Université de Montréal

L’avènement mondial du principe de la libre circulation des données personnelles et ses dérives : de la nécessité de repenser la protection des données personnelles comme une fin en soi

Par

Sylvain Longhais

Faculté de Droit

Mémoire présenté en vue de l’obtention du grade de Maîtrise en droit des technologies de l’information, cheminement général

Juillet 2022

RÉSUMÉ ET MOTS-CLÉS

Mots-clés : protection des renseignements personnels ; libre circulation des données ; *privacy* ; droit du commerce international ;

Résumé : Depuis les années 1970 et les premières législations relatives à la protection des données personnelles, la circulation des données personnelles hors des frontières a toujours été un enjeu crucial. Dans ce mémoire nous étudions comment l'on est passé de réglementations prônant la protection des données personnelles hors des frontières à des réglementations instaurant un principe de libre circulation des données à l'échelle mondiale. Cette étude se fonde dans un premier temps sur une rétrospective du droit des données personnelles en ce qui concerne les flux transfrontières de données avant de constater dans un second temps que ces questions de droit sont désormais fondues dans des enjeux de droit du commerce international. Posant enfin les dérives d'une telle libre circulation des données au niveau mondial, nous réfléchissons à certaines pistes de réflexion afin de replacer la protection des données comme une fin en soi, au centre des enjeux.

SUMMARY AND KEYWORDS

Keywords: protection of personal information; free flow of data; privacy; international trade law

Abstract: Since the 1970s and the first data protection laws, the flow of personal data across borders has always been a crucial issue. In this thesis, we study how we have moved from regulations advocating the protection of personal data outside borders to regulations establishing a principle of free data circulation on a global scale. This study is based firstly on a retrospective of personal data law with regard to transborder data flows, and secondly on the fact that these legal questions are now merged with issues of international trade law. Finally, we consider the drifts of such a free flow of data at the global level, and we reflect on certain avenues of reflection in order to place data protection as an end in itself, at the center of the issues.

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABRÉVIATIONS

ACEUM : Accord Canada-États-Unis-Mexique

APEC : Asia Pacific Economic Cooperation

CETA : Comprehensive Economic and Trade Agreement

CNIL : Commission nationale de l'informatique et des libertés

GAFAM : Désigne les géants du numérique, Google, Apple, Facebook, Amazon, Microsoft.

GATT : General Agreement on Tariffs and Trade

GATS : General Agreement on Trade in services

OMC : Organisation mondiale du commerce.

RGPD : Règlement général sur la protection des données

UE : Union européenne.

REMERCIEMENTS

Je voudrais avant tout remercier Monsieur le Professeur Karim Benyekhlef d'avoir accepté de diriger mes recherches en vue de la réalisation de ce mémoire de maîtrise, de m'avoir prodigué ses précieux conseils et de m'avoir donné l'opportunité de travailler pour le Laboratoire de Cyberjustice.

Je voudrais également remercier mes parents pour leur soutien sans faille pendant toute la rédaction du présent mémoire et pendant la pandémie de Covid-19. Mes amis pour m'avoir toujours tiré vers le haut et mes collègues du Laboratoire de Cyberjustice pour votre bienveillance, soyez également remerciés.

Plus généralement, je voudrais remercier toutes les personnes qui m'ont apporté un soutien, une discussion, une idée à un moment du processus de rédaction.

INTRODUCTION

« La richesse des sociétés dans lesquelles règne le capitalisme s'annonce comme une gigantesque accumulation de marchandises ».[1] La première phrase du *Capital* de Karl Marx pourrait trouver aujourd'hui un écho certain, si tant est que l'on considère aujourd'hui les données comme étant une marchandise. En effet, à l'ère de l'économie numérique, la richesse provient d'une gigantesque accumulation de données à tous les niveaux de nos sociétés modernes. Là où K. Marx considérait la circulation des marchandises comme le point de départ du capital[2], le même constat doit être fait dans la nouvelle économie irriguée par la circulation des données numériques de toute nature. La croissance de l'économie numérique semble conditionnée à la libre circulation des données à en croire certaines prévisions de 2018, qui lui attribuait directement une hausse de 4 % du PIB européen à horizon 2020.[3] À ce titre, l'Union européenne n'avait pas hésité à consacrer cette libre circulation des données comme « cinquième liberté » après la libre circulation des biens, des capitaux, des services et des personnes.[4] La libre circulation des données comme corollaire de la croissance de l'économie numérique est cristallisée par l'émergence puis l'hégémonie d'acteurs privés basés aux États-Unis qui transfèrent des données depuis le monde entier vers les États-Unis et qui fondent leur modèle économique sur l'exploitation des données. De manière plus générale, la circulation des données sur le plan international est au service du commerce électronique, domaine que s'est arrogé l'OMC et qui prône également la libre circulation internationale des données et notamment des données personnelles.

Dès lors, la circulation internationale des données personnelles doit être au cœur des préoccupations lorsque l'on aborde les enjeux auxquels droit de la protection des données personnelles moderne doit faire face. Entendons-nous d'emblée sur les définitions et les contours

---

[1] Karl MARX, *Le Capital*, traduit par M.J ROY, Paris, Maurice Lacharte et Cie, 1872, p. 13.
[2] *Id.*, p. 61.
[3] Anaïs CHERIF, « Pourquoi l'Europe mise sur la libre circulation des données non personnelles », *www.latribune.fr*, 4 octobre 2018, en ligne : <https://www.latribune.fr/technos-medias/pourquoi-l-europe-mise-sur-la-libre-circulation-des-donnees-non-personnelles-792766.html>.
[4] Philippe MOURON, « La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne », *La revue européenne des médias et du numérique* 2019.49, en ligne : https://la-rem.eu/2019/03/la-libre-circulation-des-donnees-est-devenue-la-cinquieme-liberte-consacree-dans-le-droit-de-lunion-europeenne/.

des termes du sujet. Par libre circulation des données, nous entendons aux fins du présent mémoire, la libre circulation des données personnelles, qui est organisée juridiquement. Nous ferons notamment l'étude des outils qui existent dans le droit international et qui permettent d'opérer la libre circulation des données personnelles en toute légalité. Le plus souvent, sauf lorsqu'il en est mentionné autrement, nous ferons référence à la libre circulation internationale dans les flux transfrontières des données. Il s'agit de la liberté d'opérer des transferts externes depuis le territoire d'un État ou bien de l'Union européenne. Par transfert de données, nous entendons : toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays autre que celui de départ. Cette définition est calquée sur celle donnée par la CNIL, reprise en droit européen.[5] Lorsque nous faisons référence aux données, nous entendons les données personnelles et la définition suivante qui s'y rattache : toute information se rapportant à une personne physique identifiée ou identifiable.[6]

La libre circulation internationale des données personnelles est un sujet clivant par nature. En effet, d'un côté, elle est extrêmement difficile à remettre en cause, ni même à questionner, tant l'économie numérique repose sur elle, et tant la brider, à l'heure de nos technologies actuelles, semble difficile. D'un autre côté, il est de plus en plus compliqué de ne pas imputer à la libre circulation internationale des données personnelles, certains effets délétères sur le plan sociopolitique. Par conséquent, la libre circulation internationale des données personnelles est un phénomène, qui doit être étudié en droit, afin de comprendre dans quelles circonstances et dans quelle mesure, elle est devenue un principe juridique contraignant de premier plan, et quelles sont ses implications dans le contexte sociopolitique et économique actuel ? Force est de constater qu'en droit, le principe de libre circulation des données ne suscite que de peu de questionnements doctrinaux, alors même qu'il représente, par nature, une des principales forces contraires à la protection des données personnelles.

Il semble que la libre circulation des données personnelles soit un principe alors acquis, et même gravé dans le marbre, sans qu'il soit question d'une quelconque remise en cause. Ainsi, une vaste majorité de la doctrine s'attache à imaginer la protection des données personnelles de demain

[5] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Transfert de données », *www.cnil.fr*, en ligne : <https://www.cnil.fr/fr/definition/transfert-de-donnees>.
[6] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Donnée personnelle », *www.cnil.fr*, en ligne : <https://www.cnil.fr/fr/definition/donnee-personnelle>.

dans un environnement numérique dans lequel, la libre circulation des données et *a fortiori* la libre circulation internationale des données est une norme quasi sacrée.

Partant de ce constat, l'idée qui va guider le présent mémoire est la suivante : la libre circulation internationale des données n'est pas nécessairement une évidence en droit des données personnelles. Ainsi, ses origines, les modalités juridiques de son avènement et les effets délétères qu'elle produit doivent être étudiés. Cela constituerait un premier pas en direction de la remise en cause, tout du moins intellectuelle et théorique, du principe de libre circulation internationale des données. Ceci fait, ce mémoire devrait contribuer à élargir la vision que l'on peut avoir de la protection des données personnelles en l'opposant à la libre circulation, plutôt que de fondre les deux notions l'une dans l'autre.

La question sur laquelle reposera la trame de fond de ce travail pourrait être libellée en ces termes : quelles sont les origines juridiques, politiques et économiques de la libre circulation internationale des données personnelles et pourquoi ce principe va-t-il à l'encontre de la protection des données personnelles ?

Pour répondre à cette double question, nous construirons notre raisonnement en trois temps. Dans un premier temps, nous nous intéresserons à la réglementation des flux transfrontières des données depuis ses prémices et comment l'on est passé d'une fin de protection des données guidant cette règlementation, à une fin de libre circulation des données (partie 1). Dans un deuxième temps, après avoir défini les contours de la consécration de la libre circulation internationale dans les flux transfrontières de données, nous étudierons l'émergence de cadres juridiques adaptés au marché international des données (partie 2). Enfin, dans un troisième temps, nous nous attarderons sur les effets délétères de la libre circulation internationale des données sur la protection des données personnelles à la fois juridiquement et sociopolitiquement (partie 3).

Partie 1 : La règlementation des flux transfrontières de données personnelles : d'une fin de protection du droit des données à un droit des données consacrant la libre circulation

Pour analyser comment le droit à la protection des données personnelles comme fin en soi a disparu pour laisser sa place à un droit des données personnelles visant à réparer un dommage, il est primordial d'étudier la réglementation des flux transfrontières de données, depuis ses balbutiements. La réglementation des flux transfrontières de données est un très bon révélateur des métamorphoses qui se sont opérées depuis les années 1970 jusqu'à nos jours, en ce qu'elle a été l'outil privilégié pour engager lesdites métamorphoses. Nous considérerons que l'avènement de la conception américaine de *privacy* en Europe a permis de consacrer en droit la libre circulation des données à des fins économiques, puisque cette doctrine du fait de la notion de dommage auquel elle se rattache est plus permissive. Ce basculement s'est fait par le truchement du droit international public[7] comme nous allons l'étudier. Par ailleurs, au moins jusqu'à la fin des années 1990, ces velléités de libre circulation semblaient davantage guidées par l'idéologie plutôt que par la certitude d'effets tangibles attendus.

Cette partie s'attache par conséquent, à démontrer comment l'on est passé d'une conception européenne de protection des données comme fin en soi, jusque dans les mesures étatiques régissant les flux transfrontières de données, à un droit issu du concept de *privacy* américaine, permettant de prôner avant tout, la libre circulation des données et s'adaptant au développement concomitant de l'économie de l'information (Chapitre 1). On analysera comment des règles d'influence américaine ont été sanctifiées dans les premiers outils internationaux de droit des données personnelles, pour ce qui concerne notamment les flux transfrontières de données. Cela permet de mieux comprendre comment le concept de *privacy* américaine, de nature beaucoup plus libérale que sa voisine européenne, s'est installée durablement en Europe, favorisant *de facto* la consécration du principe de libre circulation des données personnelles en droit. Cependant, nous observerons que les politiques visant à favoriser les échanges de données et le principe de libre circulation des données consacré en droit international n'ont en réalité eu que des effets mitigés sur l'économie (Chapitre 2).

[7] Définition du droit international public : « Ensemble des règles juridiques qui régissent les relations entre les États, entre les États et les organismes internationaux ainsi qu'entre les organismes internationaux eux-mêmes. », Hubert REID, *Dictionnaire de droit québécois et canadien*, Version abrégée., Montréal, Wilson & Lafleur, 2016, « Droit international public ».

Chapitre 1 : Le basculement de la protection des données personnelles à l'européenne vers le concept de *privacy* à l'américaine

La libre circulation des données sur le plan international n'a pas toujours été l'objectif qui gouverne désormais les politiques en droit des données personnelles. Pendant un temps maintenant révolu, la protection des données personnelles comme une fin en soi s'est affichée comme un idéal en réponse aux craintes des dérives autoritaires, induites par l'usage des technologies de l'information. La règlementation des flux transfrontières de données personnelles était par conséquent un corollaire de cet idéal de protection. La première section traitera alors de la protection des données personnelles à l'européenne dans les échanges internationaux pre-1980, ses origines et sa matérialisation (Section 1). Mais cette doctrine juridique n'a vécu qu'une dizaine d'années avant d'être mise au second plan avec l'avènement de la *privacy* à l'américaine, ayant entrainé la consécration d'un principe de libre circulation transfrontière des données personnelles (Section 2).

Section 1 : La protection des données personnelles à l'européenne dans les échanges internationaux pre-1980 : origines et matérialisation

Cette section est consacrée à l'étude fastidieuse du droit à la protection des données personnelles comme elle était conçue en Europe dans les années 1970. Elle est néanmoins nécessaire pour comprendre la logique qui encadrait la protection des données personnelles jusque dans les flux internationaux de données. Ce droit a été conçu dans les années 1970 en Europe, avec un objectif de protection comme fin en soi, du fait de l'émergence de nouvelles technologies métamorphosant les traitements automatisés de données. Partant d'un regard croisé sur les contextes qui ont stimulé cette vague législative en Europe, nous détaillerons ensuite la matérialisation de ces premiers textes de protection des données et leur appréhension des flux transfrontières de données à des fins de protection.

Les contextes technologique et social de l'émergence de lois nationales de protection des données

Ce n'est pas un hasard du calendrier si en Europe, les États ont commencé à légiférer sur ces questions de données personnelles. On peut dégager deux types de contexte, qui ont constitué un terreau fertile pour le développement de ces législations. Il y a, en effet, un contexte social et un

contexte technologique. Tandis que le contexte social varie d'un pays à un autre, le contexte technologique, lui est commun. Commençons alors par ce dernier.

1. Le contexte technologique

Le contexte technologique est celui d'une évolution constante de l'informatique qui a permis dans les années 1960 et 1970 de commencer à traiter de manière automatique de plus en plus d'information, dans une multitude de domaines.[8] Ce sont, notamment, les développements concomitants en matière de *hardware* et de *software* qui ont permis d'arriver à de telles prouesses.[9] Que ce soit la miniaturisation des composants, on pense notamment au développement du microprocesseur à la fin des années 1960 et sa commercialisation au début des années 1970[10], ou encore l'amélioration des capacités de mémoire des ordinateurs par l'utilisation de périphériques spécialisés (bandes magnétiques et disques par exemple)[11] utilisables de manière amovible et simultanée,[12] ces développements technologiques ont, sans conteste, contribué à démocratiser l'automatisation du traitement de l'information. Néanmoins, il ne faut pas non plus sous-estimer l'importance des développements en matière de logiciel, qui auront permis de développer les langages informatiques et, avec eux, les capacités qualitatives de traitement, mais qui auront surtout permis de rendre plus accessible l'utilisation de l'outil informatique. Cela a été rendu possible en transposant une réalité de langage machine à une réalité de langage de programmation, d'abord pour des applications scientifiques, puis commerciales.[13] Ni plus ni moins, l'information est lisible du fait de la retranscription par le logiciel, du traitement, qui est fait par la machine.

Ces développements informatiques ont permis à la fin des années 1960 et au début des années 1970, de traiter de l'information de manière automatisée, mais également de rendre l'outil informatique plus accessible, ce qui a contribué à sa démocratisation. De 1965 à 1975, on est passé des « ordinateurs » à des « systèmes informatiques » qui peuvent être définis comme un :

---

[8] Fritz W HONDIUS, « Computers: Data privacy: The European community grapples with protecting individual rights in the midst of rampant computer progress », (1980) 17-3 *IEEE Spectrum* 67, 67.
[9] Pierre GOUJON, « Informatique — Évolution des systèmes de traitement de l'information », dans *Encyclopédie Universalis*, Corpus 12, Paris, Encyclopédie Universalis, 1989, p. 307.
[10] *Id.*
[11] *Id.*, p. 308.
[12] Simon NORA et Alain MINC, *L'informatisation de la societé*, Rapport à M. le Président de la République, B17970, Paris, 1978, en ligne : <https://www.vie-publique.fr/sites/default/files/rapport/pdf/154000252.pdf> (consulté le 17 mars 2021), document consultatif, p.19.
[13] P. GOUJON, préc., note 9. p. 309.

« ensemble indissociable d'équipements, de logiciels, de prestations, de savoir-faire mis à la disposition d'un utilisateur pour lui permettre de gérer automatiquement, si possible de bout en bout, une certaine "application" » et dont l'ordinateur n'est plus qu'une composante.[14] Le développement du parc informatique mondial atteste d'ailleurs à l'époque de cette démocratisation de l'informatique. On passe de moins de 50 000 machines en service en 1965 à plus de 400 000 après 1975[15]. De plus, on assiste à un investissement de plus en plus fort des utilisateurs dans ces systèmes informatiques. Enfin, cette démocratisation est économique : de 1965 à 1970, on a une forte augmentation des performances des matériels informatiques pour un coût qui reste constant.[16]

C'est logiquement à cette période que l'on assiste aux premiers développements de politiques étatiques pour répondre à ce tournant informatique.[17] En 1978, en France, un rapport célèbre, est remis au président de la République faisant état de l'« informatisation de la société », plus connu sous le nom de Rapport Nora-Minc du nom des deux auteurs principaux, Simon Nora et Alain Minc. Ce rapport établit notamment un constat et pointe plusieurs défis, auxquels l'État français doit répondre.

Le constat principal est le passage de l'informatique à la télématique. Finalement, la télématique n'est que la conséquence des développements informatiques structurels ayant eu lieu dans les années 1960-1970. Si on peut la définir comme : « l'ensemble des techniques et des services qui associent les télécommunications et l'informatique »[18], il n'en reste pas moins que ce terme est apparu à l'occasion du rapport Nora Minc et qu'il fait état d'une situation du développement conjoint des systèmes informatiques et des télécommunications, ayant eu pour principale conséquence la fameuse « informatisation de la société ».[19] Mais au-delà de la technique, c'est également les conséquences de la télématique qui font la télématique. C'est, par exemple, l'émergence de nouveaux services, tels que l'accès à des bases de données à distance ou encore la généralisation des procédés de télécopie par la multiplication de transferts de signaux

[14] S. NORA et A. MINC, préc., note 12., document consultatif, p.21.
[15] *Id.*, document consultatif, p. 36.
[16] *Id.*, document consultatif, p. 44.
[17] Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992, p. 245.
[18] LAROUSSE, « Télématique », *larousse.fr*, en ligne : <https://www.larousse.fr/dictionnaires/francais/télématique/77084#:~:text=Ensemble%20des%20techniques%20et%20des,les%20télécommunications%20et%20l%27informatique.>.
[19] S. NORA et A. MINC, préc., note 12, p. 30.

numériques.[20] Mais ce que le rapport prédisait, c'était bien la démultiplication des transferts et de traitement de l'information par le biais de réseaux interconnectés, empruntant alors l'analogie à des réseaux électriques.[21]

Ainsi, devant l'évolution fulgurante de ce contexte technologique, changeant de manière importante, les pratiques dans le traitement de l'information ont évolué, pour progressivement passer d'un traitement manuel majoritaire, à un traitement automatisé majoritaire de l'information. Dès lors, il est assez logique que les États aient commencé à légiférer en matière de protection des données personnelles eu égard aux nouvelles possibilités de traitement induites par la démocratisation des systèmes informatiques. Cependant, il serait incomplet de limiter l'apparition de ces nouvelles règlementations dans les années 1970 aux seuls bouleversements du contexte technologique de l'époque. En effet, les différents contextes sociaux des États européens ont amené à s'interroger sur les risques engendrés par les développements informatiques et notamment sur les craintes aux atteintes aux droits et libertés (on pense à la vie privée), du fait de l'automatisation du traitement de l'information.

2. Les contextes sociaux

Le contexte social varie d'un pays à un autre en Europe, si bien que l'on peut parler de contextes au pluriel.

En effet, les situations en Suède, en Allemagne, en France ou même au Portugal et en Espagne sont différentes et l'éclosion de règlementations sur la protection des données personnelles, que ces dernières soient *ad hoc* ou ancrées constitutionnellement, est le fruit de contextes sociaux, ayant pour point commun le fait d'avoir une méfiance à l'égard des États quant aux données disponibles concernant leurs citoyens.

Généralement, le contexte social ayant favorisé l'émergence de règlementations de protection de données personnelles est directement lié à l'évolution technologique et l'importance qu'elle prend dans le débat public. Mais, il est, dans certains pays d'Europe, beaucoup plus ancrée historiquement du fait des fantômes de la Seconde Guerre mondiale qui hantent toujours les esprits

[20] *Id.*, p. 25.
[21] *Id.*, p. 29.

ou bien de la fin de certains régimes totalitaires à la fin des années 1960 et au début des années 1970.

