joëlle Farchy, Cécile Méadel (2017), op.cit. p.35. L'autodétermination informationnelle permet en ce sens, de renforcer le droit des individus comme le droit à l'oubli numérique et le droit à la portabilité des données. En effet, le droit à l'oubli numérique permet aux utilisateurs d'un fournisseur de service de pouvoir transférer vers un autre les données le concernant au moyen d'une conception qui lie les données directement à la personne plus qu'à l'exploitant. Le droit à la portabilité permet quant à lui de diminuer les « barrières à la sortie » d'un service numérique.

[80] Judith Rochfeld, *Une nouvelle source en droit des contrats : la loi Informatique et libertés*, Revue des contrats, n° 1, pp. 119

CONCLUSION

La géopolitique des Etats intègre désormais un nouvel espace de conquête qu'est le cyberespace. Pour assurer leur ascendant sur cet espace stratégique, les Etats recourent au droit ; ce qui implique une identification préalable des données (classification) tout en identifiant leurs propriétaires effectifs. En ce sens, les réglementations étatiques en la matière se multiplient depuis quelques années, reflétant ainsi l'intérêt économique et sociétal que suscitent les données. Néanmoins, disposer d'une souveraineté numérique nécessite de contrôler également les deux autres composantes essentielles de cet espace que sont les réseaux et les applications. En effet, dans cet espace, *« (…) une stratégie - verticale - qui tenterait de conserver des pans de souveraineté dans un secteur entier sans intégrer une vision fonctionnelle globale de nature systémique serait vouée à l'échec*[81] *».*

Dès lors, cette souveraineté peut être totale ou partielle. Comme le soulignent Germain Grégoire et Paul Massart, la souveraineté totale est aujourd'hui incarnée par les Etats-Unis. Selon eux en effet, *« seuls les États-Unis disposent aujourd'hui de cette capacité hégémonique et dominent presque tous les compartiments du terrain* [82] *».* En ce sens, Olivier de Maison Rouge parle de « colonisation du net » et énumère quelques chiffres qui sont révélateurs et montrent l'écart déjà constitué par les Etats-Unis dans la compétition numérique. Concrètement, *« 80 % des câbles de flux de données transitent par les Etats-Unis d'Amérique, les GAFAM ont accès à près de 90 % des données collectées dans le monde, et aspirent 30 % des connexions, leur chiffre d'affaires cumulé aux Etats-Unis s'est élevé à 24 milliards de dollars, 90 % des données obtenues via le réseau d'espionnage électronique Echelon couvrent des informations de nature économique, enfin, des treize grands serveurs intercontinentaux - Racine -, neuf sont gérés par des Américains*[83] *».*

A contrario, les autres Etats disposeraient d'une souveraineté partielle, même si aujourd'hui la Chine essaie à travers les données de sa population, ses BATX et son réseau, de challenger cette position de leader des Etats-Unis. Du côté de la France par exemple, on peut noter une volonté de maintenir une part de souveraineté à travers la tentative de la mise en place d'un « cloud souverain[84] ». Plus globalement en Europe, des officiels européens poussent actuellement

[81] Germain Grégoire, Paul Massart (2017), op.cit. p.54
[82] Ibid. p.55
[83] Olivier de Maison Rouge (2018), op.cit. p.3
[84] Emmanuelle Ducros, *Données numériques : la souveraineté européenne à vau-l'eau*, l'Opinion, 25 février 2019

la future présidente de la Commission, Ursula von der Leyen, a créé un fonds européen qui investirait plus de 100 milliards de dollars en participations dans des sociétés européennes à fort potentiel. L'enjeu serait alors de soutenir l'émergence de géants capables de donner le change aux grandes entreprises de la tech américaines et Chinoise[85].

Dès lors, dans un espace numérique toujours en mutation, les Etats disposant d'une souveraineté partielle gagneraient à rattraper leur retard là où ils en ont afin de garder une certaine indépendance. A défaut, ceux-ci plus que les autres doivent mettre en place une veille stratégique permanente en vue d'anticiper les futures ruptures technologiques et se positionner en leader dessus.

[85] Bjarke Smith-Meyer, Lili Bayer, Jakob Hanke, Ryan Heath, *European officials draft radical plan to take on Trump and U.S. tech companies*, Politico, 22 août 2019

BIBLIOGRAPHIE

Ouvrages

Boniface Pascal, La géopolitique, Éditions Eyrolles : 6e Ed, 2019

Defay Alexandre, *La géopolitique*, Que sais-je ? 4e éd. 2018

De Maison Rouge Olivier, Les cyberisques : la gestion juridique des risques à l'ère immatérielle, LexisNexis, 2018

Gauchon Pascal, Huissoud Jean-Marc, *Les 100 mots de la géopolitique*, Que sais-je ? 5e éd. 2019

Guibert Isabelle, Jeannin Frédéric, Les nouvelles frontières numériques : RGPD et politiques de protection des données, VA éditions, 2018

Grosjean Alain, Enjeux européens et mondiaux de la protection des données personnelles, Larcier, 2014

Kjellen Rudolf, *L'État comme forme de vie*, 1916

Nathalie Mallet-Poujol, *Appropriation de l'information : l'éternelle chimère*, Recueil Dalloz, 1997

Revelli Carlo, *intelligence stratégique sur internet,* 1998

Revues

Anciaux Arnaud, Farchy Joëlle, Méadel Cécile. *L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable*, Revue d'économie industrielle, vol. 158, n°2, 2017

Berthier Thierry, Kempf Olivier, Vers une géopolitique de la donnée, Annales des Mines - Réalités industrielles, vol. août 2016, n°3, 2016

Germain Grégoire, Paul Massart, Souveraineté numérique, Études, vol. octobre, n°10, 2017

Judith Rochfeld, Une nouvelle source en droit des contrats : la loi Informatique et libertés, Revue des contrats, n° 1

Massart Paul, Faut-il créer une nouvelle stratégie pour le cyberespace ? Revue de la Défense nationale, n° 757, février 2013

Maximilien Lanna, *Données publiques et protection des données personnelles : le cadre européen*, Revue française d'administration publique, vol. 167, no. 3, 2018, pp.502

Rapports

Léger Lucas, Landreau Isabelle, Peliks Gérard, Binctin Nicolas, Pez-Pérard Virginie, Mes data sont à moi : Pour une patrimonialité des données personnelles, Mailedit, janvier 2018

Peres Éric, *« Les Données numériques : un enjeu d'éducation et de citoyenneté »*, Les Avis du Conseil économique, social et environnemental, janvier 2015

Articles Web

APEC, *What is the Cross-Border Privacy Rules System?* https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

Bjarke Smith-Meyer, Lili Bayer, Jakob Hanke, Ryan Heath, *European officials draft radical plan to take on Trump and U.S. tech companies*, Politico, 22 août 2019. https://www.politico.com/story/2019/08/22/europe-plan-trump-tech-companies-1472326

Cabinet Koc, *RGPD : Les données professionnelles sont-elles des données personnelles* ? LinkedIn, 28 septembre 2018. https://www.linkedin.com/pulse/rgpd-les-donn%C3%A9es-professionnelles-sont-elles-des-personnelles-koc/

Ducros Emmanuelle, *Données numériques: la souveraineté européenne à vau-l'eau*, l'Opinion, 25 février 2019. https://www.lopinion.fr/edition/economie/donnees-numeriques-souverainete-europeenne-a-vau-l-eau-178970

Glossaire international sur la définition de l'extraterritorialité. https://www.glossaire-international.com/pages/tous-les-termes/extraterritorialite.html

Hauchard Lauriane, *Protection de données personnelles : bilan de l'année écoulée et perspective pour l'année 2019*, Le Petit Juriste, 17 avril 219. https://www.lepetitjuriste.fr/protection-de-donnees-personnelles-bilan-de-lannee-ecoulee-et-perspective-pour-lannee-2019/

Legras Hélène, *La loi brésilienne 13.709 du 14 août 2018 sur la protection des données (LGPD) applicable en Février 2020*, Association Data Protection Officers, 20 novembre 2018. https://www.data-protection-officer-association.eu/la-loi-bresilienne-13-709-du-14-aout-2018-sur-la-protection-des-donnees-lgpd-applicable-en-fevrier-2020/#targetText=La%20loi%20br%C3%A9silienne%20n%C2%B0,la%20vie%20priv%C3%A9e%20des%20individus.