En Suède, c'est la prompte informatisation de la société qui a fait émerger ces inquiétudes dans le débat public. Ces dernières ne concernaient au départ que l'adaptation du principe du libre accès aux documents publics à l'automatisation de données,[22] puisque la Suède s'était déjà dotée d'un système d'identification personnelle. La question était donc éminemment juridique puisqu'il s'agissait au départ de savoir si une bande magnétique (pur fruit du contexte technologique de l'époque en matière de stockage, comme nous l'avons vu) était considérée comme un document au sens de ce principe.[23][24] Mais rapidement, ces inquiétudes ont glissé vers l'accessibilité et la disponibilité par l'État des données automatisées concernant les citoyens.[25] Il fallait donc répondre dans un contexte de « méfiance » à l'égard de l'État quant à l'accès à ces données d'une part et pallier l'insuffisance de règles protégeant le droit à la vie privée d'autre part.[26] C'est donc dans un contexte social d'inquiétudes et de débat public relatif à l'apparition de ces nouvelles techniques d'automatisation de l'information que la loi de 1973 a été adoptée.

En France, l'adoption de la loi de 1978 s'est faite dans un contexte social toujours intimement lié au contexte technologique, mais moins apaisé qu'en Suède, puisqu'elle est la conséquence directe du scandale, dit SAFARI. Le scandale SAFARI a éclaté lorsque le journal *LeMonde* a dévoilé le projet de surveillance du gouvernement français, qui consistait en un vaste fichier (SAFARI) qui avait pour but de centraliser au sein du ministère de l'Intérieur quelque cent millions de données personnelles concernant les résidents français au moyen d'un superordinateur.[27] Mais en dehors du fichage des citoyens français, la question plus profonde concernait bien d'éventuelles résurgences du passé et rappelait notamment la mise en place du tristement célèbre « fichier juif » mis en place par le régime de Vichy. Ce fichier avait été ordonné

---

[22] Tore DALENIUS, « Data Protection Legislation in Sweden: A Statistician's Perspective », (1979) 142-3 *Journal of the Royal Statistical Society. Series A (General)* 285, 286.
[23] *Id.*
[24] À ce titre on peut d'ores et déjà souligner que les questions actuelles sur l'adaptation de principes de droit à des réalités technologiques ne sont pas sensiblement différentes de celles qui pouvaient exister dans les années 70, nous aurons l'occasion d'y revenir plus loin dans le développement.
[25] T. DALENIUS, préc., note 22, 286.
[26] *Id.*
[27] BUG BROTHER, « Safari et la (nouvelle) chasse aux Français », *Le Monde.fr*, 23 décembre 2010, en ligne : <https://www.lemonde.fr/blog/bugbrother/2010/12/23/safari-et-la-nouvelle-chasse-aux-francais/>.

par les occupants entre 1940 et 1944[28] et était constitué sur la base d'un recensement obligatoire auquel la population juive, d'abord de la zone occupée puis de la France entière, devait se soumettre. Les juifs de France devaient se faire inscrire sur un registre spécial qui a grandement facilité la déportation dans les camps.[29] Cette sombre page de l'histoire comme toile de fond exacerbait les inquiétudes sur un tel fichage de la population française et les risques associés dans l'hypothèse où un régime totalitaire reviendrait au pouvoir et se servirait de ce fichage pour commettre les plus affreuses exactions.[30] Dans le cas de la France alors, le contexte social et les débats suscités faisaient écho à un traumatisme historique, ayant forcé le gouvernement français à prendre des mesures de protection des données personnelles, eu égard au contexte technologique et à l'automatisation du traitement des données.

En Allemagne, la problématique était similaire, puisque la loi de Hesse sur la protection des données est venue régler des questions relatives au traitement automatisé de données dans l'administration publique et les implications sociales qui en découlaient.[31] Mais comme en France, une majeure partie de ces problématiques sociales reposaient sur des faits historiques impliquant le régime nazi. Cependant, comme le rappelle David H. Flaherty, les débats sur la protection des données personnelles en Allemagne étaient alimentés par deux intérêts concurrents, qui étaient la nécessité de contrôler la capacité de l'État à surveiller les individus en accumulant des données les concernant (fruit d'expériences historiques dramatiques), mais également la volonté d'un gouvernement dirigiste eu égard à la conception de l'ordre présente dans la société allemande.[32] Néanmoins, au sortir de la Seconde Guerre mondiale, l'Allemagne (on parle de la RFA à l'époque) a traditionnellement organisé les pouvoirs, et les contrepouvoirs de l'appareil étatique de manière globale, afin de préserver un État de droit le plus important possible, et y compris en ce qui a trait aux services de police et de renseignements.[33] Il n'est donc pas surprenant de voir émerger des règles en matière de protection des données qui constitue également une limitation au pouvoir de l'État. Plus surprenant en revanche, c'est la position de la population allemande à l'époque

[28]Philippe GRAND, « Le Fichier Juif : un malaise », (1999) 1999/3-167 *Revue d'Histoire de la Shoah* 53-101. p.1.
[29]René POZNANSKI, « Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs », *Gazette des archives* 1997.177-178, 250, 250.
[30] *Id.*, 259.
[31] David H. FLAHERTY, *Protecting Privacy in Surveillance Societies*, Chapel Hill and London, The University of North Carolina Press, 1989. p. 22.
[32]*Id.*, p. 24
[33]*Id.*, p. 25

puisqu'un sondage de 1976 montrait que les Allemands étaient plus méfiants quant aux abus liés aux données personnelles dans le secteur privé que dans le secteur public.[34] Dès lors, la règlementation en Allemagne dans les années 1970 relève moins d'une nécessité d'empêcher la surveillance de l'État dans un contexte technologique que d'apporter une pierre supplémentaire à la préservation de l'État de droit.

L'autre aspect ayant précipité la règlementation dans certains pays d'Europe, c'est la chute des derniers régimes totalitaires d'Europe de l'Ouest et notamment celle du régime franquiste en Espagne et de la dictature salazariste au Portugal.

Comme dans le reste des pays ayant connu des régimes autoritaires, on peut supposer que l'ancrage constitutionnel conféré aux données personnelles provient d'un traumatisme lié à la surveillance de masse contre les citoyens. En effet, en Espagne, le régime franquiste entretenait un registre dans lequel la population entière était divisée en catégories symbolisées par des lettres de l'alphabet. Chaque catégorie renvoyait à un groupe de personnes à surveiller. Ces groupes étaient très spécifiques et précis. Par exemple, on trouvait un groupe qui recensait tous les sympathisants d'extrême gauche qui avait rejoint la milice nationale ou encore une autre référant à des personnes à la moralité douteuse qui étaient susceptibles de céder à la corruption.[35] Il n'est dès lors pas surprenant que la surveillance et les exactions commises par le régime en place, combinées à l'émergence contemporaine de nouvelles technologies aient entraîné une volonté politique de protéger les données personnelles de la population espagnole au sortir de la dictature. C'est également à cette période qu'ont lieu les premières politiques d'informatisation du pays afin de surfer sur la vague de la « révolution » informatique, qui était mise de l'avant avec un double objectif de réforme économique et d'ouverture politique afin de rattraper les autres pays européens plus avancés.[36] Ainsi, le contexte social de l'époque en Espagne, qui a vu l'informatisation des sociétés émerger tout en étant sous le joug d'un régime autoritaire, peut expliquer cette prise de conscience de protéger les données de la population espagnole.

---

[34] *Id.*, p. 25.
[35] Javier TUSSEL, *Spain: From Dictatorship to Democracy 1939 to the Present*, Oxford, Blackwell Publishing, 2007, p. 26.
[36] Ignasi MEDA-CALVET, « Playfulness and the Advent of Computerization in Spain: The National Club of ZX81 Users », dans Fabio GADDUCI et Mirko TAVOSANIS (dir.), *History and Philosophy of Computing : 3rd International Conference on History and Philosophy of Computing (HaPoC), on October 8th, 9th, 10th et 11th 2015*, Pisa, Italie, Springer, 2015, p. 228, p. 229.

Au Portugal, bien que le contexte historique soit assez différent de celui de l'Espagne, on retrouve un régime autoritaire qui s'éteint au milieu des années 1970. Dans le même temps, l'économie portugaise s'est fortement développée entre les années 1960 et les années 1970, favorisant de ce fait l'informatisation de la société.[37] Le basculement vers une démocratie avec la constitution de 1976, instaurant la troisième république du Portugal, a également pris en compte ces développements technologiques en matière de protection des données. C'est d'autant plus le cas que cette période *post* dictature correspond à l'informatisation du secteur public, du fait de la restructuration des services publics.[38]

Ces contextes technologiques et sociaux ont, par conséquent, naturellement permis l'émergence des premières lois de données personnelles en Europe dans les années 1970. On constate un terreau fertile en faveur d'un droit à la protection des données personnelles vu comme une fin en soi. Il s'agit d'appréhender un développement technologique concomitant à des contextes sociaux afin d'éviter les possibles dérives. Dans les années 1970, les États s'attachent, comme nous allons l'étudier, à consacrer une protection des données comme fin en soi. Les questions liées à l'économie de l'information et notamment la libéralisation des flux de données n'ont été appréhendées que plus tard par le droit et notamment par le truchement d'outils internationaux que nous développerons dans la deuxième section.[39]

La première matérialisation législative de la protection des données personnelles

Cette matérialisation législative de la protection des données personnelles a été double. Elle a pris la forme de lois *ad hoc* de protection des données personnelles de première génération,[40] c'est-à-dire des lois, qui ont été spécialement taillées pour ces situations, mais également des dispositions, qui ont été ancrées constitutionnellement. Ces dispositions à travers l'Europe encadraient déjà les flux transfrontières de données. Mais cet encadrement venait compléter la loi nationale afin de préserver son efficacité.

---

[37] Pedro Ramos BRANDAO, « A brief history of Computation's in Portugal », (2018) 2-5 *Invention journal of Research technology in engineering & management* 01, 03.
[38] *Id.*
[39] *Intra*, p. 27.
[40] Dites de première génération puisqu'encore non soumise à la contrainte d'un droit supranational des données. L'évolution du contexte économique et technologique dans lequel s'échangent les données et l'apparition des premiers outils internationaux en droit des données ont entraîné des changements dans ces lois notamment en matière de flux transfrontières.

1. Des lois ad hoc

Dans les faits, la toute première loi n'était pas nationale, mais provinciale. Il s'agissait de la loi de l'État fédéral de Hesse dans le centre ouest de l'Allemagne qui, pour la première fois, établissait, un cadre de protection des données personnelles pour le secteur public.[41] Cette loi répondait notamment aux inquiétudes grandissantes concernant le traitement automatique des informations de citoyens par l'administration publique[42] alors que l'État de Hesse promouvait activement le développement de ces traitements automatiques[43]. Par conséquent, les dispositions avaient pour but de règlementer l'usage de données qui étaient stockées dans les fichiers du Land de Hesse. Plus précisément, cette loi était intéressante en ce qu'elle apportait une première définition de la protection des données — *Datenschutz* — en allemand. Cette définition peut être rattachée à la notion de confidentialité des données, puisqu'elle fait référence aux obligations sur les données obtenues, stockées et transmises de ne pas faire l'objet de consultation, d'altération, d'extraction ou de destruction de la part d'une personne non autorisée.[44] En plus de garantir des droits aux individus concernés, comme un droit de rectification[45], il est intéressant de noter que cette loi avait également créé une commission chargée du contrôle de l'application de ces règles de protection des données personnelles.[46] Cette configuration juridique a ensuite largement été reprise par d'autres États européens dans la création de lois de protection des données personnelles.

La Suède a suivi en créant la première législation nationale sur la protection des données en 1973.[47] Cette loi très générale n'avait que pour objectif de règlementer le traitement de données automatisées.[48] Elle ne contenait que peu de principes relatifs aux traitements des données comparativement à la loi du Land de Hesse. Mais, elle établissait un principe de déclaration préalable pour tout registre de données personnelles automatisées, ouvrant la voie à la délivrance d'un permis par l'autorité de protection des données fraichement constituée.[49] Cette autorité

[41] D. H. FLAHERTY, préc., note 31, p. 22.
[42] *Id.*
[43] Gloria González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, coll. Law, Governance and Technology Series, n°16, Cham, Springer. p. 56.
[44] *Id.*, p. 57.
[45] *Id.*
[46] *Id.*
[47] Sören ÖMAN, « Implementing Data Protection in Law », (2004) 47 *IT Law – Scandinavian Studies in Law* 389, 390.
[48] *Id.*
[49] *Id.*

émettait par la même occasion des instructions spécifiques de protection des données personnelles pour chaque registre.[50]

La loi suédoise générale, assez rapidement agrémentée de textes de protection des données taillés pour des situations spécifiques,[51] constituait la première loi nationale en la matière en Europe. Beaucoup de pays ont suivi cette dynamique en adoptant des lois de protection des données personnelles. Les années 1970 ont en effet été prolixes, puisqu'en Europe, on ne recense pas moins de sept pays qui ont adopté des lois sur la protection des données.

En Allemagne, il a fallu attendre 1977 avant que la loi fédérale de protection des données ne soit promulguée ; en cause notamment, de nombreux débats depuis 1971 et une tentative avortée de texte refusée devant le Bundestag.[52] C'est en 1973 que la proposition de texte aboutissant à la loi de 1977 a été soumise au Parlement allemand. L'objectif de cette loi était d'abord de compléter les champs d'application matériels, qui n'étaient pas couverts par les différentes lois provinciales, en se concentrant notamment sur la protection des données dans le secteur privé.[53] Pour ce faire, l'objectif affiché dans la loi était de protéger les personnes concernées des mauvais usages faits de leurs données. Cela concernait le stockage, la transmission, la modification ou encore la suppression, afin de préserver les intérêts de la personne qui étaient dignes d'être protégés.[54] Le principe de base de la loi allemande est le suivant : le traitement des données personnel est réputé illégal à moins de remplir au moins un des critères présents dans la loi, qui sont, soit l'autorisation du traitement par l'autorité de protection des données ou par une loi, soit le consentement de l'individu.[55] Il est intéressant de noter que la loi fédérale allemande avait déjà établi une obligation pour certains opérateurs privés de nommer un délégué à la protection des données interne à l'entreprise[56], fonction, qui a été un des fers de lance du Règlement européen sur la protection des données personnelles de 2016.

Eu égard aux révélations de 1974 sur le fichier Safari, la promulgation de la loi de protection des données en France s'est fait à marche forcée, et ce, bien que des réflexions eussent déjà été

[50] *Id.*
[51] *Id.*
[52] G. G. FUSTER, préc., note 43, p. 60.
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*, p.61.

engagées dès les années 1970, notamment sous l'impulsion du député Michel Poniatowski, avec une proposition de loi visant à créer un « comité de surveillance de l'informatique » couplée à un « tribunal de l'informatique » dans le but de règlementer l'usage de l'informatique.[57] Suite à l'affaire SAFARI, une commission fut créée par le ministère de la Justice au nom évocateur de Commission informatique et libertés (CIL) afin de réfléchir à comment régler les problèmes connexes de l'informatisation de la société et des atteintes aux libertés. Les réflexions de cette commission ont débouché sur le fameux rapport Tricot intitulé « Informatique et libertés ». Il pointe les « problèmes qu'il est temps d'aborder » et notamment les potentielles atteintes aux libertés.[58] Il est également question de données personnelles dans le chapitre IV « Régler le recours aux traitements informatisés nominatifs » qui visent les traitements effectués dans le secteur public et qui comportent l'identification des personnes,[59] ainsi que les règles qui devraient s'appliquer à ces traitements.[60] En ce qui concerne la circulation des données, c'est bien la finalité qui doit conditionner la collecte et non pas des interdictions *a priori* selon le rapport.[61] Cependant, de telles interdictions peuvent tout de même exister et notamment, en ce qui a trait aux données sensibles consacrées dans le rapport,[62] et ce pour les raisons historiques déjà mentionnées.[63] Il est à noter que le rapport fait déjà état du recoupement de données dans le but d'obtenir des données sensibles.[64] Ce rapport constituera le squelette du projet de loi informatique et libertés, déposé devant l'Assemblée nationale par le ministre de la Justice Jean Lecanuet et qui sera adopté en 1978.

2. Des dispositions ancrées constitutionnellement

Les années 1970 ont également été marquées par des ancrages constitutionnels de la protection des données personnelles. On retrouve ces ancrages au Portugal, en Espagne et en Autriche à la fin des années 1970. L'Espagne a, par exemple, incorporé ce qui semble être une protection des données comme un droit fondamental dans la constitution de 1978 à l'article 18.[65]

---

[57] *Id.*
[58] Bernard TRICOT, *Rapport de la Commission Informatique et Libertés*, Rapport de la commission informatique et libertés, 410, coll. La documentation française, Paris, Ministère de la Justice, 1975, p. 11.
[59] *Id.*, p. 30.
[60] *Id.*, p. 31.
[61] *Id.*, p. 46.
[62] *Id.*, p. 47.
[63] *Supra*, p. 18.
[64] B. TRICOT, préc., note 58, p. 47.
[65] *Constitución Española [Spanish Constitution]*, BOE, 1978, BOE-A-1978-31229.

En effet, on peine à distinguer si les quatre aspects mentionnés dans cet article, que sont le droit à la vie privée, à l'inviolabilité de son domicile, au secret de ses communications et à la limitation à l'usage de l'informatique, forme un droit fondamental à la vie privée[66] englobant le droit à la protection des données personnelles, ou bien plusieurs droits distincts ayant une valeur constitutionnelle, dont le droit à la vie privée n'est qu'une composante, au même titre que le droit à la protection des données personnelles. La constitution portugaise va plus loin. L'article 35 prévoit explicitement des règles de protection des données, notamment liées au droit d'accès des individus à leurs données ou à l'interdiction d'utiliser un système informatisé pour traiter une liste de données sensibles.[67] En Autriche, la loi sur la protection des données comprenait une clause constitutionnelle signifiant que la protection des données est traitée comme un droit fondamental.[68]

À ce stade, le constat est le suivant. Nous sommes dans une logique résolument protectrice. Les organisations traitant des données personnelles de façon manuelle ou automatisée ne peuvent pas faire ce qu'elles veulent. Elles doivent respecter des règles qui sont contraignantes, qui ont été édictées spécialement dans le but de protéger les individus en encadrant strictement les traitements de données personnelles. Nous ne sommes pas dans une logique dans laquelle on laisse faire les organisations qui traitent des données. Ces règles répondent à des problématiques qui se posent dans des contextes sociaux donnés, comme nous l'avons vu, ce qui montre la volonté des États à répondre aux craintes de leurs citoyens, mais visent également à protéger des exactions du passé. Il est alors logique que la circulation des données transfrontières soit également appréhendée par ces textes. En effet, cette règlementation naît des craintes de contournement du droit national.

L'encadrement des flux transfrontières comme extension de la protection

Plus précisément, les règles régissant les flux transfrontières de données prévues dans ces lois suivaient des objectifs initiaux de protection forte des données, en répondant à la fois aux problèmes de vie privée et de surveillance. Avec le développement des systèmes informatisés, le concept de frontières a évolué et le contrôle de quelque chose d'« immatériel » devenait de plus en plus difficile. Il n'est donc pas surprenant d'observer cette tendance à protéger l'efficacité des règles nationales contre les risques de contournement en appliquant de telles règles transfrontières

[66] G. G. FUSTER, préc., note 43, p. 68.
[67] *Constitución de la República Portuguesa [Constitution of the Portuguese Republic]*, 1976 Diário da República.
[68] Fritz W HONDIUS, « Data Law in Europe », (1980) 16 *Stan J Int'l L* 87, 94.

aux flux de données personnelles. Ainsi, cette règlementation vient compléter un arsenal juridique résolument protecteur. Si les règles applicables en interne étaient conçues pour protéger les données à caractère personnel dans le pays, les règles régissant les flux sortants de données étaient quant à elles adoptées afin de maintenir l'efficacité de la loi.[69] Cela signifie essentiellement que pour garantir la vie privée des personnes à l'intérieur de leur pays, les États devaient créer des garanties pour s'assurer que les données n'étaient pas traitées dans un pays où aucune protection n'existe et éviter ainsi le contournement de leur loi.[70] Dès lors, on constate l'apparition concomitante d'aspects territorial et extraterritorial dès le début de la règlementation sur la protection des données. Les législations nationales traitaient les flux de données sortants de différentes manières, mais nous pouvons faire ressortir trois tendances.

1. Le modèle de licence

La première catégorie est basée sur les autorisations délivrées par les pouvoirs publics. Ce modèle également connu sous le nom de « licence » a été principalement développé dans les pays scandinaves.[71] En résumé, une autorisation de transfert de données vers un pays tiers devait être accordée par les autorités publiques avant l'exportation de données. Pour obtenir la licence, le demandeur devait se conformer aux règles relatives au traitement des données.[72] Par exemple, la loi suédoise prévoyait que lorsque le but de l'exportation était de saisir des données dans un système informatisé pour les traiter, l'exportateur devait demander une licence, peu importe le caractère manuel ou automatisé des données.[73] En outre, la licence ne devait pas être accordée s'il y avait des raisons de croire que la vie privée du sujet était menacée.[74] L'autorisation était généralement délivrée par l'autorité de protection des données. Cette tendance de réglementation des flux transfrontières de données était le modèle le plus strict.