Newcomb Alyssa, *How Much Is Your Data Worth to Facebook and Google? A New Senate Bill Aims to Find Out*, 25 juin 2019. https://finance.yahoo.com/news/much-data-worth-facebook-google-224956457.html

Leslie Saladin, *La souveraineté des données, pourquoi est-ce essentiel ?* Journal du net, 27 juin 2018. https://www.journaldunet.com/solutions/expert/69340/la-souverainete-des-donnees--pourquoi-est-ce-essentiel.shtml

Simon-Rainaud Marion, *Comment Facebook veut vous « redonner le contrôle» avec son nouvel outil de gestion des données*, O1net, 21 août 2019. https://www.01net.com/actualites/comment-facebook-veut-vous-redonner-le-controleavec-son-nouvel-outil-de-gestion-des-donnees-1753125.html

SVP, *RDPG : Les dispositions particulières à l'international*, Livre Blanc, 2 avril 2019

Thomas-Jérôme Bouche, *Qu'est-ce qu'une donnée à caractère personnel – donnée personnelle ?* https://dpoexpert.fr/donnee-a-caractere-personnel/

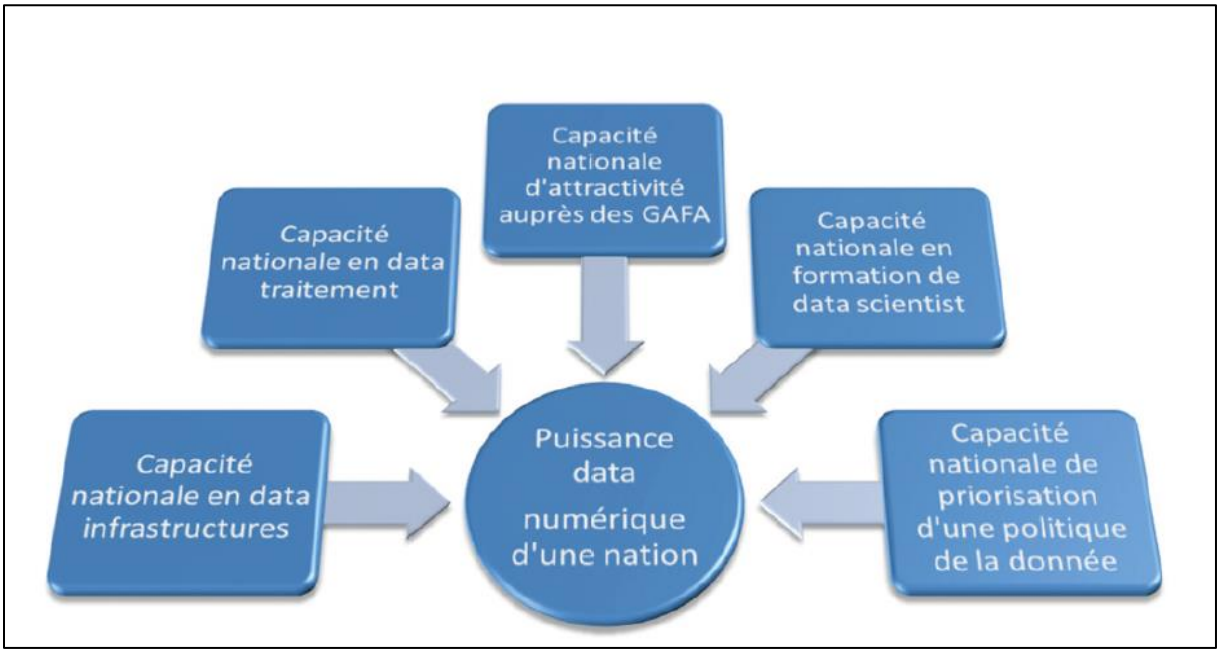
T.d.L, *Tout comprendre à l'affaire Snowden*, Leparisien, 5 novembre 2017. http://www.leparisien.fr/international/tout-comprendre-a-l-affaire-snowden-07-11-2017-7378926.php