[69] K. BENYEKHLEF, préc., note 17, p. 245.
[70] *Id.*
[71] Tor HAFLI, « Transborder Data Flows - The Scandinavian Solution », dans Jon BING et Knut S. SELMER (dir.), *A Decade of Computers and Law*, Oslo, Universitetsforlaget, 1980, p. 59, aux p. 60 et 61.
[72] *Id.*, p. 62.
[73] *Id.*
[74] *Datalag [Data Act]*, 1973 SFS. 289.

2. Le modèle centralisé

La deuxième catégorie est la régulation des flux transfrontières de données dans un modèle centralisé. Dans ce système, les règles internes s'appliquaient à tous les transferts, que les données soient traitées à l'intérieur ou à l'extérieur du pays. Un tel modèle a été mis en œuvre en République fédérale d'Allemagne en 1977. Il s'agit d'un système par défaut puisque la loi ne prévoyait tout simplement aucune règle relative aux flux transfrontières de données.[75] Cela se traduisait par l'application d'un régime général, qui couvre à la fois le traitement des données internes et externes.[76] En définitive, la qualité du destinataire des données importait plus que le pays où la donnée était envoyée, lorsqu'il s'agissait de se conformer à la loi.

3. Le modèle d'enregistrement

La troisième catégorie est le système d'enregistrement. Ce système figurait dans la loi française sur la protection des données de 1978 et concernait les personnes privées. L'article 16 de la loi prévoyait que tout traitement informatisé de données à caractère personnel effectué par une personne privée devait être déclaré à la CNIL.[77] [78] Cet enregistrement devait contenir une liste de fonctionnalités liées au transfert parmi lesquelles la finalité du traitement consistant à transférer les données personnelles vers un pays étranger.[79] Ces règles visant le traitement informatisé pouvaient être étendues au traitement manuel.[80] L'exception à ce principe est qu'un transfert pouvait être soumis à autorisation aux conditions de l'article 24.[81]

Ces trois catégories de réglementation des flux de données sortants par la législation nationale démontrent que les flux transfrontières de données étaient déjà pris en compte, lorsqu'il s'agissait d'éviter les contournements des normes nationales et que certains relevaient même d'une construction juridique élaborée. Ces règles sont venues soutenir la protection des données personnelles mises en œuvre pour protéger les citoyens. Dès lors, ces règles protectrices remplissaient une fonction de suppléance des dispositions applicables en interne. Elles

[75] K. BENYEKHLEF, préc., note 17, p. 254.
[76] *Id.*
[77] *Id.*, p. 246.
[78] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O 7 janv. 1978.
[79] La CNIL est l'autorité de protection des données en France.
[80] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, préc., note 78.
[81] K. BENYEKHLEF, préc., note 17, p. 246.

contribuaient à la finalité protectrice du droit des données personnelles de l'époque. À ce stade on doit alors comprendre que les règles encadrant les flux de données personnelles en dehors des frontières visaient une restriction de ces derniers. Tout du moins, elles visaient à étendre l'application de la protection des données qui était prévue dans la loi nationale. On est plutôt ici, dans une logique dans laquelle on fait en sorte que les données n'aillent pas à un endroit où elles ne seraient pas protégées, mais restent sur le territoire duquel la loi de protection des données comme une fin en soi s'applique.

Cependant, cette façon d'appréhender la protection des flux transfrontières par le droit a été largement remise en question lorsque s'est opéré le basculement vers une conception de *privacy* américaine remettant en cause la protection comme fin en soi, en faveur de considérations de libre circulation des données. Cette conception va surtout s'imposer en Europe par le biais d'instruments juridiques internationaux, prônant la libre circulation internationale des données, pour des raisons économiques, au sein des États y adhérant.

Section 2 : La consécration de la doctrine américaine de *privacy* au début des années 1980 : analyse de la doctrine et application de la libre circulation transfrontière en droit international

À première vue, on aurait tendance à expliquer la plus grande permissivité du droit des données personnelles contemporain par la nécessité économique de permettre aux données de circuler librement à travers les frontières et des volontés politiques de rendre cette libre circulation possible. C'est vrai. Cependant, il semble que peu d'auteurs ou d'organisations se soient intéressés à la facilitation de cette libre circulation découlant de la consécration implicite de la doctrine juridique américaine de *privacy,* qui a joué un rôle aussi grand que l'essor de nouvelles technologies ou que les politiques économiques libérales et le développement du commerce international.[82] Cette doctrine offre, en effet, un degré de permissivité nécessaire à l'application des doctrines libérales de l'époque bien plus large que la conception originelle européenne de protection des données, ce qui peut également expliquer le basculement en Europe de la conception européenne vers la conception américaine de la vie privée. Ainsi, il s'agira d'étudier dans cette section, la philosophie états-unienne de gestion des données personnelles par le droit et sa grande

[82] *Intra*, p. 89

influence dans les approches de règlementations transnationales, ayant consacré la libre circulation transfrontière des données personnelles**.**

La philosophie états-unienne de gestion des données personnelles par le droit

La philosophie américaine d'appréhension des données personnelles par le droit est réglée au travers du concept juridique de *privacy*. Après avoir étudié les fondements de ce concept, nous observerons comment il a permis à une libre circulation des données de s'instaurer, permettant ainsi l'accomplissement des doctrines économiques néo-libérales de l'époque.

1. Aux fondements de la « *privacy* »

S'il est établi que les premières matérialisations législatives et plus largement juridiques ont émergé en Europe, il ne faut pas pour autant mésestimer les recherches doctrinales qui ont été menées aux États-Unis, sur le concept de « *privacy* », concept intimement lié aux problématiques de données personnelles, sans pour autant constituer le travers synonymique qu'il est d'usage de constater dans le langage courant. En réalité, les recherches américaines sur ce concept de *privacy* sont pionnières et ont ouvert la voie à ce qui constitue l'essence du droit à la vie privée, dont le droit des données personnelles est une composante. On peut citer l'ouvrage de référence d'Alan Westin, *privacy and Freedom* dans lequel une étude exhaustive du concept de ses fondements les plus primaires (dans le monde animal par exemple),[83] jusqu'à ses implications dans un contexte de développement technologique. *Ipso facto*, l'ouvrage aboutit à la confrontation de ce concept avec celui de surveillance, et a été le point de départ d'une vague doctrinale sur les différentes implications et applications du concept aux États-Unis et ailleurs au début des années 70 et ayant mené à l'adoption du *Privacy Act* en 1974.

Bien que l'ouvrage d'A. Westin constitue une pierre angulaire dans le développement de la « *privacy* » à l'Américaine, il faut remonter près d'un siècle en arrière pour trouver les premiers écrits doctrinaux relatifs à ce concept. Nous faisons ici référence à l'article fondateur de Samuel Warren et Louis Brandeis, *The Right to Privacy* paru dans la prestigieuse *Harvard Law Review* en 1890. Et force est de constater que beaucoup des problématiques soulevées dans cet article sont facilement transposables à nos époques et à nos réalités technologiques. Finalement, le droit à la

[83] Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967.

« vie privée »[84] tel que théorisé par S. Warren et L. Brandeis repose sur un contexte technologique ayant fait augmenter de manière significative des atteintes à ce que les auteurs appellent « l'intellect et aux émotions »[85]. C'est celui de l'apparition d'appareils permettant : « d'enregistrer ou de reproduire des scènes ou des sons »[86]. Ce droit à la vie privée émerge là où les différentes autres branches du droit échouent à protéger efficacement la vie privée des individus eu égard à l'évolution du contexte technologique. Cependant, les auteurs ne remettent pas en cause l'utilisation de fondements en propriété intellectuelle ou en droit des contrats et dégagent de certaines décisions des solutions s'apparentant à une protection de la vie privée dans certaines mesures. L'idée de faire émerger un droit à la vie privée relève alors plutôt de l'importance de protéger la vie privée à un moment, où les fondements juridiques utilisés par les juges ne pourraient plus s'appliquer, du fait de l'évolution du contexte technologique et de nouvelles réalités leur échappant[87] (propriété intellectuelle, droit des contrats, droit à la propriété ou encore protection contre la diffamation). Ainsi, il ne s'agit pas de créer un nouveau principe, mais reconnaître ce droit à la vie privée au travers de multiples fondements et fictions juridiques.[88] Dès lors, le droit à la vie privée à l'américaine, tel que décrit par S. Warren et L. Brandeis, est une pure construction doctrinale, dont les contours restaient à être dessinés par les juges.

Cependant, les auteurs apportent d'emblée quelques freins à ce droit à la vie privée. Par exemple, le droit à la vie privée n'interdit pas les publications qui sont d'intérêt public ou général. Cette limite est intéressante, puisqu'on la retrouve dans le droit contemporain des données personnelles en Europe. En effet, dans l'application du droit à l'effacement (ou droit à l'oubli) en matière de données personnelles, c'est bien cette mise en balance qui avait été effectuée par la Cour de Justice de l'Union européenne dans l'affaire *Google Spain*. Les juges avaient rappelé qu'un individu pouvait demander qu'une information le concernant ne soit plus mise à disposition du grand public sur le fondement des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne sauf s'il : « apparaissait, pour des raisons particulières, telles que le rôle joué par ladite

[84] Ici, nous faisons faisant référence au terme de « vie privée » comme traduction littérale de « *privacy* ».
[85] Samuel D. WARREN et Louis D. BRANDEIS, « The Right To Privacy », (1890) 4-5 *Harvard Law Review* 193, 213.
[86] *Id.*, 206.
[87] Irwin R KRAMER, « The Birth of Privacy Law: A Century Since Warren and Brandeis », (1990) 39-3 *Catholic University Law Review* 703, 713.
[88] « The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise. », S. D. WARREN et L. D. BRANDEIS, préc., note 85, 213.

personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question ».[89] Ce considérant fait largement écho à la limite du droit à la vie privée, telle que théorisée par S. Warren et L. Brandeis, puisque ces derniers clamaient que certaines personnes ont renoncé au droit de vivre leur vie à l'abri de l'observation publique.[90] On doit également souligner les balbutiements de la notion de consentement comme renoncement au droit à la vie privée,[91] qui apparaît comme transposable au droit des données personnelles dans nos sociétés contemporaines (et qui est[92] la clé de voûte du droit des renseignements personnels au Canada). Si nous nous bornons à ne citer que ces deux limites ici, puisque ce sont ces dernières qui nous paraissent les plus pertinentes, eu égard aux débats sur les données agitant la doctrine au niveau mondial, il convient quand même de mentionner que les autres limites établies par S. Warren et L. Brandeis trouvent encore aujourd'hui une résonance certaine.

Aux États-Unis, le droit à la vie privée a par la suite connu deux courants juridiques :

Le premier courant juridique, qui a été développé par des auteurs comme A. Westin ou R. Wasserstrom est la théorie du contrôle.[93] Le principe est que l'individu devrait avoir le contrôle sur les aspects de sa vie privée, qu'il dévoilerait ou non. Par conséquent, un individu devrait être capable de « filtrer » ce qui sort de sa sphère privée, en direction de la sphère publique.[94] À ce titre A. Westin a une vision assez englobante de la théorie du contrôle :

> « *Privacy* is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. »[95]

---

[89] *Google Spain SL et Google Inc.* c. *Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12, 13 mai 2014, Recueil numérique (Recueil général) (Cour de Justice de l'Union européenne) [*Google Spain*], en ligne : <https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=316327>. considérant 97.

[90] S. D. WARREN et L. D. BRANDEIS, préc., note 85, 215.

[91] *Id.*, 218.

[92] Bientôt « a été », mais à l'heure où nous écrivons ces lignes, l'état du droit positif canadien en matière de renseignements personnels est celui que nous décrivons.

[93] Richard A. WASSERSTROM, « Privacy: some arguments and assumptions », dans FERDINAND D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy: an Anthology*, Cambridge, Cambridge University Press, 1984, p. 317.

[94] Karim BENYEKHLEF et Pierre-Luc DEZIEL, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Yvon Blais, 2018, p. 26.

[95] A. F. WESTIN, préc., note 83, p. 24.

R. Wasserstrom adopte une vision pratique de l'exercice de ce contrôle, au travers de quatre situations, comprenant des degrés d'atteintes à la vie privée plus ou moins sévères.[96]

Dans une vision de la vie privée peut-être plus adaptée au droit des données personnelles, A. Miller considère que la vie privée, c'est la capacité de l'individu à contrôler la circulation des informations le concernant.[97]

Finalement, la théorie du contrôle est fortement basée sur la notion de choix par l'individu, de qui a accès à telle ou telle information le concernant.[98] Cette notion de choix rejoint la notion de consentement de l'individu qui, comme on a pu le mentionner, est le socle du droit canadien des données personnelles. Mais, elle est importante dans beaucoup d'autres législations et reste une des bases légales principales du traitement de données personnelles. Cette théorie du contrôle aura, on peut s'en douter, donné des idées aux législateurs européens dans la rédaction des premières lois des données personnelles ; on pense notamment à l'Allemagne.[99] Mais cette théorie du contrôle a également inspiré le *Privacy Act* américain de 1974, dans lequel on retrouve le principe de contrôle et de consentement, comme condition de la divulgation d'information par une agence fédérale américaine :

> « No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains »[100]

La seconde théorie est celle de l'accès. Elle a été développée plus tard par des auteurs comme Ruth Gavison dans un article paru en 1980 dans le *Yale Law Journal*.[101] Cette théorie de l'accès englobe un nombre plus large de situations relatives à la vie privée, du fait du paradigme qui en est à la base. Le principal aspect de cette théorie, c'est le pouvoir que l'individu a sur l'accès à sa vie privée par des tiers ; ce pouvoir est matérialisé par sa capacité à empêcher les tentatives

---

[96] R. A. WASSERSTROM, préc., note 93, à la p. 318.
[97] Herman T. TAVANI, « Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy », (2007) 38-1 *Metaphilosophy* 1, 7. p. 7.
[98] *Id.*
[99] *Supra*, p. 22.
[100] *The Privacy Act*, 5 U.S.C. § 552a, 5 U.S.C. § 552a (b) (1974).
[101] Ruth GAVISON, « Privacy and the Limits of Law », (1980) 89-3 *The Yale Law Journal* 421.

d'accès depuis la sphère publique dans sa sphère privée.[102] Ainsi, la protection de la vie privée est davantage une affaire de degré d'accès à la sphère privée d'un individu[103] ; que l'on parle d'un accès physique ou bien d'un accès à des données personnelles, le degré le plus élevé est par conséquent, l'inaccessibilité pure et parfaite, degré assez utopique dans nos sociétés modernes. C'est d'autant plus le cas si l'on considère qu'une des caractéristiques de la vie privée est celle se rapportant au nombre d'informations que l'on connaît à propos d'un individu.[104]

Les différentes théories, que ce soit celle du contrôle ou de l'accès, sont alors élaborées et on serait tenté de penser qu'elles sont tout à fait à même de répondre aux problématiques de protection de la vie privée. À notre avis, là où le bât blesse en matière de protection, c'est au niveau du rattachement du concept de la vie privée au droit des *torts*. Nous l'avons vu avec l'article de Samuel Warren et Louis Brandeis, depuis les prémices de la *privacy*, le concept est très majoritairement rattaché à la notion de dommage. Cela signifie que le droit à la vie privée n'existerait dans les faits que pour protéger d'un dommage ou d'une atteinte à ce dernier.[105] En effet, le droit à la vie privée aux États-Unis est appréhendé par le truchement des *« torts »*. La théorie des *torts* relève d'une conception de *Common Law*. Les *torts* sont des actes fautifs et dommageables qui ouvrent un droit à la réparation, notamment une action en dommage et intérêts pour la victime.[106] Certains *torts* peuvent portent atteinte à la vie privée, comme la diffamation ou l'immixtion dans l'intimité d'une personne.[107] C'est sur ce point que l'on fait notamment une distinction avec la conception européenne de la vie privée, qui a souvent été abordée comme un droit fondamental.[108] Une autre distinction que l'on peut faire, c'est le caractère général ou restreint

---

[102] K. BENYEKHLEF et P. — L. DEZIEL, préc., note 94, p. 37.
[103] Judith DECEW, « Privacy », *plato.stanford.edu*, 18 janvier 2018, en ligne : <https://plato.stanford.edu/entries/privacy/#PriResAcc>.
[104] R. GAVISON, préc., note 101, 429.
[105] On fait référence à Warren et Brandeis dans leur article fondateur : « An action of tort for damages in all cases » comme recours pour les individus, S. D. WARREN et L. D. BRANDEIS, préc., note 85, p. 219. ; mais c'est également la position de A. Westin dans *Privacy and Freedom* puisque la question de la vie privée se pose dans le cadre de la surveillance mise en œuvre par les États, notamment en ce qu'elle a été facilitée par l'informatisation de nos sociétés. A. Westin donne l'exemple de la surveillance au travers de la collecte de données de permis de conduire mise en place par la police de New York dans les années 1960 qui a notamment mené à une plainte pour invasion de la vie privée, A. F. WESTIN, préc., note 83, p. 212.
[106] SENAT FRANCE, « Étude de législation comparée n° 33 — janvier 1998 — La protection de la vie privée face aux médias », *senat.fr*, janvier 1998, en ligne : <http://www.senat.fr/lc/lc33/lc3312.html> (consulté le 17 mars 2021).
[107] *Id.*
[108] On l'a vu dans les années 70 avec la consécration comme droit constitutionnel en Espagne ou au Portugal (*supra*, p. 24) et nous le verrons jusqu'à la consécration comme droit fondamental, que ce soit dans la charte des droits fondamentaux de l'Union européenne ou encore dans la convention européenne des droits de l'homme.

du droit à la vie privée. Là, où il a eu tendance à être général en Europe dans les années 1970, la constitution américaine ne prévoit qu'une protection contre les intrusions du gouvernement.[109] À ce titre, le Quatrième amendement de la constitution américaine consacre :

> « The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. »[110]

Ces distinctions ont sans doute contribué à ériger le droit à la vie privée et *a fortiori* le droit des données personnelles, comme une fin en Europe au début des années 1970[111], tandis qu'il est resté aux États-Unis, comme une action civile et non comme une fin en soi. Cela peut dès lors contribuer à expliquer pourquoi les courants promouvant l'importance de la libre circulation des données, qui se sont imbriqués dans la théorie globale de la *privacy*, (qui ont été le point de départ du droit des données personnelles moderne, fondé sur la libre circulation) ont vu le jour aux États-Unis.

2. La libre circulation des données comme composante à part entière de la *privacy* américaine

Il est évident que le droit à la vie privée aux États-Unis a été érigé en barrière contre certaines dérives de surveillance, qu'elles émanent du secteur privé ou bien de l'État, et qu'il a eu à ce titre une influence sur le droit européen de première génération, notamment du fait des théories poussées dont il a fait l'objet (on fait notamment référence à la théorie du contrôle développée plus haut). Une autre doctrine a cependant été avancée au début des années 1980 et s'imbrique complètement dans la vision de la *privacy* comme un *tort*. Elle consiste à considérer le droit à la vie privée comme un frein économique. Dans cette perspective, la libre circulation des données personnelles est la seule chose qui compte, pour peu qu'un dommage ne survienne pas. Cette théorie mêle par ailleurs, marchandisation de l'information et propriété sur l'information des individus, autrement dit sur leur vie privée. Ce sont autant d'éléments, que l'on peut finalement

[109] SÉNAT FRANCE, préc., note 106.
[110] U.S. CONST., amend. IV.
[111] *Supra*, p. 20.

retrouver, quand il est question de l'exploitation contemporaine des données personnelles par des acteurs privés, qui sera traitée dans la troisième et dernière partie.

Cette théorie est notamment défendue par Richard Posner lorsqu'il faisait la démonstration selon laquelle : si un potentiel employé cachait à son futur employeur des informations personnelles le concernant (informations personnelles importantes pouvant affecter la productivité dans l'entreprise), il pouvait y avoir des retombées économiques importantes, puisque cela empêchait l'optimisation des profils des salariés et affectait *in fine* l'entreprise et donc l'économie à plus forte mesure.[112] Derrière cet exemple, dont la pertinence doit être débattue autant que l'absence d'empathie doit être soulignée, R. Posner considère les éléments de la vie privée et le fait de vouloir les obtenir, comme des biens intermédiaires, c'est-à-dire des biens qui permettent de produire un bénéfice, de l'utilité ou encore du bien-être.[113] Ainsi, on assiste à une augmentation de la demande d'éléments de vie privée, puisque ces biens permettent au demandeur d'en tirer un bénéfice.[114] C'est notamment le cas pour un individu qui cacherait des éléments de sa vie privée pour son utilité personnelle (dans l'exemple de l'embauche) et pour un employeur qui demanderait ces éléments pour transformer ces informations en un bénéfice (dans le cas qui nous intéresse, optimiser son équipe de production).[115] Cependant, la demande d'information peut parfois être désintéressée dans le sens ou l'information n'a pas de valeur intrinsèque ; bien qu'utile, elle est plutôt d'ordre informatif.[116] Au-delà du mépris de classe dont fait preuve R. Posner (voir n 116.), il est intéressant de noter que déjà deux éléments font la valeur de l'information : la rareté de l'information et l'utilité de l'information.[117] Et finalement, c'est bien la presse qui est productrice de ces biens intermédiaires que sont les éléments de vie privée,[118] bien intermédiaires, monnayés au travers de la vente de ces colonnes de ragots. Plus qu'une vision économique de la vie privée, on a une première matérialisation de la monétisation de données personnelles. Cette marchandisation de l'information, couplant à la fois rareté et utilité de l'information, se retrouve aujourd'hui au cœur

[112] Richard POSNER, « The Economics of Privacy », (1980) 71-2, Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association *The American Economic Review* 405, 406.
[113] Richard POSNER, « The Right of Privacy », (1978) 12-3 *Georgia Law Review* 393, 394.
[114] *Id.*
[115] *Id.*
[116] Posner prend ici l'exemple des informations personnelles concernant les personnes riches qui se retrouvent dans les « gossip columns » et qui ont davantage de valeur que les informations de personnes pauvres car elles sont premièrement, sont plus facile à obtenir et, deuxièmement, sont plus utiles en ce qu'elles servent davantage comme modèle, *Id.*, 396.
[117] *Id.*, 394.
[118] *Id.*, 397.

de ce qu'est l'économie des données. On comprend que cette vision économique de la vie privée est parfaitement en adéquation avec une libre circulation des données personnelles à des fins de profit, au détriment de la protection des individus. Mais le raisonnement ne serait pas complet sans le deuxième élément qui est le droit de propriété sur une information privée.