Winston Maxwell, *Le cloud act américain ne permet pas d'espionner les entreprises européennes*, Eurocloud. https://www.eurocloud.fr/le-cloud-act-americain-ne-permet-pas-despionner-les-entreprises-europeennes/

ANNEXES

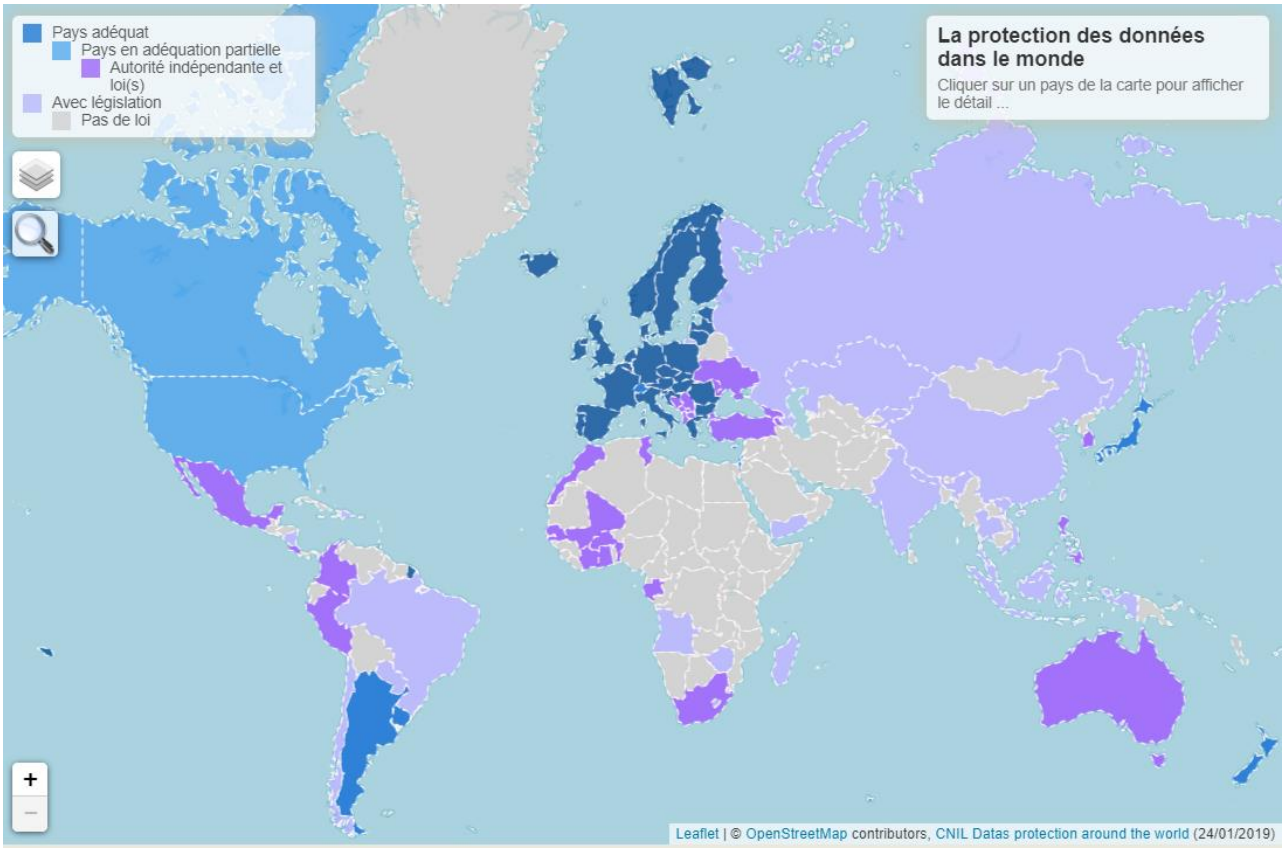
Schémas et graphiques

Annexe 1 : Les différents facteurs constitutifs de la puissance data-numérique d'une nation.