Selon R. Posner toujours, l'élément de vie privée n'est pas nécessairement la propriété de celui à qui il est attaché. Succinctement, si les risques pour l'individu sont faibles concernant la divulgation de ses informations, et que les bénéfices pour le possesseur de ces éléments sont forts, alors la propriété de ces éléments de vie privée devrait être donnée à celui qui les détient.[119] Ainsi, la personne concernée n'a pas forcément voix au chapitre concernant la divulgation d'un élément de sa vie privée. En effet, pour que tel soit le cas, il faudrait que l'information soit déshonorante pour la personne concernée.[120] En d'autres termes, il faudrait qu'il y ait une atteinte ou un dommage causé à la personne. En principe, on a donc bien affaire à la description d'une théorie selon laquelle la libre circulation de l'élément de la vie privée est consacrée, tant qu'il n'y a pas d'atteinte. Dans le contexte américain, la libre circulation des données est alors loin d'être dénuée de sens. Après tout, cette théorie s'insère parfaitement dans un cadre dans lequel la vie privée est vue comme un simple recours (*tort*) et non pas comme une fin en soi. Par ailleurs, la propriété des données est une question centrale aujourd'hui et débattue ardemment en doctrine et fait logiquement écho à la libre circulation de laquelle elle émane. Si l'information à propos d'une personne circule et n'appartient pas à cette personne, alors à qui appartient-elle ? De là, découlent également les questions de marchandisation et de qui devrait en tirer les bénéfices.

Ainsi, en ajoutant une composante économique à l'édifice du concept de *privacy* à l'américaine venant réparer un *tort*, on comprend mieux pourquoi des voix se sont élevées dans la doctrine aux États-Unis, qualifiant les lois européennes de protectionnisme de l'information et de barrières non tarifaires notamment en ce qui concerne les restrictions sur les flux transfrontières de données.[121] On saisit également mieux les enjeux actuels sur la nécessité pour les acteurs faisant

[119] Ici, Posner prend deux exemples, l'un du « bureau of the census » et l'autre la vente d'une liste d'abonné par un magazine à un autre magazine. Pour le cas du magazine il considère que : « In the magazine case the costs of obtaining subscriber approval would be high relative to the value of the list. If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to the subscribers, we should assign the property right to the magazine; » *Id.*, 398.
[120] *Id.*, 399.
[121] John M EGER, « Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers », (1978) 10-4 *Law & Pol'y Int'l Bus* 1055.

du profit avec les données personnelles, de maintenir coûte que coûte la libre circulation des données. Le système de la *privacy* américaine dans son ensemble, à savoir son appréhension par le truchement des *torts*, et la composante économique de la vie privée que cette appréhension emporte, permet de banaliser la libre circulation des données, en ne consacrant pas la protection de la vie privée comme une fin en soi. En des termes plus clairs, elle permet la libre circulation des données et l'utilisation de ces dernières en conférant au détenteur, un droit de propriété arraché à l'individu auquel elles se rattachent. Cela entraîne une monétisation ou une marchandisation des données.

La vision américaine globale de la vie privée est dès lors difficilement compatible avec les pratiques législatives européennes de l'époque qui, rappelons-le, vise à protéger la vie privée comme un droit fondamental et une fin en soi. Il est donc intéressant de noter que si un pan de la doctrine américaine sur le droit à la vie privée a fortement influencé les législateurs des États européens dans les années 1970 (on pense notamment à la théorie du contrôle), elle s'inscrit globalement dans une conception juridique très distincte de celle de l'Europe. On comprend que rattacher le droit à la vie privée à la notion de dommage ouvre la porte à des interprétations larges quant à l'utilité de l'information personnelle (en l'occurrence l'utilité économique). C'est ce que l'on constate par exemple en étudiant la vision de R. Posner, qui est révélatrice de l'orientation de l'époque aux États-Unis. La conception américaine globale de la vie privée, plus libérale et plus permissive, a gagné du terrain en Europe, dès qu'il a été question de règlementer la circulation des données personnelles au niveau international. C'est à cette période que l'on peut dater le déclin de la doctrine européenne de la protection des données personnelles vu comme en fin en soi, au profit de la vision américaine plus libérale permettant de consacrer dans le même temps un principe de libre circulation transfrontière des données. Le contexte technologique changeant et l'avènement des thèses néolibérales auront constitué un terreau fertile à ce basculement.

Les premières approches internationales d'influence nord-américaine et la consécration du principe de libre circulation transfrontière des données

Les premières approches internationales en matière de libre circulation des flux transfrontières de données au début des années 1980 sont représentées par deux textes célèbres : Les *Lignes directrices de l'OCDE* de 1980 et la *Convention du Conseil de l'Europe pour la*

protection des personnes à l'égard du traitement des données à caractère personnel, dite convention 108.

1. Les lignes directrices de l'OCDE de 1980

On peut assez facilement lier les premiers travaux de l'OCDE relatifs à la régulation des flux transfrontières de données personnelles avec les travaux doctrinaux américains sur la vie privée, et notamment la « deuxième vague » de développements[122] ayant eu lieu dans les années 1960 et 1970 représentés principalement par les travaux d'A. Westin. En effet, un comité créé par l'OCDE en 1972 intitulé « Data Bank Panel » et dont la mission était l'étude de la régulation des traitements automatisés de données personnelles[123] avait organisé en 1974 un séminaire sur les politiques en matière de vie privée et de protection des données[124] pour lequel les discussions étaient fondées sur les travaux de A. Westin.[125] Ce séminaire constituera la pierre angulaire des politiques mises de l'avant par l'organisme. Il est néanmoins utile de mentionner que l'OCDE a commencé à étudier les potentiels impacts sur la vie privée du fait de l'évolution du contexte technologique de l'époque, encore plus tôt, au travers d'un groupe spécialement mandaté pour étudier le développement des banques de données, des ordinateurs et des télécommunications.[126] Ces études avaient soulevé des problèmes relatifs à la vie privée et aux données personnelles des individus concernés, consignés dans un rapport intitulé *Digital Information and the Privacy Problem* paru en 1971, dans lequel était annexée une version traduite en anglais et en français de la loi de protection des données de l'État de Hesse.[127]

À ce stade, on peut dégager deux constats. Le premier est qu'au départ, les questions de vie privée et de données personnelles étaient, du point de vue strictement juridique, abordées par l'OCDE avec une influence européenne, du fait des premiers développements législatifs du début des années 1970. Le second constat est que la philosophie américaine, du fait de l'impact des travaux de A. Westin à cette époque, exerçait déjà une influence considérable sans qu'il soit pour

---

[122] Pour rappel, la première est matérialisée par l'article de Samuel Warren et Louis Brandeis : voir, S. D. WARREN et L. D. BRANDEIS, préc., note 85.
[123] G. G. FUSTER, préc., note 43, p. 76.
[124]Michael D. KIRBY, « Transborder Data Flows and the Basic Rules of Data Privacy », (1980) 16 *Stan J Int'l L* 27, 42.
[125] G. G. FUSTER, préc., note 43, p. 76.
[126]*Id.*
[127] *Id.*

le moment question de libre circulation des données ou d'« économie de l'information ». Il se pourrait cependant que la boîte de Pandore ait été ouverte à ce moment, puisque par la suite, c'est bien l'ensemble de la théorie de la vie privée américaine que l'on va retrouver en Europe, à savoir, une conception par le truchement des *torts*, assortie d'une composante économique de la vie privée, et non plus seulement les seuls travaux d'A. Westin sur la théorie du contrôle.

Ainsi, il faudrait avant tout voir dans ces travaux internationaux, des influences juridiques fondues l'une dans l'autre, avant même de développer d'autres facteurs économiques, politiques et sociaux ouvrant la voie à la libre circulation des données. En effet, nous avons jusqu'ici développé, d'une part, les composantes des prémices du droit européen à la protection des données eu égard aux contextes technologiques et sociaux (et plus précisément la réglementation des flux transfrontières de données déjà existante) de l'époque, et d'autre part, la vision américaine de la vie privée qui tend naturellement vers une libre circulation eu égard à la conception doctrinale globale qui en est faite. Il ne s'agit pas simplement d'en faire une note informative, mais bien d'expliquer que la réglementation contemporaine des flux transfrontières de données résulte bien au début, d'une double influence américano-européenne. Cette double influence, nous aurons l'occasion d'y revenir, ne va pas totalement disparaître, l'une prenant progressivement le pas sur l'autre. C'est dans le premier texte international à valeur juridique sur le droit de la protection des données personnelles, que représente les *Lignes directrices de l'OCDE*, que la théorie américaine de *privacy* va gagner du terrain. C'est également à ce moment-là que des paramètres extrajuridiques, de nature économique, rentrent en ligne de compte. Ces paramètres extrajuridiques sont précisément la raison pour laquelle la promotion de la libre circulation des données personnelles d'une frontière à une autre a eu le vent en poupe et pourquoi c'est bien un courant d'obédience américaine qui, dans les faits, s'est imposée.

Si l'on reprend le fameux séminaire de 1974[128] sur lequel nous nous sommes brièvement arrêtés, il faut noter que ce dernier a conduit à la création en 1978 d'un groupe d'experts mandatés pour l'étude de la vie privée et des flux transfrontières de données et l'élaboration de lignes directrices. Il est intéressant de noter que ce groupe avait pour mission : « d'étudier les problèmes juridiques et économiques liés au flux transfrontalier de données non personnelles afin de fournir

[128] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Policy issues in data protection and privacy : concepts and perspectives : proceedings of the OECD seminar 24th to 26th June 1974*, OECD Publications Center, coll. OECD Informatics studies, n°10, Paris, 1976.

une base pour l'élaboration de lignes directrices dans ce domaine afin de prendre en compte le principe de libre circulation de l'information. »[129] On a alors, d'une part, une organisation internationale dont les États membres se soucient de savoir quelles vont être les conséquences de ces nouveaux modes de traitement automatisées, notamment en ce qui a trait au respect des droits des individus concernés[130], mais on a, d'autre part, la prise en compte du développement de l'économie de l'information, optimisé par le contexte technologique permettant un traitement automatisé de l'information. À cet égard, n'oublions pas que la mission première de l'OCDE est avant tout économique.

Les travaux de Friedrich Hayek dans les années 1945[131] auront été le point de départ de l'information comme valeur économique et du développement d'un courant économique connu sous le nom d'« économie de l'information », notamment sous la plume de George J. Stigler, auteur d'un article éponyme paru en 1961 dans la revue *The Journal of Political Economy*. Au début des années 1960, la théorie de l'économie de l'information intervient dans un contexte dans lequel l'économie est de plus en plus rythmée par l'informatisation de la société, ce qui a poussé à se poser des questions sur la nature de l'information, son interaction avec l'économie et *in fine* sa valeur.[132]

L'interaction entre l'information et l'économie a principalement été étudiée sous deux angles. Un premier angle, privilégié par les chercheurs en science de l'information, consistait à définir les contours de l'information et à l'étudier comme un produit économique avec les conséquences qui y sont attachées (achat, vente, usage, droit de propriété, etc.).[133] À ce titre, l'appréhension du caractère économique de la vie privée par le droit en *privacy* américaine, notamment par le biais de R. Posner, est dans la continuité de ces questions.[134] Le second angle, privilégié par les économistes, consistait à étudier le rôle de l'information dans l'économie que ce

[129] M. D. KIRBY, préc., note 124, 43.
[130] F. W. HONDIUS, préc., note 68, 91.
[131] Nous faisons ici référence à l'article fondateur « The Use of Knowledge in Society » paru dans la revue American Economic Review dans lequel il considère que les problèmes économiques sont résolus efficacement à la lumière de connaissances spécifiques et pratiques détenues par les individus. De ce fait, il plaide pour une décentralisation de l'économie prenant en compte les choix économiques basés sur de telles connaissances. Cependant, il plaide également pour qu'un degré commun de connaissances minimal circule de façon à garder une coordination dans l'économie au plan large. Cette communication de l'information serait faite au travers du système de prix. Friedrich August VON HAYEK, « The Use of Knowledge in Society », (1945) XXXV-4 *American Economic Review* 519.
[132] Will WHEELER, « Economics of Information: a brief introduction », (2011) 36/37 *Progressive Librarian* 42, 42.
[133] *Id.*, 43
[134] *Supra*, p. 34.

soit sur le processus de décision des individus dans leurs choix économiques[135], mais également les impacts des flux d'informations sur le marché et la distribution de l'information et son influence sur l'économie. L'information est alors devenue assez rapidement une question centrale dans l'économie à la fin des années 1970 et au début des années 1980. Là encore, on comprend mieux le développement concomitant de positions doctrinales américaines, visant à insérer dans le droit à la vie privée, une composante bénéfices/risques consacrant ainsi la libre circulation des données à des fins économiques.[136] Cette position s'articulait parfaitement avec les développements en économie de l'information de l'époque. En effet, les données personnelles se rattachent à la vie privée certes, mais elles restent des données appréhendées comme un produit économique.

Lors d'une réunion de l'OCDE portant sur les flux transfrontières de données et la protection de la vie privée, l'accent avait été mis sur la valeur économique de l'information et ses potentielles dérives par Louis Joinet, à l'époque président de la CNIL, qui considérait que :

> « Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows ».[137]

Dès lors, du fait de la place de l'information dans l'économie, à en croire Louis Joinet, un des risques à appréhender dans la rédaction des futures lignes directrices était la potentielle perte de souveraineté informationnelle pour les États, du fait de la circulation internationale des données.[138] On peut penser que l'on s'éloigne du sujet, mais au contraire : les trente années suivantes ont démontré que la perte de la souveraineté informationnelle des États, induite par l'obligation de libre circulation des données pour des raisons économiques, impliquait souvent un abaissement de la protection de la vie privée au sein des États. À cet égard L. Joinet avait appréhendé de manière clairvoyante, une des dérives de l'internationalisation des règles sur les données personnelles que nous traiterons dans la troisième partie.[139]

---

[135] Ce que l'on donnera lieu plus tard à l'apparition du courant de l'économie comportementale.
[136] *Supra*, p. 35.
[137] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers, 176, coll. OECD Publishing, Paris, France, OECD, 2011, p. 10.
[138] *Id.*
[139] *Infra*, p. 121.

Le mémorandum explicatif du groupe d'experts mandaté par l'OCDE soulevait également que les intérêts de vie privée pussent être confondus avec d'autres intérêts de nature commerciale, culturelle, ou encore de souveraineté nationale.[140] Dès lors, ces lignes directrices devaient répondre à plusieurs enjeux croisés. Les intérêts commerciaux notamment induisent un niveau de libre circulation des données élevé, ce qui signifie qu'une trop grande protection pourrait nuire à ces intérêts. Dès lors, un juste milieu devait être trouvé entre protection/libre-circulation, si tant est que l'on considère la protection des données comme un frein à la libre circulation, comme c'était la position de l'OCDE dans le mémorandum.[141]

Ainsi, les Lignes directrices de l'OCDE, dont nous vous proposons un rapide tour d'horizon, en mettant l'accent sur la réglementation des flux transfrontières de données, qui consacre un principe de libre circulation des données sont révélatrices de deux oppositions. La première opposition est une différence de conception juridique de la vie privée et la protection des données personnelles entre les doctrines européennes et états-uniennes. Nous aurons l'occasion de constater que concernant les flux transfrontières de données, c'est bien la philosophie américaine que l'on retrouve dans ces *Lignes directrices*, du fait de l'empreinte importante du concept de *privacy* dans les travaux préparatoires et dans le texte final. La seconde opposition, c'est l'opposition entre protection des données et libre circulation des données.

En 1980, à la suite des différentes études et travaux, l'OCDE publie les *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données à caractère personnel*,[142] texte dans lequel la double opposition mentionnée plus haut transparaît. Ces Lignes directrices couvrent certains aspects de protection des données qui ne seront pas abordés ici, priorité étant faite aux mesures concernant la réglementation des flux transfrontières de données. Sur ce point, les *Lignes directrices* établissent surtout le principe de libre circulation des données entre les pays membres de l'OCDE.[143] Par exemple, l'article 16 dispose que :

---

[140] OECD, préc., note 137, p. 10.
[141] *Id.*
[142] ORGANISATION DE COOPERATION ET DEVELOPPEMENT ÉCONOMIQUES, *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 1980, en ligne : <https://www.oecd-ilibrary.org/docserver/9789264296398-fr.pdf?expires=1657048928&id=id&accname=ocid43014084&checksum=10CE661288DA17325BE1CB630986BAC3>.
[143] *Id.*

> « Les pays membres devraient prendre toutes les mesures raisonnables et appropriées pour garantir que les flux transfrontières de données à caractère personnel, y compris le transit par un pays membre, soient ininterrompus et sécurisés. »[144]

Cet article démontre assez clairement que si les intérêts de protection des données existent, ils ne peuvent être favorisés au détriment de la libre circulation. Ainsi, la libre circulation reste bien le principe qui doit gouverner les flux transfrontières de données personnelles entre les pays membres de l'OCDE. Mais le point de bascule est bien l'article 18 qui reconnaît implicitement la protection des données comme une barrière non tarifaire et qui grave dans le marbre la suggestion présente dans le mémorandum explicatif, en ce qui concerne la confusion entre intérêts relatifs à la vie privée et intérêts économiques.[145] Pour rappel, le mémorandum insinuait que les intérêts de vie privée, s'ils venaient à trop limiter la libre circulation transfrontière des données, pouvaient être dommageables pour l'économie de l'information. Ainsi, l'article 18 des lignes directrices protège la libre circulation des données et les intérêts économiques qui en découlent :

> « Les pays membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-delà des exigences propres à cette protection. »[146]

Dès lors, en deux articles, on retrouve bien les éléments qui ont été caractérisés en amont, à savoir l'importance de préserver des intérêts que seule la libre circulation peut préserver et qu'*a contrario* une trop forte protection des données freinerait : il s'agit principalement des intérêts économiques inhérents au développement de l'économie de l'information. Rappelons à cette fin que l'OCDE est une organisation dont les objectifs et les aspirations sont principalement économiques.

Finalement, ces deux sections ne représentent-elles pas l'avènement d'une vision américaine du droit à la vie privée qui, *de facto*, embrasserait une vision assez restrictive de la

---

[144] *Id.*, art. 16
[145] OECD, préc., note 137, p. 10.
[146] *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, préc., note 142, art. 18.

protection des données quand il est question de flux transfrontières ? On est en droit de le penser puisque libellé en ces termes, l'article 18 peut être interprété comme l'absence d'un droit à la vie privée général et qu'à ce titre, il ne peut être mis en place de mesure de prévention (notion d'« exigences propres à cette protection »). Autrement dit, les lois, politiques et procédures mises en place par les États doivent intervenir dans la réparation d'un dommage, ce qui signifie *a contrario* que tant que le dommage n'a pas lieu, le principe de libre circulation s'applique. Dans ce cas de figure, la philosophie américaine contemporaine du droit à la vie privée permet de promouvoir une libre circulation quasi sans limites, là où la philosophie européenne serait moins libérale.

S'il s'agissait de freiner le protectionnisme informationnel induit par les lois de protection des données personnelles européennes, certains principes issus du droit européen de l'époque ont tout de même été conservés dans l'article 17,[147] afin de maintenir un certain degré de protection dans les législations internes sur les flux sortants.[148] Juste arbitrage, maigre consolation ou pragmatisme libéral, reste que dans les faits, c'est la première fois qu'un texte à valeur juridique vise à restreindre la protection des données personnelles au profit de considérations autres que le droit à la vie privée. Ce texte prend notamment en compte des considérations économiques, démontrant dans le même temps toute l'influence de la doctrine américaine de l'époque. Cet outil juridique international est le point de départ à l'instauration de la libre circulation en droit international public (et plus tard en droit du commerce international) à des fins économiques, restreignant de ce fait la capacité des États à légiférer à contre-courant.[149] Il marque également le début du déclin de la doctrine européenne de la protection des données personnelles comme une fin en soi, doctrine qui s'attelait justement à ne pas faire prévaloir la libre circulation sur la protection. Cependant, la valeur non contraignante de ces lignes directrices n'était en théorie pas de nature à remettre en cause la souveraineté des États quant à la possibilité de légiférer en matière de protection des données. L'avènement de la *privacy* américaine et le principe de libre circulation

[147] « Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, sauf lorsqu'un ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de protection équivalente. », *Id.*, art. 17.
[148] *Id.*
[149] *Infra*, p. 118.

internationale des données à des fins économiques se sont théoriquement imposés aux États avec l'adoption de la *Convention 108* du conseil de l'Europe.

2. La convention 108 de 1981

S'il peut paraître logique que l'OCDE, par les missions dont elle a la charge et notamment les missions économiques,[150] puisse étudier ces questions sous un angle que nous qualifierons ici de libéral, il est plus surprenant que le Conseil de l'Europe, qui de prime à bord est un espace juridique commun axé sur le développement de la protection de l'individu, ait apporté des réponses à ces questions dans des termes assez équivalents.

Il convient de mentionner que le Conseil de l'Europe a également développé une réflexion en matière de protection des données assez tôt, dans les années 1970. Elle a abouti dans un premier temps à deux résolutions en 1973 et 1974, concernant les banques de données électroniques dans les secteurs privé et public. Dans ces dernières, le Conseil se retire délibérément et laisse les États s'occuper de ces questions. Ainsi, ils recommandent aux gouvernements des États membres : « de prendre toutes les mesures qu'ils jugent nécessaires pour donner effet aux principes énoncés dans l'annexe à la présente résolution ».[151] On assiste alors dans un premier temps à un raisonnement logique et dans la continuité des valeurs qui sont promues par le Conseil de l'Europe, puisqu'est laissé aux États, le soin d'organiser la protection des données autour de dix principes.[152] Cette mise en retrait n'est d'ailleurs pas si surprenante, puisqu'on assiste parallèlement aux premiers développements législatifs européens en matière de protection des données. Et si ces derniers se font en ordre dispersé, ils sont surtout peu nombreux. Pour rappel il n'y avait en 1973 et 1974 que très peu de législations *ad hoc*, et c'est surtout dans la deuxième moitié des années 1970 que ces dernières ont fleuri. Cela peut être une explication de la passivité du Conseil de l'Europe, d'autant

---

[150] OECD, « À propos », *oecd.org*, en ligne : <http://www.oecd.org/fr/apropos/#:~:text=La%20mission%20de%20l%27Organisation,social%20partout%20dans%20le%20monde.>.

[151] COUNCIL OF EUROPE, COMMITTEE OF MINISTERS, *Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Private Sector*, (73)22,1973. ; COUNCIL OF EUROPE, COMMITTEE OF MINISTERS, *Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector*, (74)29,1974.

[152] *Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Private Sector*, préc., note 151; *Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector*, préc., note 151.

plus que le droit à la vie privée était consacré à l'article 8 de la Convention européenne des droits de l'homme, et qu'il a semblé dans un premier temps suffisant pour répondre aux défis technologiques.[153]

Cet article 8 a d'ailleurs beaucoup fait parler de lui à la fin des années 1960 comme nous allons maintenant l'observer, puisqu'il est au cœur du basculement doctrinal en droit de la vie privée et de la consécration de la libre circulation des données, qui va intervenir sur le vieux continent. C'est précisément dans l'évolution de l'interprétation de l'article 8 que l'on assiste à une américanisation du concept de la vie privée en Europe, jusque dans la sémantique employée et dans le sens que l'on donne aux mots. En effet, une précision terminologique doit être soulignée. L'article 8 de la Convention européenne des droits de l'homme fait référence au « droit à la vie privée », traduit littéralement en version anglaise par « Right to respect for private and family life ».[154] La notion de droit à la vie privée n'était donc pas initialement traduite en anglais, par le terme de *privacy,* contrairement à la Déclaration universelle des droits humains qui, elle, consacre le terme de « *privacy* » à son article 12.[155] Pour cette raison, la Cour européenne des droits de l'homme avait toujours soigneusement évité d'utiliser le terme « *privacy* », y voyant justement un lien direct avec la doctrine juridique sur le droit à la vie privée développée à la même période aux États-Unis. Il convient alors de souligner qu'eu égard à cette différence sémantique, les juges de Strasbourg se gardaient bien d'interpréter le droit à la vie privée au prisme de la philosophie américaine, à savoir comme un *tort*.[156]

Ce n'est qu'en 1967, à l'occasion de motions soumises entre différents organes du Conseil de l'Europe, portant notamment sur les impacts des développements technologiques et, plus précisément, sur les outils d'écoute clandestine et leurs impacts sur la vie privée, que la sémantique a changé.[157] Sans surprise, ce sont les travaux de l'époque d'Alan Westin qui ont contribué à faire entrer le terme *privacy* dans le vocabulaire juridique du Conseil de l'Europe.[158] En effet, certains

[153] G. G. FUSTER, préc., note 43, p. 84.
[154] *Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales*, 4 novembre 1950, S.T.E. n° 5 (entrée en vigueur le 3 septembre 1953) [Convention européenne des droits de l'homme], art. 8.
[155] UNITED NATIONS, *Déclaration universelle des droits de l'homme*, Rés. 217 A (III), Doc. off. A.G.N.U., 3e sess., suppl. n° 13, p. 17, Doc. N.U A/810 (1948), art. 8. Dans ce texte, on traduit « *droit à la vie privée* » par « *privacy* », ce qui n'est pas le cas dans la Convention européenne des droits de l'homme.
[156] G. G. FUSTER, préc., note 43, p. 82.
[157] *Id.*, p. 83.
[158] *Id.*

représentants du comité légal du Conseil de l'Europe, dont M. Czernetz, utilisèrent le mot *privacy* et non la notion de *right to respect for private life,* dans certaines conclusions. Ces dernières citaient les travaux de A. Westin,[159] ce qui renvoyait à la réalité juridique outre-Atlantique. On peut par conséquent dater à cette période, le changement de sémantique et le basculement vers l'usage du terme de *privacy,* pour renvoyer au droit à la vie privée en Europe. Ces conclusions naquirent des interrogations sur la capacité de l'article 8 de la Convention à protéger efficacement la vie privée (cette fois entendue au sens de *privacy*) et plus spécialement au regard de l'usage grandissant des ordinateurs.[160] Cette problématique avait fortement incité le Conseil de l'Europe à protéger les individus et leur vie privée face aux développements technologiques de l'époque. Mais cet épisode a également contribué à confondre les terminologies renvoyant au droit à la vie privée et donc à brouiller les frontières entre les philosophies juridiques européenne et américaine.

Ce changement terminologique peut paraître anodin, mais il a considérablement influencé la manière dont la doctrine de *privacy* à l'américaine s'est répandue en Europe. Pour rappel, le droit à la vie privée à l'européenne, entendu en anglais comme *right to private life* est un droit fondamental (consacré par la *Convention européenne des droits de l'homme* et ancré dans plusieurs constitutions d'États européens). C'est également un droit général, plaçant par principe les intérêts de protection des données au-dessus du reste même si ce n'est pas pour autant un droit absolu. La *privacy* américaine obéit quant à elle à la règle des *torts* et n'existe que pour réparer un dommage. On comprend donc que la confusion juridique de ces termes en Europe a bouleversé l'approche européenne initialement plus protectrice que sa voisine américaine. On se doit de garder en tête ce changement de sémantique, lorsqu'il s'agit d'expliquer comment l'approche libérale américaine a été privilégiée dans la Convention 108 et, plus largement, en Europe à la fin des années 1970 et au début des années 1980, à des fins de libre circulation des données. De prime à bord, on pouvait s'attendre à un raisonnement juridique plus *européaniste* de la part du Conseil de l'Europe dans la convention 108.

Un autre aspect pouvant expliquer la teneur du texte de la convention 108, c'est la nécessité d'être en adéquation avec les *Lignes directrices de l'OCDE*, comme en témoigne un échange de lettres entre le comité d'experts en protection des données du Conseil de l'Europe et de l'OCDE.

[159] *Id.*, p. 83.
[160] *Id.*, p. 84.

Dans cet échange, les deux entités tombaient d'accord sur la nécessité de coopération et d'assistance mutuelle, ainsi que sur le principe de libre circulation des données, afin d'empêcher les obstacles non tarifaires que constitueraient des mesures trop protectrices mises en œuvre par les États.[161] À cela s'ajoute l'ouverture du traité aux pays non membres du Conseil de l'Europe, ayant permis à certains observateurs, dont les États-Unis, de participer aux travaux préparatoires.[162]

Au vu de tous ces éléments, il n'est alors pas surprenant d'observer la consécration du principe de la libre circulation des données par la convention du Conseil de l'Europe. Comme il a été mentionné, sur le plan juridique, le remplacement terminologique du terme anglais *right to respect for private life* en *privacy* a sans doute contribué à introduire une conception doctrinale plus américaine dans le texte : les mots ont un sens. Cette conception fondée sur la réparation du dommage, comme nous l'avons souligné, est plus facilement compatible avec la libre circulation des données. Combiné aux facteurs économiques et politiques, le texte reflète assez bien les réalités juridiques de l'époque concernant les flux transfrontières de données. L'avènement de la *privacy* américaine est plus compatible avec une libre circulation des données transfrontières pour des motifs économiques, que l'est la conception européenne du début des années 1970. Par ailleurs, ce texte constitue le premier outil juridique régional contraignant en droit des données personnelles. Pour ce qui intéresse la règlementation sur les flux transfrontières de données à caractère personnel, le texte prévoyait notamment à l'article 12 :

> « Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie. »[163]

Même si le texte ne précise pas explicitement que la protection des données dans les flux transfrontières peut être considérée comme un obstacle, il indique que la protection de la vie privée ne doit pas stopper la libre circulation servant des intérêts concurrents. Ainsi, on assiste à une mise en balance entre le principe de la libre circulation et la protection des données. *De facto*, on est bien dans une logique américaine de droit à la vie privée, puisque le texte court-circuite les mesures trop préventives qui viendraient impacter la circulation des données. Dans les faits, on comprend que

[161] *Id.*, p. 87.
[162] *Id.*
[163] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 novembre 1981, S.T.E. n° 108 [Convention 108].

la protection de la vie privée ne peut être l'unique fin gouvernant la protection des données. D'autres fins, facilitées par la libre circulation, doivent être prises en compte qu'elles soient économiques, technologiques ou sociales. Ces dernières doivent avoir le même poids que l'objectif de protection de la vie privée. Encore une fois, on est dans l'optique où le droit à la vie privée interviendrait pour réparer un dommage et non pas pour prévenir d'une atteinte, puisque cette dernière option impliquerait une limitation trop grande de la libre circulation des données.

Pour garantir la libre circulation des données, l'un des principaux objectifs de cette convention était d'harmoniser le droit des données personnelles dans les pays participants en obtenant l'engagement des parties de transposer les principes de la Convention.[164] On peut également supposer qu'une des volontés sous-jacentes était de mettre fin aux régimes spécifiques sur les transferts internationaux de données personnelles au sein des législations nationales, ce qui n'a été qu'une réussite partielle. Pour rappel, au moins deux modèles de régulation impliquant des régimes spéciaux existaient dans certaines lois *ad hoc* européennes. On pense en effet au système de licence à la suédoise pour les transferts internationaux dont les certificats étaient délivrés par les autorités. C'est également le cas du modèle d'enregistrement à la française nécessitant des formalités supplémentaires pour permettre le transfert de données personnelles à l'étranger.[165] La ratification de la Convention a parfois entraîné la transposition des règles relatives aux flux transfrontières de données dans la législation des États-parties ou leur interprétation par les autorités de protection des données. Par exemple, l'autorité allemande de protection des données a déclaré, au début de 1981, que la loi allemande autorise un flux transfrontière de données si le pays d'accueil dispose d'un niveau de protection équivalent[166] conformément au paragraphe 3 de l'article 12.[167] Au Royaume-Uni, la loi sur la protection des données de 1984 a également incorporé

[164] *Id.*, art. 4.
[165] *Supra*, p. 26.
[166] Klaus BOHLOFF et Axel BAUMANNS, « Harmonising German Data Protection and the Council of Europe Convention », (1984) 12 *Int'l Bus Law* 175, 179.
[167] « 1. Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement. 2. Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie. 3. Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2 : a. dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente ; b. lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter

le niveau de protection équivalent prévu dans la Convention 108.[168] Cependant, l'efficacité de cette transposition doit être nuancée. En effet, la Convention n'a pas eu pour effet de démanteler les régimes étatiques spécifiques sur les transferts internationaux de données, en attestent les situations *post*-Convention en Suède[169] ou encore en France. Ce dernier État a abrogé son système d'enregistrement sur les transferts de données seulement au moment de la transposition de la directive de 1995 dans la loi française, par la loi de 2004 pour répondre aux exigences de l'Union en matière de droit des données personnelles.[170]

De plus, il s'agit d'une convention internationale ratifiée par les États membres du Conseil de l'Europe ainsi que certains pays invités. Cela signifie que les règles de la Convention ont vocation à s'appliquer entre États signataires seulement. Ces États restent donc libres quant à la mise en place de dispositions sur les flux transfrontières s'appliquant aux États non-signataires. Même si la transposition du texte n'a pas toujours été très rigoureuse de la part de certains États comme c'est le cas de la France ou de la Suède, on peut néanmoins considérer que le droit à la vie privée et à la protection des données des années 1970 « à l'européenne » comme fin en soi, prend du plomb dans l'aile avec cette Convention. Peut-on pour autant considérer que le principe de libre circulation des données a eu des effets tangibles sur l'économie ? Ne relevait-il plutôt pas de l'idéologie ? C'est ce sur quoi nous allons nous attarder, maintenant que nous avons pu planter le décor en ce qui concerne le basculement d'une protection des données à l'européenne vers un concept de *privacy* à l'américaine par le truchement d'outils de droit international public règlementant les flux transfrontières de données.

Chapitre 2 : La libre circulation idéologique : de ces effets mitigés sur le développement de l'économie et sur le progrès technologique

Jusqu'à maintenant, nous avons abordé l'abandon progressif de la doctrine de protection des données comme fin en soi à l'européenne, au profit de la doctrine de *privacy* américaine. Cette

que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe. », *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, préc., note 163, art. 12.

[168] K. BENYEKHLEF, préc., note 17, p. 249.

[169] S. ÖMAN, préc., note 47, 390.

[170] *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. 7 août 2004.

dernière aura permis de consacrer un principe de libre circulation en droit international public du fait de son caractère plus permissif. Le principe de libre circulation s'imbriquait dans l'avènement des thèses néolibérales pour lesquelles le marché est l'entité suprême et l'intervention de l'État, néfaste. Ainsi, la protection des données personnelles a été reléguée au second plan sur le fondement de promesses de progrès technologique, synonyme de croissance économique. Pour autant, est-ce que la mise au service de la règle de droit, comme nous l'avons vu dans les *Lignes directrices de l'OCDE* et la *Convention 108,* pour assurer cette libre circulation des données à des fins économiques était justifiée ? En d'autres termes, avait-on prévu les effets de ces politiques et de leurs répercussions sur la protection des données ou bien était-ce davantage guidé par l'idéologie ?

Pour répondre à cette question, il convient d'abord de relever que le marché des technologies de l'information a connu un changement majeur depuis les années 1970 jusqu'à nos jours. Il s'agit du passage des technologies de l'information comme *support* de l'activité économique, au traitement de la donnée, devenue une *caractéristique* de l'économie à part entière. Pour autant il semblerait que, dans un cas comme dans l'autre, le principe de libre circulation des données ait davantage été guidé par l'idéologie et que ces effets réels soient à relativiser. Tandis que le développement des technologies de l'information comme support de l'activité économique paraît difficilement justifier les politiques de l'époque favorisant les échanges de données (Section 1), nous devons nous interroger sur l'influence du droit à libre circulation des données dans une économie pour laquelle le traitement des données est devenu une caractéristique essentielle (Section 2).

Section 1 : Les technologies de l'information comme support de l'activité économique : un argument discutable pour justifier les politiques de libre circulation des données

Dans notre partie sur le contexte technologique en Europe ayant favorisé l'émergence de lois de protection de données en Europe, nous avons pu aborder succinctement l'état du marché de « l'informatique » à la fin des années 1960 et dans les années 1970. Nous avons également constaté que le principe de libre circulation des données avait été entériné par la suite, pour des raisons économiques notamment, mais sans que nous ayons vraiment pu entrer dans le détail, quand il a été question d'aborder successivement la doctrine américaine de *privacy* et l'avènement de cette

dernière dans les premiers outils de droit international public en matière de données personnelles. C'est ce que nous vous proposons de faire maintenant.

Cette vision du développement des technologies de l'information et du traitement des données au service d'un dopage de l'économie, des promesses de création de nouveaux marchés et d'accélération de la croissance est somme toute, celle que l'on retrouve entre le milieu des années 1970 et le milieu des années 1990. L'informatisation de la société, déjà bien avancée, ouvrait de nouvelles perspectives économiques. En Europe, en 1976, des analyses montraient que l'informatisation de la société se faisait pratiquement à parts égales dans les entreprises et en dehors des entreprises,[171] pour un parc informatique d'une valeur avoisinant les 25 milliards de dollars. Plus tard, aux États-Unis, en 1984, quasiment sept millions de ménages possédaient un ordinateur pour le foyer, soit 8,2 % des ménages.[172] Et plus de 25 % de la population active utilisait un ordinateur au travail.[173] Au Canada à la même époque, c'est plus de 10 % des ménages qui avaient accès à un ordinateur.[174] L'apparition, puis la démocratisation, du micro-ordinateur auront également permis l'informatisation de la production dans les usines dans les années 1980 entraînant notamment l'accroissement de la production, dite de « niche », en dopant la production de produits hyper spécialisés avec des lignes d'assemblage plus performantes.[175] Économiquement parlant, le développement du traitement automatisé des données à l'époque est davantage perçu comme un outil qui favoriserait la concurrence et l'adaptation au marché pour les entreprises.[176] Dès lors jusqu'au milieu des années 1990, le développement des technologies de l'information est considéré comme un *support* de l'activité humaine et notamment de l'activité économique. En effet, l'informatisation de la société aura eu pour conséquence non pas, l'apparition de nouvelles manières de produire, mais principalement la « modernisation » des moyens de production. Par conséquent, la libre circulation des données et notamment des données personnelles se justifiait politiquement par la volonté de ne pas entraver le développement technologique perçu comme un

---

[171] S. NORA et A. MINC, préc., note 12, p. 658.
[172] Robert KOMINSKI et U.S DEPARTMENT OF COMMERCE, BUREAU OF THE CENSUS, *Computer Use in the United States: 1984*, Current Population Reports, 155, coll. Special Studies Series P-23, Washington, D.C., U.S Government Printing Office, 1988, p. 1.
[173] *Id.*
[174] OECD, *Perspectives des technologies de l'information de l'OCDE*, coll. Technologies de l'information et des communications, Paris, France, OECD, 2004, p. 397.
[175] Melvin KRANZBERG et Michael T. HANNAN, « History of the Organization of Work Automation », *Britannica.com*, en ligne : <https://www.britannica.com/topic/history-of-work-organization-648000/Automation>.
[176] COMMISSION EUROPEENNE, *Croissance, compétitivité, emploi ; Les défis et les pistes pour entrer dans le XXIe siècle*, Livre blanc, Bruxelles, Commission Européenne, 1994, p. 111.

catalyseur de l'économie. En effet, cette volonté de ne pas entraver, de ne pas contraindre, est la doctrine fondamentale de l'Union européenne depuis les années 1980, englobant tous les aspects de la technologie et du développement technologique dont le traitement automatisé de données fait partie. Des mots de Laurence Jourdain, il s'agit d'une « interprétation économiste et libérale de l'enjeu scientifique et technologique »,[177] jusque dans les politiques de recherche communautaire, dictées par l'idéologie néolibérale de l'époque, la reconnaissance des intérêts privés et les volontés de « hands-off », afin de répondre aux demandes du marché.[178] Évidemment, dans ce contexte, le développement des technologies de l'information auquel la question des données est intimement liée ne fait pas exception. Au milieu des années 1990, les investissements des pays du G7 en matière de technologies de l'information avaient fortement augmenté[179], conséquence des politiques menées au début des années 1980 en matière de développement de l'informatique et de la production à moindre coût des matériels informatiques. Après 1995, la part des technologies de l'information dans le capital des entreprises avait pratiquement doublé dans les pays du G7,[180] ce qui semble attester d'une tendance générale au succès des politiques menées, favorisant le traitement et les échanges d'informations, parmi lesquelles, la consécration du principe de libre circulation des données personnelles en droit figure en bonne place.