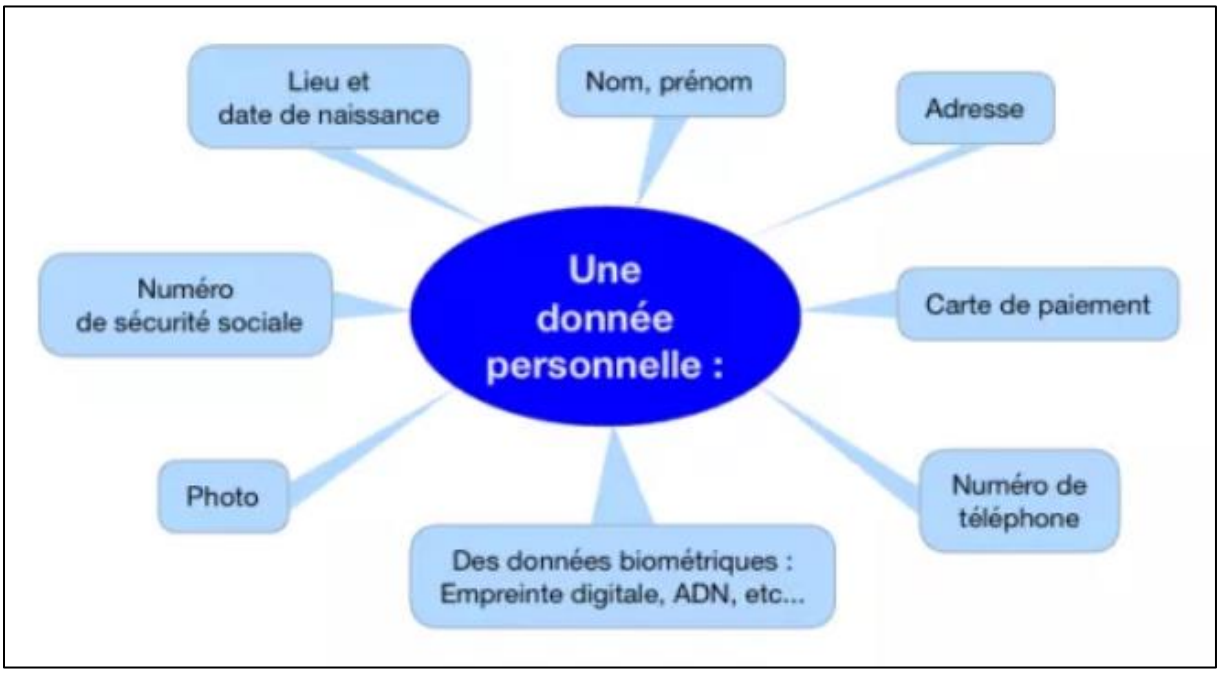
Source : Berthier Thierry, Kempf Olivier, *Vers une géopolitique de la donnée, Annales des Mines - Réalités industrielles*, vol. août 2016, n°3, 2016, p.16