Pour autant, il semblerait que les politiques qui ont été menées dans les années 1980 aient été un pari plus qu'autre chose, puisqu'avant le milieu des années 1990, peu de corrélations entre les investissements dans les technologies de l'information et le développement économique étaient observées.[181] Certains chercheurs établissaient par exemple que ces investissements dans les technologies de l'information étaient concomitants à la baisse de la productivité au milieu des années 1970 aux États-Unis.[182] [183] Selon Robert Gordon, la productivité a connu un ralentissement

---

[177] Laurence JOURDAIN, « La Commission européenne et la construction d'un nouveau modèle d'intervention publique. Le cas de la politique de recherche et de développement technologique », (1996) 46-3 *Revue française de science politique* 496, 507.
[178] *Id.*
[179] Dale W. JORGENSON et Khuong VU, « Information Technology and the World Economy », (2005) 107-4 *Scandinavian Journal of Economics* 631, 633.
[180] *Id.*, p. 639.
[181] Jason DEDRICK, Vijay GURBAXANI et Kenneth L. KRAEMER, « Information technology and economic performance: A critical review of the empirical evidence », (2003) 35-1 *ACM computing Surveys* 1, 2.
[182] *Id.*
[183] Ce qui a donné une décennie plus tard le fameux paradoxe de Solow : « you can see the computer age everywhere but in the productivity statistics » théorisé par Robert Solow, prix nobel d'économie dans un article du New York Times du 12 juillet 1987. Ce paradoxe a pu être induit par le fait que les investissements en matière de technologies de

important sur la période allant de 1970 à 1995,[184] période à laquelle, paradoxalement, le développement des technologies de l'information a explosé. Cette baisse de la productivité est corrélée à la baisse de la stimulation de la production produite par les inventions de la seconde révolution industrielle qui auront eu des effets durables. L'informatisation de la société aura, certes, permis un rebond de la productivité à partir du milieu des années 1990. Cela correspond à l'apparition du traitement des données comme caractéristique à part entière de l'économie, induite par le développement de ces technologies. Pour autant, il semble que les impacts de cette troisième révolution industrielle soient limités, puisque depuis le milieu des années 2000, on assiste à nouveau à un ralentissement du taux de productivité.[185] Sur la corrélation entre développement des technologies et croissance économique, Robert Gordon suggère dans *The Rise and Fall of American Growth*, que la troisième révolution industrielle, associée à l'informatisation de la société, était loin d'avoir eu les mêmes impacts que la deuxième révolution industrielle du début du XX^{e} siècle.[186] Il considère en effet que, sans dénigrer les apports de nouveaux moyens de communication de l'information, cette informatisation n'avait pas radicalement transformé la société dans tous ses aspects, comme cela a pu être le cas pendant la deuxième révolution industrielle à l'époque des grandes inventions.[187] En effet, cette dernière a profondément bouleversé les modes de production et de consommation en matière de biens de consommation comme la nourriture ou les vêtements, les équipements ménagers, mais également les loisirs, les communications ou encore les transports.[188] Pour lui, la croissance économique des années 1960 jusqu'aux années 1970 est davantage imputable aux inventions de la deuxième révolution industrielle, qui continuaient de se démocratiser à l'ensemble des ménages.[189] Tout cela tend à montrer qu'en effet, les politiques du début des années 1980 pour accélérer l'économie basée sur l'informatisation de la société aient été menées sur la base de spéculations. Les taux de productivité de l'époque dans les pays industriels semblent en recul et on assiste à ce qui ressemble à l'achèvement de la deuxième révolution industrielle et la démocratisation de ses inventions. De

---

l'information n'ont pas toujours été suivi par des remises en question organisationnelles, Robert M. SOLOW, « We'd Better Watch Out », *The New York Times*, éd. The New York Times Company, sect. New York times Book Review, 12 juillet 1987, p. 36.

[184] Robert J. GORDON, *The Rise and Fall of American Growth: The U.S. Standard of Living since the Civil War*, Princeton, NJ, Princeton University Press, 2016, p. 341.

[185] *Id.*, p. 351.

[186] *Id.*, p. 639.

[187] *Id.*

[188] *Id.*

[189] *Id.*, p. 345.

plus, ces tendances ne plaidaient pas franchement en la faveur d'un développement des technologies de l'information comme support de l'économie. Il semble au contraire que les politiques de l'époque soient basées sur les chiffres impressionnants du développement et du déploiement des technologies de l'information des années 1970-1980, tout en omettant de confronter ses chiffres avec des indicateurs de développement économique, comme le taux de productivité et la croissance.

De surcroît, la définition des investissements relatifs aux technologies de l'information était mal délimitée. Faisait-on référence aux investissements en matière de *hardware*, de *software*, de services, ou bien les trois réunies ?[190] Ainsi, il était difficile de définir le rôle des technologies de l'information et de mesurer leur efficacité dans la production. Certains chercheurs, comme Shoshanna Zuboff avait distingué l'usage des technologies dans une entreprise en trois catégories qu'étaient, l'automatisation des procédés, l'amélioration de la qualité de l'information et la transformation des procédés de production, chaque catégorie ayant un impact sur la productivité.[191] Il y avait donc une multitude de facteurs à prendre en compte avec des résultats différents dans chaque secteur et notamment dans l'industrie. Dès lors, il faut se demander si les politiques de laisser-faire des États, menées dans les années 1980 et au début des années 1990, qui ont été faites selon une perspective macro-économique, étaient vraiment adaptées à la réalité des impacts du déploiement des technologies de l'information.

Remettant cela en question, il doit être fait de même quant à la pertinence des dispositions visant à promouvoir la libre circulation des données entre les États, et notamment des données personnelles, garanties par de maigres mécanismes de protection. En effet, les technologies de l'information, dont on connaissait mal les imbrications au sein de l'économie, ne produisaient que peu d'effets tangibles. Pire même, elles étaient corrélées à un ralentissement de la productivité et de la croissance. Par conséquent, les politiques libérales en faveur de leur développement sans limite ne se justifiaient que sur la base de spéculations et non de certitudes. Plus inquiétante, l'ouverture des vannes en matière de flux transfrontières de données personnelles de l'époque semble trouver pour seule justification la promotion du traitement automatisé de données. Ce traitement automatisé est lui-même lié aux promesses économiques discutables, justifiant les

[190] J. DEDRICK, V. GURBAXANI et K. L. KRAEMER, préc., note 181, 4.
[191] *Id.*, 5.

politiques libérales de l'époque, à savoir le dopage de l'économie par le truchement du développement des technologies de l'information. Ces politiques de l'époque et les impacts qu'elles ont eus sur le droit des données et notamment en matière de flux transfrontières semblaient davantage guidées par l'idéologie.

En effet, le lien de causalité entre les dispositions entérinant la libre circulation des données personnelles et le développement de l'économie est difficile à établir à l'époque, étant donné que les technologies de l'information issues de la troisième révolution industrielle sont davantage un *support* aux acteurs économiques, qu'un évènement qui change radicalement la donne. On a peut-être surestimé l'importance de la circulation des données à un moment où les données ne constituaient pas un enjeu économique aussi important que ça l'est devenu dans les années 1990. Par conséquent, reléguer la protection des données au second plan en invoquant la nécessité de libéraliser les flux d'informations à l'époque pour des raisons de développement économique était purement idéologique et injustifié dans les faits. Pourtant, on aura constaté que c'est l'incompatibilité entre la libre circulation des données à des fins économiques et la doctrine européenne protectrice des années 1970, qui a précipité la perte de cette dernière, au profit de l'avènement de la *privacy* américaine plus souple et libérale. Est-ce le point de départ des dérives contemporaines en matière de données personnelles ?

Ce n'est que dans les années 1990 avec l'arrivée d'internet, que l'on peut admettre que le traitement des données est devenu une caractéristique à part entière de l'économie. Certes, cette économie bénéficiait *ipso facto* d'un contexte favorable à la libre circulation du fait des politiques et des dispositions internationales des années 1980. Cependant, ce sont avant tout des politiques infrastructurelles et des politiques de déresponsabilisation d'acteurs qui ont stimulé ce nouveau pan de l'économie et l'émergence d'un marché international des données.

Section 2 : L'influence relative de la libre circulation dans l'émergence d'une économie fondée sur le traitement des données

Au début des années 1990, ce sont tout d'abord des politiques de déploiement des infrastructures de télécommunications qui sont à la base de la circulation de l'information. Puis, les politiques de déresponsabilisation des acteurs intermédiaires, par lesquels transitent les données semblent également avoir eu un impact non négligeable, puisque leur ôtant la responsabilité de faire la police de l'information, rôle qui restreindrait par conséquent les flux d'informations. Le

droit des données, entérinant le principe de libre circulation, a davantage servi de couveuse en s'assurant de faire tomber les barrières à cette économie sans la stimuler en tant que telle.

Les politiques infrastructurelles

Aux États-Unis, l'administration Clinton a proposé très tôt un agenda pour le déploiement d'une infrastructure nationale de l'information qui était mise entre les mains d'opérateurs privés par le biais d'avantages accordés par le gouvernement.[192] La vision, qui s'est avérée assez juste en ce qu'elle voyait un vaste réseau de communications entre ordinateurs, bases de données et appareils électroniques personnels, était baptisée « information superhighway ».[193] Le pari a été gagnant puisque ces politiques ont entraîné énormément d'investissements en capital-risque dans les entreprises technologiques de la Silicon Valley dans les années 1990.[194] Le développement de l'internet et les entreprises technologiques capitalisant sur ce médium de communication auront sans doute contribué à une circulation mondiale plus dense des données. En effet, les politiques infrastructurelles aux États-Unis auront eu une double conséquence :

- Permettre l'accroissement des échanges d'informations par une infrastructure de réseau destinée à la circulation des données.

- Amorcer des financements par les acteurs privés dans des entreprises fondant leur activité sur internet et par définition sur les échanges d'informations.

Cet agenda américain sur la mise en place d'infrastructure réseau a permis de mettre en place un cadre économique en matière de télécommunications, régulé par le gouvernement, principalement dans le domaine de la concurrence, par le biais notamment de politiques fiscales ou bien de règles de propriété intellectuelle.[195] De ces politiques infrastructurelles alors, ont émergé les acteurs privés d'internet d'aujourd'hui, comme *Google*, dont l'activité économique principale découle du traitement des données. L'expansion d'internet sur la base de ces politiques

[192] Pamela SAMUELSON et Hal R. VARIAN, « The New Economy and information technology policy », dans Jeffrey A. FRANKEL et Peter R. ORZAG (dir.), *Economic Policy During the 1990 s*, Cambridge (MA), MIT Press, 2002, p. 1131, à la p. 1132.
[193] *Id.*
[194] *Id.*, à la p. 1134
[195] *Id.*

infrastructurelles des années 1990 a été saisissante. On passe en 1990 de 313.000 hébergeurs en 1990 à plus de 43 millions en 2000.[196] C'est autant de nœuds dans le réseau, qui permettent le stockage, le traitement, l'émission, la réception de l'information. À cet égard, l'accroissement des échanges de données dans les années 1990, du fait du développement d'internet, tire notamment sa source de politiques infrastructurelles aux États-Unis, ayant dopé la circulation de l'information.

En Europe, c'est une approche libérale, voire dérégulée des infrastructures de télécommunications, qui a été privilégiée par la Commission dans les années 1990. En effet, un groupe de travail sous la direction du Vice-président de la Commission et commissaire chargé du marché intérieur et de l'industrie, Martin Bangemann a rendu un rapport (ci-après rapport Bangemann) dans lequel il était en substance préconisé d'accélérer la libéralisation du secteur des télécommunications.[197] Ce rapport somme les États de s'abstenir de réguler le marché de l'information et ne jamais entraver la concurrence en affirmant que :

> « Le secteur de l'information se caractérise par son évolution rapide. C'est le marché qui jouera un rôle moteur, et c'est lui qui désignera les gagnants et les perdants. Compte tenu de la puissance des technologies en cause et de leur omniprésence, le marché ne peut être qu'universel. Le premier devoir des gouvernements est de préserver les forces concurrentielles et de créer un climat politique durablement favorable à la société de l'information de manière à ce qu'ici comme ailleurs, la demande puisse tirer la croissance. »[198]

Cette non-immixtion des États, dans la lignée des thèses néolibérales prônant la toute-puissance du marché, recommandée par ce rapport, va guider les futures politiques de libéralisation et de dérèglementation qui font, entre autres, que l'Europe a raté le coche et se trouve aujourd'hui dépourvue de tout acteur d'internet de poids.[199] En effet, ces politiques ont empêché le contrôle du marché par les États, dont on sait que c'est ce contrôle par le biais de politiques interventionnistes, qui ont permis l'émergence des grands acteurs technologiques que l'on connaît

---

[196] *Id.*, à la p. 1133
[197] LE MONDE, « Selon le rapport de Martin Bangemann, vice-président de la Commission européenne La déréglementation des télécommunications faciliterait l'accès aux "autoroutes de l'information" », *lemonde.fr*, 2 juin 1994, en ligne : <https://www.lemonde.fr/archives/article/1994/06/02/selon-le-rapport-de-martin-bangemann-vice-president-de-la-commission-europeenne-la-dereglementation-des-telecommunications-faciliterait-l-acces-aux-autoroutes-de-l-information_3833332_1819218.html>.
[198] Cédric DURAND, *Techno-féodalisme*, Paris, Zones, 2020, p. 80.
[199] *Id,* p. 78.

aujourd'hui, y compris aux États-Unis.[200] On comprend alors que dans cette logique néolibérale, les instruments juridiques n'ont pas un but purement régulatoire, mais servent à mettre en place des « cadres réglementaires adéquats »,[201] phagocytant l'intervention étatique au profit d'un marché largement dérégulé. Et dans ce contexte d'ivresse technologique des années 1990, le droit des données personnelles ne fait pas exception.

Le rapport Bangemann conduit la Commission à déposer un plan d'action sous la forme d'une communication au Parlement européen.[202] Ce dernier reprend les recommandations du rapport Bangemann avec des actions dans quatre domaines : le cadre règlementaire et légal ; les réseaux, les services de base, les applications et le contenu ; les aspects sociaux, sociétaux et culturels et ; la promotion de la société de l'information.[203] Ce plan d'action est résolument en faveur d'une libéralisation, puisqu'il s'agit, d'une part, de casser les monopoles existant en Europe et de confier les rênes d'un tel déploiement à des opérateurs privés.[204] Dès 1995 et jusqu'en 1998, une série de directives viennent mettre en place le plan de déploiement du réseau européen de télécommunications au travers de textes tels que la directive 97/51/CE[205] adaptant notamment la *directive relative à l'établissement du marché intérieur des services de télécommunication par la mise en œuvre de la fourniture d'un réseau ouvert de télécommunication* de 1990 et visant à ouvrir le marché des télécommunications à la concurrence. Les années 1990 marquent alors un tournant dans la libéralisation des infrastructures de télécommunications de part et d'autre de l'Atlantique.

Concomitamment, l'internet grand public, le *World Wide Web* entre officiellement en service en 1991 avec le fameux message publié par Tim Berners-Lee,[206] et la circulation de l'information sur ce médium sera justement rendue possible par le développement d'infrastructures gérées par des opérateurs indépendants, utilisant des standards interopérables (d'initiative privée

---

[200] *Id*., p. 80.
[201] *Id*., p. 81.
[202] Milda K. HEDLBOM et William B. GARRISON, *The Global Telecommunications Infrastructure: European Community (Union) Telecommunications Developments*, Charleston, S.C., Fourth BiEuropean Community Studies Association Fourth Biennial International Conference, 11 mai 1995, p. 3.
[203] COMMISSION DES COMMUNAUTES EUROPEENNE, *Vers la societé de l'information en Europe : un plan d'action*, Communication, C0M (94) 347, Bruxelles, Commission des communautés européenne, 1994, p. 2.
[204] M. K. HEDLBOM et W. B. GARRISON, préc., note 202, p. 4.
[205] *Directive du Parlement Européen et du Conseil du 6 octobre 1997 modifiant les directives 90/387/CEE et 92/44/CEE en vue de les adapter à un environnement concurrentiel dans le secteur des télécommunications*, 6 octobre 1997, J.O. 29 octobre 1997, p. 23-33.
[206] HISTOIRE CIGREF, « World Wide Web, toute une histoire ! », *cigref.fr*, 12 août 2013, en ligne : <https://www.cigref.fr/archives/histoire-cigref/blog/world-wide-web-toute-une-histoire/#:~:text=Le%206%20août%201991%2C%20Tim,«%20n%27importe%20où%20»%20 !>.

ou bien dictées par des règles de droit). Jusqu'ici, on peut alors affirmer que la stimulation de l'économie de service, qui va découler de l'avènement du Web a pu voir le jour de manière tangible, grâce aux politiques infrastructurelles menées par les différents acteurs étatiques, que ce soit aux États-Unis ou en Europe.[207] En effet, les infrastructures permettent à l'information de circuler plus librement et permettent pragmatiquement le développement de ce pan de l'économie.

Intéressons-nous maintenant aux politiques de déresponsabilisation des acteurs qui ont également eu un impact sur l'accroissement des échanges de données personnelles, du fait de l'absence de contraintes sur les acteurs du transport de l'information et sur le développement de la « nouvelle économie ».

Les politiques de déresponsabilisation des acteurs

La régulation des acteurs, façonnant cette nouvelle économie de services, fondée sur les données, s'est faite sous l'égide de la déresponsabilisation. Au premier rang de ces règles, on doit citer la section 230 du *Communication Decency Act,* qui a véritablement façonné l'internet moderne. Le texte dispose que :

> « No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. »[208]

Ce texte venait notamment prendre le contrepied de la jurisprudence américaine du milieu des années 1990. En effet, dans la décision *Stratton Oakmont* c. *Prodigy Services Co*., la Cour suprême de l'État de New York avait établi le statut d'éditeur de contenu au fournisseur de service internet dans le cas de contenu diffamant publié sur son site.[209] La section 230 du *Communication Decency Act* venait clairement remettre en question cette solution et clarifier le régime d'irresponsabilité de ces acteurs.[210]

Pour autant, c'est l'interprétation par les tribunaux qui a été faite de ce texte et qui a eu pour conséquence un régime d'irresponsabilité illimitée pour les acteurs d'internet. Notamment la décision *Zeran* c. *America Online Inc.* a élargi le régime d'irresponsabilité aux distributeurs de

[207] Nous n'entrerons pas ici dans la question de savoir si ces politiques infrastructurelles étaient bonnes ou mauvaises.
[208] *Communication Decency Act*, 47 U.S.C. (1996) § 230.
[209] *Stratton Oakmont* c. *Prodigy Services Co.*, 1995 N.Y. Misc. Lexis 229, § 13, [N.Y. Sup. Ct. 1995].
[210] Paul EHRLICH, « Communications Decency Act § 230 », (2002) 17-1 *Berkeley Technology Law Journal* 401, 405.

contenu considérant que la responsabilité du distributeur est une sous-catégorie de la responsabilité de l'éditeur.[211] Dès lors l'immunité pour les opérateurs d'internet américain était proclamée. Cela a permis un développement considérable de ces acteurs américains qui ne pouvaient pas se voir inquiétés à cause des contenus qui étaient partagés par leur intermédiaire. De cette déresponsabilisation découle une liberté dans la circulation des données qui a eu pour conséquence un accroissement dans les échanges de données et une croissance économique considérable du secteur. Sur ce terreau fertile, des grands acteurs de l'internet que l'on retrouve aujourd'hui et qui disposent d'un grand pouvoir ont pu voir le jour. En effet, rappelons-nous qu'entre 1990 et 2000, le nombre d'hébergeurs sur internet a été multiplié par quatorze et qu'à cette époque, les investissements privés dans les entreprises technologiques de la Silicon Valley explosaient du fait des politiques infrastructurelles menées aux États-Unis. Dès lors, un cadre réglementaire prônant la déresponsabilisation ne pouvait qu'entraîner davantage d'échanges de données au vu des politiques infrastructurelles de l'époque et de leurs effets.

Pour autant, même si le texte portait une idéologie libérale visant à laisser faire les entreprises afin qu'elles se développent, il n'est pas certain que l'effet attendu par le Congrès fût l'immunité absolue des plateformes.[212] Cette vision libérale s'attachait davantage à préserver une liberté d'expression immaculée sur les nouveaux canaux de communications que représentaient les services sur internet, avec notamment le maintien du fameux concept de « marketplace of ideas ».[213] Ce n'est que lorsque les juges ont interprété le texte, que l'immunité complète de ces opérateurs a été proclamée. Même si les conséquences économiques de la section 230 sont palpables et faisaient partie des objectifs annoncés par les représentants du Congrès, on peut considérer qu'elles sont en partie fortuites, puisque c'est une conjonction de faits, aidée par ce régime d'irresponsabilité états-unien, qui a permis la croissance des géants de l'internet que l'on connaît aujourd'hui et la libre circulation sans limite des données, que cela a induit.

En Europe, le régime d'irresponsabilité des acteurs d'internet et de l'économie de service découle largement de la directive dite commerce électronique de 2000. Les raisons en faveur d'un

[211] *Id.*, p. 407.
[212] *Communication Decency Act*, préc., note 208, § 230 (c).
[213] P. EHRLICH, préc., note 210, 419.

tel régime sont le développement du commerce électronique dans une société de l'information.[214] En effet, entre 1999 et 2003, les prédictions annonçaient une croissance du marché du commerce électronique multipliée par plus de dix, passant de 100 milliards de dollars à 1200 milliards de dollars.[215] Ainsi, dès 1998, la Commission européenne a soumis une proposition de directive au Parlement européen,[216] afin de surfer sur la vague du commerce électronique. Parmi les propositions de la Commission, figurait notamment un régime d'irresponsabilité large.[217] La directive adoptée en 2000 découle, par conséquent, de cette proposition à laquelle ont été soumis quelques amendements sur le régime de responsabilité des intermédiaires notamment.[218]

Trois catégories d'intermédiaires sont visées par la directive. La première catégorie représente les intermédiaires remplissant la fonction de « simple transport », qui sont principalement les fournisseurs d'accès.[219] Ces derniers jouissent d'une présomption d'irresponsabilité à condition qu'il ne soit pas à l'origine de la transmission d'informations, qu'ils ne sélectionnent pas le destinataire de la transmission et qu'ils ne modifient pas les informations faisant l'objet de la transmission.[220] La seconde catégorie concerne les opérateurs qui stockent de l'information en vue de la rediffuser ensuite à la demande d'autres destinataires (dit « caching »).[221] Ces intermédiaires bénéficient du même régime d'irresponsabilité selon les conditions mentionnées à l'article 13.[222] Enfin la dernière catégorie d'intermédiaire est celle des hébergeurs. Ces derniers doivent être exonérés de toute responsabilité dans le cas où ils n'ont pas connaissance de l'activité ou d'informations illicites.[223] Afin de compléter ce régime d'irresponsabilité des intermédiaires, l'article 15 § 1 de la directive dispose que :

> « Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils

---

[214] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*, 8 juin 2000, J.O. 17 juillet 2000, [*Directive sur le commerce électronique*], considérants 1 à 5.
[215] Luc GRYNBAUM, « La directive "Commerce électronique" ou l'inquiétant retour de l'individualisme juridique », *Communication Commerce électronique* 2001.7-8.chron. 18, 1.
[216] *Proposition de directive COM/98/0586 du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur*, 23 décembre 1998, J.O. 5 février 1999.
[217] *Id.*, art. 12.
[218] L. GRYNBAUM, préc., note 215, 1.
[219] *Directive sur le commerce électronique*, préc., note 214, art. 12.
[220] *Id.*
[221] L. GRYNBAUM, préc., note 215, 11.
[222] *Directive sur le commerce électronique*, préc., note 214, art. 13.
[223] L. GRYNBAUM, préc., note 215, 11.

transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. »[224]

C'est la tendance inverse qui a été observée en Europe en ce qui concerne les réponses jurisprudentielles, puisque ces dernières ont eu tendance à tempérer l'irresponsabilité des hébergeurs dans un certain nombre de cas, en l'assortissant d'une obligation de moyens pour ce qui est de la vigilance et de l'intermédiaire.[225] En effet, la Cour de justice de l'Union européenne a atténué ce régime de responsabilité en opérant une distinction entre le rôle actif et le rôle passif que jouerait l'intermédiaire. Dès lors, le degré d'activité et de passivité dépendrait de la catégorie de l'intermédiaire. Selon les affaires *Google France* et *L'Oréal*, les hébergeurs (article 14) sont réputés avoir un rôle plus actif, du fait du degré de contrôle sur le contenu hébergé et doivent retirer les contenus litigieux de manière plus stricte.[226] Ainsi, là où des raisons économiques gouvernaient explicitement l'esprit de la directive de 2000, la jurisprudence est venue tempérer ce régime d'irresponsabilité sans toutefois apporter un frein ni à l'économie du commerce électronique ni à la libre circulation des données. Il y a donc lieu de considérer qu'en Europe, la libre circulation des données découle directement et volontairement des politiques de déresponsabilisation des acteurs en ce que la volonté première de la Commission était de casser toutes les barrières au commerce électronique, par la déresponsabilisation des acteurs.

Il n'est pas surprenant d'assister à l'avènement de régimes permettant aux acteurs d'internet de ne pas être responsables des contenus qui sont partagés par leurs utilisateurs. Que ce soit dans le cas des États-Unis ou de l'Union européenne, l'irresponsabilité s'accorde avec la libre circulation de l'information, puisqu'on exempte les intermédiaires de faire la police de l'information. Dès lors, les politiques de déresponsabilisation contribuent à pérenniser la libre circulation de l'information. Dans un contexte marqué par l'avènement de la *privacy* américaine, comme étant une action civile visant à réparer un dommage, un tel régime d'irresponsabilité, qui viserait à empêcher qu'une action soit dirigée contre un de ces acteurs vient compléter une tendance juridique libérale. Logiquement, les politiques infrastructurelles facilitant le transport de l'information et le régime

[224] *Directive sur le commerce électronique*, préc., note 214, art. 15.
[225] L. GRYNBAUM, préc., note 215, 12.
[226] Tambiama MADIEGA, *Réforme du régime européen de responsabilité des intermédiaires en ligne : contexte de la future législation relative aux services numériques*, Analyse approfondie, PE. 649.404, Strasbourg, Service de recherche du Parlement européen, 2020, en ligne : <https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA (2020) 649404_FR.pdf>, p. 3.

d'irresponsabilité des acteurs d'internet entraînent naturellement un accroissement de la circulation des données. L'accroissement des échanges d'informations, du fait des politiques menées et les progrès en matière de traitement, de stockage et de transfert de l'information fondent dans ces années, une économie basée sur les données. En effet, l'économie des données existe au travers de l'accumulation de données, rendue possible par l'accroissement des échanges d'information, et dans les moyens de tirer de la valeur des données accumulées. Encore fallait-il alors posséder les infrastructures pour le faire et mécaniquement ouvrir les flux de données en déresponsabilisant les acteurs concernés. C'est désormais chose faite dans les années 1990.

Le droit des données a, quant à lui, joué le rôle de couveuse de cette nouvelle économie fondée sur la donnée.

La libre circulation en droit des données : une couveuse au service de la nouvelle économie

On aura alors constaté que le développement de la « nouvelle économie » fondée sur la circulation des données est autant une histoire de politiques infrastructurelles, que des régimes d'irresponsabilité des opérateurs en ligne permettant le transport de ces données. Nous devons maintenant nous interroger sur la place du principe de libre circulation consacrée en droit sur l'économie des données ?

Aux États-Unis, la question n'est pas aussi pertinente. Là où il n'y a pas de règle, il n'y a pas de problème ; cette maxime improvisée était particulièrement valable jusqu'à récemment. En effet, la circulation des données personnelles n'était soumise à aucun cadre règlementant le secteur privé, puisque la majorité des lois fédérales sectorielles concernaient bien le secteur public à l'exception du *Children's Online Privacy Protection Act* protégeant les données personnelles des enfants de moins de 13 ans. On ne peut alors valablement considérer qu'un principe de libre circulation des données au détriment de la protection ait pu favoriser l'émergence d'une économie fondée sur les données puisque la protection des données personnelles *ad hoc* était quasi inexistante. À titre informatif, la donne a tendance à changer de nos jours, avec l'émergence de règles étatiques, comme le *California Consumer Privacy Act,*[227] signé en 2018 par le gouverneur

[227] Il est tout de même à noter que la Californie s'est dotée d'un texte de règlementation en matière de vie privée dès 2003 avec le *California Online Privacy Protection Act* qui imposait à toute personne physique ou morale collectant des données de résidents californiens, via un site internet ou un service en ligne, pour des finalités commerciales,

de Californie Jerry Brown.[228] Pour autant, la libre circulation des données ne saurait être remise en question, même avec un texte comme celui que l'on a qualifié de « RGPD californien ». La libre circulation des données est toujours plébiscitée,[229] ce qui au demeurant n'est pas surprenant : qui aurait envie de saborder son fleuron de l'économie basée sur les données, en adoptant des mesures trop restrictives ? Rappelons-nous que les investissements privés ayant entraîné le développement des grandes compagnies américaines de la technologie ont eu lieu en Californie. L'heure est, par conséquent, au maintien d'un *statu quo* préservant la libre circulation des données plutôt qu'à un changement fondamental des politiques américaines, comme le montrent les projets de loi en droit des données personnelles à l'échelle fédérale.[230]

Mais peut-on vraiment blâmer les États-Unis lorsque c'est la même idéologie qui gouverne les règlementations canadiennes et européennes ? En effet, quand bien même le droit des données personnelles est plus fourni, les règles des vingt-cinq dernières années relèvent plus d'une protection au service de la libre circulation des données, que d'une véritable volonté de « consacrer » la protection des données personnelles. Cette direction politique est avant tout le reflet d'une volonté de croissance de l'économie de service basée sur l'exploitation des données, comme nous aurons l'occasion d'y revenir lorsque nous aborderons les régimes étatiques en droit des données adaptés au marché international des données.[231] Comprenons-nous bien, en comparaison aux politiques infrastructurelles et à la déresponsabilisation des acteurs intermédiaires d'internet, le droit des données personnelles n'a pas à proprement parler « stimulé » l'économie comme les politiques sur les infrastructures ont pu le faire. Il a plutôt indirectement accompagné ce développement économique et les conséquences que l'on connaît aujourd'hui en « laissant faire ». En somme, il a joué un rôle de *couveuse*. Encore aujourd'hui, on doit souligner ce rôle. Si juridiquement, des différences notoires existent entre la directive de 1995 et le *Règlement général*

---

d'identifier les différentes catégories de données collectées sur les utilisateurs, d'identifier les tiers avec qui les données sont susceptibles d'être partagées, et de publier une politique de confidentialité compréhensible et accessible sur le site internet ou dans le cadre du service en ligne : *California Online Privacy Protection Act*, CALIFORNIA BUSINESS & PROFESSIONS CODE §§ 22575, 22578, (2018). N.B : d'autres textes de règlementations plus spécifique ont suivi.

[228] Sylvain LONGHAIS, *Le Privacy Shield : cadre juridique efficace ou accord politico-économique ?*, Master of Laws Thesis, Aix-en-Provence, Aix-Marseille Université, 2019, en ligne : <http://www.iredic.fr/wp-content/uploads/2020/04/longhais-s.-macopymoire-privacy-shield-2018-2019.pdf>, p. 125. ; Stuart L. PARDAU, « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », (2018) 23-1 *J. Tech. L. & Pol'y* 68, 71.

[229] S. LONGHAIS, préc., note 228, 128.

[230] Karen SCHULER, « Federal data privacy regulation is on the way — That's a good thing », *iapp.org*, 22 janvier 2021, en ligne : <https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/>.

[231] *Intra,* p. 75.

sur la protection des données existent, l'idéologie reste inchangée. Et au vu des discussions et des propositions publiées ou adoptées, quant aux nouveaux projets de loi fédérale au Canada et provinciale au Québec[232], on se doit de faire le même constat. Ainsi, les idéaux de protection des données propres aux années 1970 sont loin. Le principe de libre circulation gouverne le droit positif depuis le début des années 1990, sous l'impulsion des outils du droit international public du début des années 1980. La libre circulation est au service d'une économie qui n'a cessé de se développer durant les deux dernières décennies ; la protection des données a été pensée pour ne pas en constituer un frein. Beaucoup s'en réjouiront puisque l'objectif est atteint. En somme, la partie idéologique s'est probablement jouée entre 1980 et 2000. Les problématiques qui se posent aujourd'hui ne sont pas nouvelles[233], mais sont sûrement beaucoup plus visibles du fait de l'avènement de technologies permettant le traitement et le transport de l'information et des données dans des volumes toujours plus grands et de manière toujours plus rapide,[234] et de l'avènement de ce qu'on appelle la *data driven economy* (cette même économie des données qui a vu le jour grâce aux politiques infrastructurelles et de déresponsabilisation).

Pour résumer, nous aurons vu qu'à ce stade, l'avènement conceptuel de la doctrine de *privacy* a ouvert la voie à la consécration du principe de libre circulation entre les États en droit international public. Cette réglementation a légitimé des politiques dont l'objectif était d'ouvrir les vannes des échanges de données (pour stimuler le progrès technologique notamment). Cela confirme la tendance depuis le début des années 1980 qui est de placer le droit des données au service d'une libre circulation économique sans frontières. Depuis la fin des années 1970, les politiques menées dans les grandes puissances économiques occidentales ont récité la partition du néolibéralisme économique en l'appliquant au contexte des technologies de l'information. Ces politiques visant à faciliter les échanges de données ont d'abord suivi l'évolution du marché des technologies de l'information. Cependant, on aura pu constater que les effets sur l'économie des politiques de libre circulation menées depuis le début des années 1980 sont à relativiser et sont

---

[232] *Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois*, projet de loi n° C-11, (1ère lecture à la chambre - 17 novembre 2020), 2e sess., 43e légis. (Can.). ; *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi n° 64 (sanction - 22 septembre 2021), 2e sess., 42e légis. (Qc).

[233] Par exemple, la responsabilité de plateformes comme Twitter (responsabilité des intermédiaires) ou les différents scandales en matière de données personnelles.

[234] Nous faisons ici référence aux technologies de big data et de Cloud Computing qui ont émergé durant la dernière décennie.

davantage guidés par l'idéologie, que l'on soit dans le cadre de traitement de données comme support de l'économie ou bien dans le cadre de l'émergence de l'économie de données au début des années 1990. Sur ce dernier point, la libre circulation consacrée en droit international n'a, alors pas nécessairement, joué un rôle de catalyseur lorsque le traitement des données est devenu une caractéristique de l'économie. D'autres événements conjoncturels plus pertinents semblent expliquer ce phénomène. Cette conclusion tirée, on doit alors questionner les choix qui ont été faits. Si les politiques de libre circulation n'ont pas eu tant d'impacts que ça en matière de croissance économique, avoir sacrifié la protection des données pour ces considérations et écarter une vision européenne plus protectrice est une erreur. À la fin de cette première partie, on doit pointer la responsabilité de tels choix et très certainement leur imputer pour partie l'origine des dérives contemporaines que nous aborderons dans la dernière partie de ce travail.

L'augmentation des échanges d'information et la croissance de l'économie des données ont sensiblement dopé les flux internationaux de données, du fait d'acteurs privés désireux de conquérir de nouveaux marchés. Les effets tangibles des politiques de libre circulation des données en droit international sont, par conséquent, plutôt à rechercher du côté de l'émergence d'un marché international des données.

Partie 2 : La mise en œuvre de cadres juridiques adaptés au marché international des données

Précédemment, nous avons pu démontrer comment l'avènement du concept de *privacy* américain, beaucoup plus permissif que la doctrine européenne des années 1970, aura permis de consacrer un véritable principe de libre circulation des données dans des outils juridiques internationaux de droit public. La libre circulation des données s'inscrivait dans un contexte de politiques économiques néo-libérales pour lesquelles, l'intervention de l'État est néfaste. Étant donné la valeur économique de l'information, il fallait casser la capacité des États à légiférer de manière trop contraignante pour les organisations privées. À cet égard, le concept américain répondait beaucoup mieux à ces considérations. L'avènement de la *privacy* américaine et le principe de libre circulation des données à l'international auront accompagné le développement de la nouvelle économie fondée sur les données en constituant un cadre juridique libéral. Bien que ce sont avant tout des politiques infrastructurelles et de déresponsabilisation des acteurs de l'internet qui ont entraîné des conséquences directes sur le développement de la nouvelle économie, le droit des données prônant la libre circulation internationale a rendu possible le développement d'un véritable marché international de la donnée basé sur le principe de libre circulation (Chapitre 1). Après avoir étudié son émergence et ses conséquences sur les régimes étatiques de droit des données notamment, nous aborderons comment au niveau international, droit des données et droit du commerce international ont commencé à converger, le dernier prenant peu à peu le pas sur le premier (Chapitre 2).

Chapitre 1 : L'émergence du marché international de la donnée et l'adaptation par le droit des États

Dans ce chapitre, nous étudierons dans quelles mesures, un marché international des données a émergé (section 1). Puis, nous observerons que les régimes étatiques régissant le droit des données personnelles se sont adaptés au principe de libre circulation dans le cadre de ce marché international (section 2) au détriment de la protection des données. L'étude de ces deux aspects est primordiale pour comprendre comment droit des données et droit du commerce international ont convergé, sujet que nous aborderons dans le chapitre suivant.

Section 1 : L'émergence du marché international de la donnée

Dans un premier temps, l'émergence d'un marché international de la donnée, rendue possible par la libre circulation des flux transfrontières des données s'est matérialisée par un changement dans la cartographie des flux transfrontières de données. C'est le premier point que nous allons développer. Nous observerons par la suite les caractéristiques de ce marché, induites par la libre circulation des données.

Le changement de cartographie des flux transfrontières de données

Le paysage des flux transfrontières de données a beaucoup changé ces trente dernières années. Ces flux ont énormément augmenté et les facteurs sont multiples. Bien entendu, cela provient des différents changements que nous avons pointés dans la première partie, comme le développement de politiques infrastructurelles, de déresponsabilisation des acteurs. On peut également pointer plus généralement la mondialisation, ayant entraîné une réduction du contrôle des capitaux qui circulent à travers le monde et la libéralisation des règles en matière de commerce international sous l'impulsion de l'OMC dans les années 1990.[235] En conséquence, l'importance grandissante des données dans l'économie et, notamment, la donnée personnelle devenue le

[235] Christopher KUNER, *Transborder data flows and data privacy laws*, Oxford, UK, Oxford University Press, 2013.

carburant de nos économies modernes, a dopé la croissance des services dans le secteur numérique avec l'apparition d'une industrie de l'analyse des données.[236]

En soi, l'analyse des données n'est pas une nouveauté et peut être définie comme un : « ensemble des méthodes permettant la description de tableaux d'observations statistiques sans faire intervenir aucune hypothèse sur l'origine de ces observations. Fondée sur des instruments mathématiques connus depuis longtemps, l'analyse des données est l'objet d'un développement assez récent (1965), favorisé par l'ordinateur. Elle regroupe des méthodes d'analyse factorielle (analyse en composantes principales et analyse des correspondances) et des méthodes de classification automatique. »[237] Cependant, les récentes techniques de triage des données, souvent associées au *Big Data*, ont permis de faire de l'analyse des données à elle seule, un marché hautement valorisé. Selon le cabinet de conseil Gartner, le marché de l'analyse de donnée pesait 18,3 milliards de dollars en 2017 et avait bondi de plus de 7 % depuis 2016.[238]

Bien évidemment, la démocratisation d'internet et l'offre de nouveaux services notamment par le biais de grandes plateformes explique également l'augmentation des flux transfrontières de données. Plus précisément, ces « nouveaux » transferts de données proviennent de la capacité décuplée pour chaque individu, à titre personnel, de transférer des données à travers le monde.[239] En effet, dans les années 1980 notamment, de tels transferts étaient coûteux, réservés à de grosses entreprises ou à des États et intervenaient la plupart du temps dans le cadre de réseaux fermés.[240]

Il existe un facteur davantage relié à l'évolution technologique et ayant entraîné une augmentation et une transformation des flux transfrontières de données. Il s'agit du passage d'un transfert de données d'un point A à un point B, à un transfert pour lequel les données transitent par de multiples points, ce qui rend leur nature ubiquitaire. Cette nature ubiquitaire entraîne naturellement une augmentation des flux transfrontières. En réalité, la donnée peut transiter par d'autres points du globe avant de se rendre là où elle a été sollicitée. En effet, le principe qui gouverne la régulation du trafic informationnel est celui selon lequel, le flux ne prend pas la

---

[236] *Id.*, p. 2.
[237] LAROUSSE, « Analyse de données », *www.larousse.fr*, en ligne : <https://www.larousse.fr/encyclopedie/divers/analyse_des_données/44425>.
[238] Susan MOORE, « Gartner Says Worldwide Business Intelligence and Analytics Market to Reach $18.3 Billion in 2017 », *gartner.com*, 17 février 2017, en ligne : <https://www.gartner.com/en/newsroom/press-releases/2017-02-17-gartner-says-worldwide-business-intelligence-and-analytics-market-to-reach-18-billion-in-2017>.
[239] C. KUNER, préc., note 235, p. 4.
[240] *Id.*, p. 6.

direction la plus courte en distance, mais la plus courte en temps[241], ce qui rend la trajectoire empruntée imprévisible et ce qui tend également à multiplier les flux. À ce titre, les technologies d'infonuagique ou *Cloud Computing* illustre bien le fait que très souvent, les données transitent par plusieurs localisations sans même que l'envoyeur ne le sache[242] bien que ce fût déjà le cas dans de moindres proportions, avant l'apparition de ces technologies.

On l'aura compris, les schémas de circulation ont considérablement changé et le volume des flux transfrontières de données, a beaucoup évolué. Dès lors, ces flux transfrontières ne répondent plus nécessairement à une logique géographique bien définie et c'est la territorialité de la donnée qui est remise en cause depuis une vingtaine d'années maintenant. De plus, nous sommes passés à un réseau ouvert qui permet de tels transferts en masse. Les pratiques ont alors évolué, mais certaines problématiques relatives à la circulation de l'information restent les mêmes. C'est notamment le cas de la gestion des infrastructures permettant à ces transferts de s'opérer. Il faut garder à l'esprit que ces transferts ne peuvent s'opérer que si l'infrastructure physique fonctionne également, et plus précisément les câbles sous-marins qui assuraient en 2016, 99 % du trafic mondial de données.[243]

De ce rapide panorama de l'évolution des flux transfrontières durant les dernières décennies, on constate que l'émergence du marché international des données est assurée socioéconomiquement, technologiquement et géopolitiquement. Cela a permis, depuis les années 1980-1990 jusqu'à aujourd'hui, de favoriser la mondialisation de l'économie numérique basée sur les données et, plus tardivement, de l'économie guidée par les données. Il convient maintenant de développer davantage sur ce marché international de la donnée assuré par le principe de libre circulation.

---

[241] Laurent VIENNOT, « Internet, le conglomérat des réseaux », *Interstices.info*, 17 novembre 2006, en ligne : <https://interstices.info/internet-le-conglomerat-des-reseaux/#:~:text=L%27internet%20est%20donc%20un,la%20destination%20%3A%20son%20adresse%20IP.>.
[242] C. KUNER, préc., note 235, p. 3.
[243] FRANCE INFO, « Internet : des câbles sous-marins pour faire transiter les données », *francetvinfo.fr*, 5 juillet 2016, en ligne : <https://www.francetvinfo.fr/internet/securite-sur-internet/internet-des-cables-sous-marins-pour-faire-transiter-les-donnees_1532971.html>.