Annexe 2 : La protection des données dans le monde



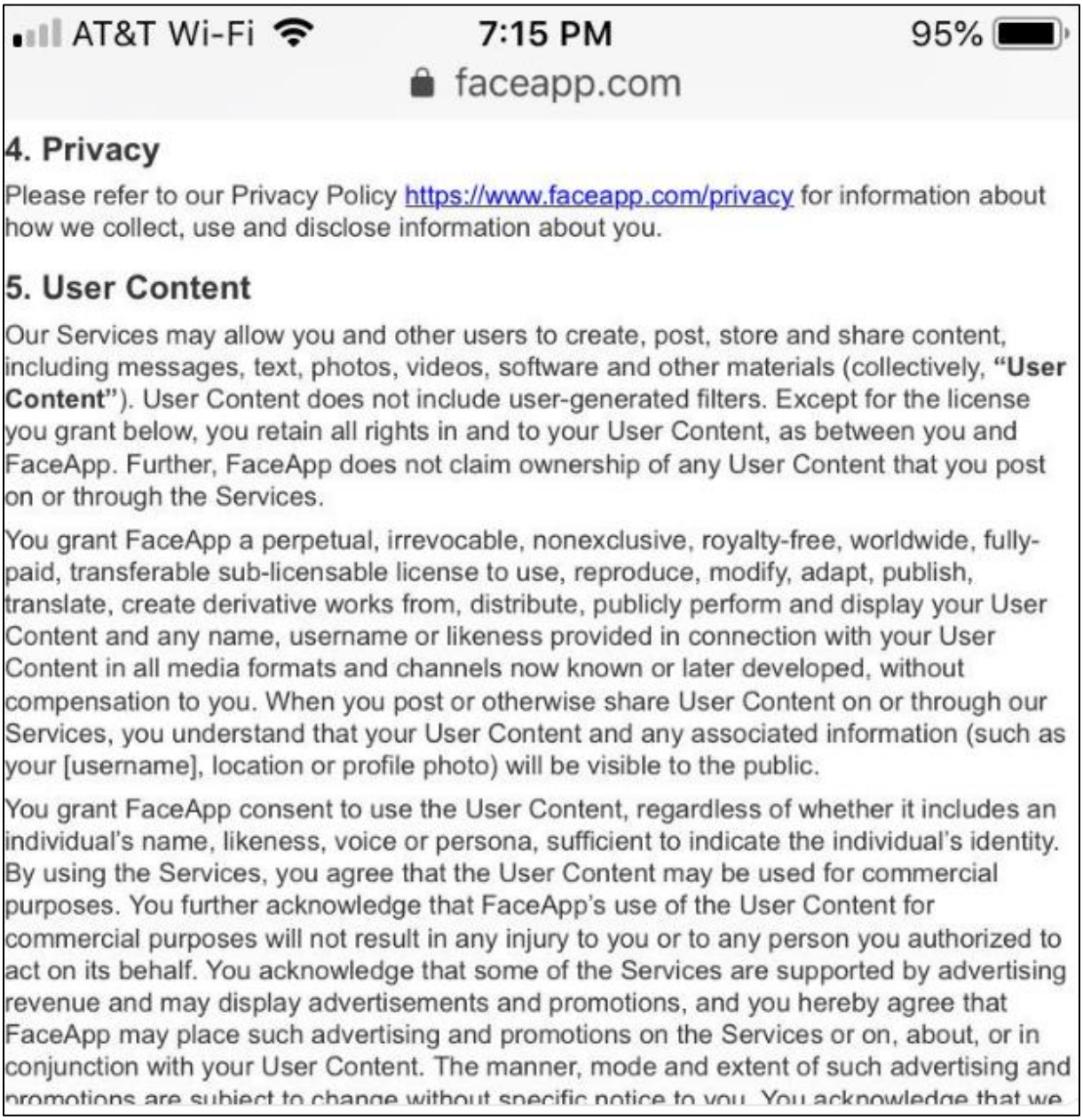
Cette carte permet de visualiser les différents niveaux de protection des données des pays dans le monde.

Annexe 3 : Eléments constitutifs d'une donnée personnelle



Source : Thomas-Jérôme BOUCHE, *Qu'est-ce qu'une donnée à caractère personnel – donnée personnelle ?* Expert DPO

Annexe 4 : Conditions générales d'utilisation de l'application mobile FaceApp



AT&T Wi-Fi 7:15 PM 95%

faceapp.com

4. Privacy

Please refer to our Privacy Policy https://www.faceapp.com/privacy for information about how we collect, use and disclose information about you.

5. User Content

Our Services may allow you and other users to create, post, store and share content, including messages, text, photos, videos, software and other materials (collectively, **"User Content"**). User Content does not include user-generated filters. Except for the license you grant below, you retain all rights in and to your User Content, as between you and FaceApp. Further, FaceApp does not claim ownership of any User Content that you post on or through the Services.

You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you. When you post or otherwise share User Content on or through our Services, you understand that your User Content and any associated information (such as your [username], location or profile photo) will be visible to the public.

You grant FaceApp consent to use the User Content, regardless of whether it includes an individual's name, likeness, voice or persona, sufficient to indicate the individual's identity. By using the Services, you agree that the User Content may be used for commercial purposes. You further acknowledge that FaceApp's use of the User Content for commercial purposes will not result in any injury to you or to any person you authorized to act on its behalf. You acknowledge that some of the Services are supported by advertising revenue and may display advertisements and promotions, and you hereby agree that FaceApp may place such advertising and promotions on the Services or on, about, or in conjunction with your User Content. The manner, mode and extent of such advertising and promotions are subject to change without specific notice to you. You acknowledge that we

Source : capture des conditions générales d'utilisation de l'application mobile FaceApp

TABLES DES MATIERES