L'émergence du marché international de la donnée

L'émergence et le développement d'un marché international de la donnée sont garantis par principe de libre circulation des données au même titre que l'économie globale est assurée par la libre circulation des marchandises et des capitaux. À cet égard, les règles en droit international public consacrant la libre circulation des données et liant les États occidentaux auront permis au marché international de la donnée de se constituer. Ce marché est protéiforme, puisque les données ont inondé tous les secteurs d'activité. De nos jours, on parle beaucoup de l'économie guidée par les données personnelles, dont nous avons dit quelques mots de sa naissance dans les années 1990, qui représente une part colossale du marché de la donnée et qui est souvent reliée à des activités du secteur tertiaire et à des activités numériques.[244] On pense notamment aux techniques automatisées de profilage qui sont utilisées dans de nombreux domaines de l'économie de service et qui requièrent des masses de données personnelles. On pense également à ces fins de profilage, aux activités d'analyse des données qui sont une pierre angulaire de l'économie guidée par les données personnelles. L'émergence des géants de l'internet a évidemment joué un rôle dans cette croissance du marché international de la donnée, du fait de leur présence planétaire et de leur très grand nombre d'usagers. Ainsi, ces deux facteurs cumulés vont *in fine* favoriser les transferts de données massifs entre frontières. Si l'on prend le cas des GAFAM, beaucoup de données personnelles sont rapatriées vers les États-Unis depuis l'Europe.[245] Mais, le secteur industriel n'est pas en reste lorsqu'il s'agit d'exploitation de données. On retrouve cette exploitation à tous les niveaux de la production, du *design* du produit jusqu'à la livraison.[246] Les transferts de données se retrouvent dans tous les secteurs d'activités : du secteur agricole jusqu'au secteur tertiaire, tandis que les transferts de données personnelles se cantonnent surtout au secteur tertiaire, secteur prééminent dans l'univers numérique qui caractérise nos sociétés modernes.

De manière plus terre-à-terre, la moindre réservation d'hôtel à l'étranger en ligne va entraîner le transfert des données du client vers l'hôtel qui va l'accueillir. Cet exemple illustre d'une part, le fait que le marché international de la donnée est alimenté directement par l'individu, ce qui constitue un changement par rapport aux années 1980. Mais, d'autre part, cela souligne le

[244] S. LONGHAIS, préc., note 228, Annexe n° 2 p. 157.
[245] *Id.*, p. 104.
[246] Francesca CASALINI et Javier López GONZÁLEZ, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers, 220, Paris, France, OECD Publishing, 2019, p. 31.

fait que l'environnement numérique a décuplé l'offre de services et que les transactions effectuées entre les parties nécessitent des transferts de données personnelles. Ce n'est dès lors pas surprenant que dans les années 1990, l'Organisation mondiale du commerce, au travers du texte de *l'Accord général sur le commerce de service*/*General Agreement on Trade in Services* (*GATS*), se soit emparée de ces questions à des fins de libéralisation du marché mondial et que l'on est progressivement assisté à une main mise en droit du commerce international sur ces questions. Nous y reviendrons. La même logique doit être appliquée en matière de commerce en ligne. Dans ce contexte, le transfert de données personnelles accompagne une transaction. Ainsi, pour être certain que la protection des données ne constitue pas une barrière au commerce, le transfert de données ne devrait pas être interdit.[247] Ce n'est pas un hasard si les dispositions relatives à la libre circulation des données personnelles que l'on retrouve dans les accords de commerce internationaux[248], se retrouvent dans les chapitres portant sur le commerce électronique.

Le marché international de la donnée et son corollaire que représentent les flux transfrontières de données ont connu un développement concomitant au phénomène de mondialisation économique fortement accéléré au début des années 1990 après la chute du mur de Berlin et la tombée des barrières au commerce induite par la création de l'OMC.[249] Les politiques infrastructurelles et de déresponsabilisation des acteurs, mais également le développement mondial de l'économie, le passage du secteur secondaire au secteur tertiaire, les gains d'intérêts pour l'économie de l'information et le développement des technologies de l'information, sont autant de facteurs intervenus à la même période et qui auront constitué un terreau fertile pour le développement du marché international des données. Quand bien même les technologies de l'information ont permis, à partir de la fin des années 2000, de traiter de vastes quantités d'informations, il serait réducteur de leur attribuer la seule paternité du « boom » du marché international des données. Ce sont avant tout les politiques ayant favorisé l'accroissement des échanges d'informations couplées au phénomène de la mondialisation économique, qui ont permis cette expansion. Les règles de libre circulation internationale des données sont venues légaliser de tels transferts et ainsi permettre la création de ce marché international. Les technologies modernes de traitement de l'information ont davantage joué un rôle d'accélérateur, puisqu'elle qu'elles

[247] *Accord général sur le commerce des services de 1994*, Annexe 1B de l'accord instituant l'OMC, section XIV.
[248] *Infra*, p. 91.
[249] Jean-Yves HUWART et Loïc VERDIER, *Economic Globalisation — Origins and Consequences*, coll. OECD Insights, Paris, France, OECD Publishing, 2013, p. 50.

pouvaient être exploitées à leur plein potentiel dans un environnement largement dérégulé. Et même, si dans les années 1990, le terme de mondialisation référait surtout au libre mouvement des biens et des capitaux,[250] la même tendance s'est vérifiée en ce qui concerne les données.

Par ailleurs, on a progressivement assisté à un détachement des données liées aux transactions « conventionnelles », c'est-à-dire de biens et de capitaux. Dans une transaction conventionnelle, les données transférées sont l'accessoire rattaché à une transaction principale. Par exemple, un opérateur commercial français qui envoie un véhicule appartenant à M. X à un opérateur commercial canadien effectue une transaction principale, qui est l'envoi du véhicule. À des fins d'identification du propriétaire, M. X, il transmet également les données personnelles de ce dernier (accessoire). Ces transactions sont caractérisées en premier lieu par des transferts *B to B* et *B to C*[251] pour des raisons commerciales. Cependant, on a progressivement basculé vers des transactions matérialisées par le transfert de la donnée elle-même, ce qui signifie que le transfert de la donnée constitue la transaction principale et non plus l'accessoire à une transaction principale. Mais, il s'agit davantage d'une scission dans la nature des transferts de données plutôt que d'un remplacement ou d'un basculement d'une réalité à une autre. En effet, encore aujourd'hui, les données peuvent être transférées autant pour leur valeur intrinsèque, que comme accessoire à une transaction principale.

Enfin, un autre facteur de la croissance de ce marché résultant notamment des politiques menées dans les années 1990, est le phénomène de plateformisation. Il est à noter d'entrée que la plateformisation de nos sociétés revêt des caractéristiques différentes et qu'il n'y a pas une plateformisation unique.[252] Selon le Conseil national du numérique en France, une plateforme est :

> « Un intermédiaire dans l'accès aux informations, contenus, services ou biens édités ou fournis par des tiers. Au-delà de sa seule interface technique, elle organise et hiérarchise les contenus en vue de leur présentation et leur mise en relation aux utilisateurs finaux »[253].

Cette définition est intéressante, puisqu'elle renvoie principalement à la notion d'intermédiaire qui caractérise la plateformisation de nos sociétés, mais insiste sur le rôle actif de

[250] *Id.*, p. 51.
[251] *Business to Business* et *Business to Consumer*
[252] Jean-Samuel BEUSCART et Patrice FLICHY, « Plateformes numériques », (2018) 2018/6-212 *Réseaux* 9, §10.
[253] *Id.*

ces intermédiaires, rôle actif qui cristallise les débats en doctrine juridique et dans les prétoires, notamment en ce qui concerne la reconnaissance de la responsabilité de ces intermédiaires. Pour les fins qui nous intéressent, à savoir le rôle de la plateformisation sur le marché international des données, notons simplement que les intermédiaires jouent un rôle primordial dans la croissance de ce marché. Schématiquement, au-delà des services variés sur lesquels ils sont positionnés, ils sont autant un conduit pour la circulation de l'information d'un utilisateur à un autre, qu'une régie publicitaire collectant et traitant les informations des utilisateurs pour vendre à des annonceurs des espaces de publicité dédiés sur les plateformes contre rémunérations.[254] On comprend alors que la plateformisation par le biais de grands intermédiaires (les GAFA pour ne citer qu'eux), dope le marché de la donnée en favorisant leur circulation à une échelle planétaire et en exploitant un modèle économique lucratif de courtier en données. À ce titre, on peut relever que les politiques de déresponsabilisation de ces acteurs, que nous avons décrites ont eu des effets tangibles.

Ce développement du marché international de la donnée et l'augmentation exponentielle des flux transfrontières de données ont entraîné des tentatives de règlementation de ces flux par les États tout en respectant le principe de libre circulation des données consacré en droit international public. Ces derniers ont mis en place des régimes permettant à l'information de circuler hors de leurs territoires, les uns comme le Canada, poursuivant une logique de *privacy* américaine de laisser-faire jusqu'à la survenance d'un dommage, les autres comme les pays membres de l'Union européenne, favorisant des règles extraterritoriales qui imposent des contraintes sur les transferts internationaux de donnée, sans remettre en cause la libre circulation internationale des données personnelles. L'idée sous-jacente est cependant toujours la même. Il s'agit de protéger le marché international des données en sanctifiant le principe de libre circulation des données. En effet, cette libre circulation internationale des données est protégée par des outils juridiques de droit international public qui s'appliquent aux États. On peut d'ores et déjà citer les *Lignes directrices de l'OCDE* et la *Convention 108* mais il en existe bien d'autres, particulièrement sous l'égide du droit du commerce international qui est l'objet du chapitre 2 de cette partie.

[254] *Infra*, p. 135.

Section 2 : Les régimes juridiques étatiques adaptés au marché international de la donnée

Afin de respecter le principe de libre circulation internationale des données personnelles tout en gardant une composante de protection des données, des initiatives étatiques adaptées au marché international se sont développées selon des modèles différents. Deux modèles de règlementation des flux transfrontières peuvent être dégagés. Un modèle que l'on peut qualifier de « modèle centralisé » et un modèle basé sur des règles à portée extraterritoriale.

Le modèle centralisé canadien

Ce modèle est le même que celui de la première loi fédérale allemande de 1977, quant à la manière de règlementer les flux transfrontières.[255] La principale qualité de ce modèle de règlementation, c'est son pragmatisme. Dans les grandes lignes, il s'agit de faire appliquer les mêmes règles aux flux internes de données qu'aux flux externes de données. En d'autres termes, les règles applicables sur le territoire de l'État sont celles qui vont s'appliquer pour des données personnelles qui quittent le territoire de cet État pour se rendre dans un autre État. Cependant, ce modèle a été remplacé en Allemagne du fait de l'entrée en vigueur de la règlementation de l'Union européenne. En revanche, ce modèle subsiste de manière contemporaine dans certains États ; c'est le cas du Canada, qui servira ici d'exemple au développement du modèle centralisé que nous allons maintenant détailler. Ce modèle centralisé canadien est influencé par les *Lignes directrices de l'OCDE* et par le principe de libre circulation. Il est d'ailleurs aisé de faire le rapprochement entre les *Lignes directrices de l'OCDE* et la *Loi sur la protection des renseignements personnels et les documents électroniques*.[256] Notamment, un des principes des *Lignes directrices* va guider cette loi et par conséquent le modèle canadien. C'est la responsabilité des maîtres des fichiers[257]. En effet, elles énoncent que :

---

[255] *Supra*, p. 26.
[256] Éloïse GRATTON, « Dealing with Canadian and Quebec Legal requirements in the Context of trans-border Transfers of Personnal Information and Cloud Computing services », dans Jean CHARTIER et BARREAU DU QUEBEC (dir.), *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels, les 30 ans de la Commission d'accès à l'information*, 358, Cowansville, Québec, Yvon Blais, 2012, p. 7, à la p. 11.
[257] *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, préc., note 142.

« Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus. »[258]

Dès lors, on comprend que le « maître des fichiers » est responsable des données, dont il a la garde et qu'il doit, peu importent les circonstances, respecter les principes des *Lignes directrices* comme la limitation de la collecte, la limitation dans l'utilisation (un assimilé du principe d'exactitude) ou encore un certain nombre de droits qui devraient être conférés aux individus concernés.[259] On a alors un principe de responsabilité très fort des acteurs traitant les données, principe que l'on va retrouver dans la législation canadienne.[260] En effet, on place le transfert de données à un tiers à l'étranger au même niveau que celui qui aurait lieu au Canada. Ainsi, l'organisation doit s'assurer que le tiers destinataire du transfert remplit les mêmes obligations auxquelles elle est soumise dans le cadre de la loi canadienne. Ce principe de responsabilité est d'ailleurs expressément consacré dans l'annexe I de la loi qui énonce les dix principes énoncés en matière de protection des données personnelles. L'article 4.1.3 dispose que :

« Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés […] ».

Et d'ajouter :

« Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie »[261].

C'est d'ailleurs ce qu'a rappelé le Commissariat à la protection de la vie privée du Canada dans les *Lignes directrices sur le traitement transfrontalier des données personnelles* qu'il a publié en 2009 :

---

[258] *Id.*
[259] *Id.*
[260] Voir à ce titre le principe de responsabilité que l'on retrouve dans la LPRPDE, *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5. annexe 1, art. 4.1 et 4.1.3, s'appliquant également en matière de flux transfrontières.
[261] *Id.*, art. 4.1.3.

> « Peu importe l'endroit où l'information est traitée, que ce soit au Canada ou dans un pays étranger, l'organisation doit prendre toutes les mesures raisonnables pour protéger celle-ci contre l'utilisation ou la communication non autorisée par la tierce partie. L'organisation doit avoir l'assurance que la tierce partie a mis en place des politiques et des processus, y compris de la formation à l'intention de son personnel et des mesures de sécurité efficaces, pour s'assurer que l'information qu'elle a sous sa garde est adéquatement protégée en tout temps. »[262]

Cependant, le transfert qui ne respecterait pas les principes de la loi n'engage pas la responsabilité de l'organisation, si cette dernière fait l'objet d'une demande d'une instance gouvernementale étrangère pour ledit transfert, comme l'avait souligné le CPVPC dans une enquête conformément à l'alinéa 7 (3) c) de la Loi.[263]

Cette approche est efficace, mais critiquable puisqu'elle ne permet pas d'assurer une protection suffisante s'agissant de flux transfrontières de données. Tout d'abord, on se situe à un niveau *ex post*, ce qui signifie que l'on privilégie le recours en cas de problème pour la personne concernée, plutôt qu'une protection *a priori*. En effet, le principe général s'appliquant indifféremment au traitement et aux transferts au Canada et en dehors, la personne concernée doit former un recours devant le CPVPC, puis devant la Cour fédérale le cas échéant, afin d'obtenir gain de cause.[264] Cela implique que le dommage ait déjà eu lieu, afin qu'il soit sujet à réparation. À ce titre, on est dans une logique de *privacy* à l'américaine, puisque le recours est conditionné à la survenance d'un dommage. Ainsi, se placer sur le terrain de la responsabilité revient à consacrer un droit à la vie privée comme recours et non comme une fin en soi. Dans tous les cas, l'organisation doit prendre ses dispositions afin d'être en conformité ou ne pas se faire prendre. Ainsi, on comprend que cette approche de responsabilisation est basée sur la confiance que l'on accorde aux organisations qui traitent nos données. De manière évidente, ce mécanisme est conforme avec la libre circulation des données, puisqu'il induit l'autorisation de transférer des données à l'étranger, tant que des dispositions contractuelles ou le recours à d'autres mécanismes

---

[262] COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA, *Traitement transfrontalier des données personnelles*, Lignes directrices, Ottawa (ON), Commissariat à la protection de la vie privée du Canada, 2009, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/>.
[263] *Commissaire à la protection de la vie privée du Canada* c. *SWIFT*, 2007 CPVC, par. 47.
[264] É. GRATTON, préc., note 256, à la p. 11.

ont été pris. Mais en termes de protection des données de l'individu, il est plus discutable. En effet, la responsabilisation des acteurs peut être assurée dans un pays ou une communauté partageant les mêmes valeurs, puisqu'il existe une protection qui émane de l'État ou plus simplement d'une norme législative. Cependant, dans le cadre des flux transfrontières de données, on a une protection qui varie, selon l'État de provenance et l'État de destination et force est de constater que ce modèle ignore le niveau de protection offert ou non, par les États dans lesquels les données sont transférées. En l'absence d'une telle prise en compte, le danger d'un modèle centralisé semble émaner de l'impossibilité d'assurer une protection *ex ante,* si les régimes de protection des données ne sont pas alignés. À moins d'avoir des régimes équivalents dans les États de provenance et de destination, on voit difficilement comment un modèle univoque de réglementation des flux de données interne et externe peut assurer une protection efficace *a priori*. Par conséquent, un tel modèle est seulement viable pour traiter les problèmes quand ils surviennent et non pour les prévenir. On comprend alors pourquoi placer la responsabilité sur les organisations, au moyen de recours pour les individus en cas de dommages, est finalement la seule issue possible d'un modèle centralisé.

Ainsi, dans un modèle centralisé, le degré de protection des données personnelles se trouve sacrifié au profit de l'efficacité du transfert ; ce modèle est parfaitement adapté à la compétitivité des acteurs sur le marché international fondé sur la donnée, en assurant largement la circulation des données personnelles.

Le modèle de règles extraterritoriales à l'européenne

Le deuxième modèle contemporain dans la règlementation des flux transfrontières des données est celui qui consiste à prendre des mesures qui ont des effets extraterritoriaux afin de s'assurer que la protection des données est *a minima* assurée dans l'État dans lequel le transfert a lieu. Ici, on a une conception plus protectrice, mais qui n'a pas non plus vocation à remettre en cause le principe de libre circulation des données personnelles entre les États. Ici, il sera principalement fait état du modèle de l'Union européenne au travers de la directive de 1995 et du *Règlement général sur la protection des données personnelles* (ci-après *RGPD*). L'étude de cette règlementation est intéressante en ce qu'elle soulève une réelle interrogation quant au véritable objectif des règles de protection des données personnelles en Europe. Il est d'ores et déjà utile de mentionner que si, dans la lettre du texte, la libre circulation des données est consacrée seulement

dans les flux intracommunautaires de données personnelles,[265] les règles établies dans le chapitre concernant les flux transfrontières que nous allons détailler,[266] ainsi que les pratiques entre l'Union européenne et certains pays tiers, démontrent que la libre circulation des données est au moins aussi importante que la protection des données en soi comme nous l'expliquons plus loin dans le présent paragraphe.

Mais une fois n'est pas coutume, un peu de contexte est nécessaire même si nous nous épargnerons l'histoire des textes européens sur le droit des données. Il convient simplement de garder à l'esprit que la libre circulation des données personnelles a été l'approche privilégiée par les instances européennes à la création de la directive de 1995 et, encore plus, en 2016, avec l'adoption du *RGPD*. Cette approche est de longue date, puisqu'en 1979 déjà, le Parlement européen déclarait son intention de favoriser un équilibre entre la protection des données et la libre circulation des données,[267] ce qui rejoignait alors la tendance voulue par les instances internationales dont on a déjà pu faire état.[268] Ainsi, cette position correspondait à une tendance de l'époque de favoriser la libre circulation pour des considérations économiques, en se basant sur une conception américaine de la *privacy* plus permissive. D'ailleurs, ces considérations économiques, outre le fait qu'elles soient clairement énoncées dans les considérants de la directive de 1995, se retrouvent également dans plusieurs documents des instances de l'UE. En particulier, le livre blanc de la Commission européenne portant sur la stimulation de la croissance, de la compétitivité et de l'emploi plaçait la règlementation sur la protection des données comme répondant à une priorité d'établir un cadre règlementaire promouvant l'économie de l'UE dans le contexte de développements des systèmes d'information.[269] Ces développements libéraux fondés sur l'économie d'un marché unique sont, toutes proportions gardées, ceux que l'on retrouve aujourd'hui dans la stratégie du marché unique numérique, dont le *RGPD* est une pierre angulaire.

---

[265] « La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. », *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*, 27 avril 2016, J.O. 4 mai 2016 [*R.G.P.D*], art 1 § 3.

[266] Il sera beaucoup fait référence au chapitre V du RGPD portant spécialement sur les flux sortants de données personnelles.

[267] K. BENYEKHLEF, préc., note 17, p. 279.

[268] *Supra*, p. 37.

[269] COMMISSION EUROPEENNE, préc., note 176, p. 25.

Dès les années 1970, à l'époque de l'émergence des systèmes d'information et de l'informatisation de la société, la Communauté européenne faisait face à des problématiques de domination du marché européen par des acteurs américains. On pense notamment à IBM qui contrôlait plus de 50 % du marché mondial des ordinateurs.[270] La Commission européenne regrettait alors que les États, comme l'Allemagne et la France, accordent en ordre dispersé des aides aux entreprises pénétrant le marché de l'information. À titre d'autorité de la concurrence, la Commission autorisait ces États à maintenir ces aides, mais alertait sur le manque de coordination européenne. Aux yeux de la Commission, cette coordination constituait un moyen efficace pour empêcher cette domination américaine.[271] Des approches communautaires se sont alors développées afin de stimuler le développement de l'économie européenne des traitements automatisés de données. Sans surprise, la régulation des données par le droit européen est apparue comme la solution pour harmoniser le droit des données en Europe,[272] toujours dans un but de croissance du marché. De manière générale, la protection des données personnelles en Europe a toujours été guidée par un contexte de promotion des traitements automatisés de données, et nombreux sont les travaux des différentes instances européennes depuis le début des années 1970, qui en attestent.[273] La promotion de ce nouveau pan de l'économie passait alors nécessairement par la libre circulation des données personnelles qui est érigée en principe dans les textes. Le projet européen étant avant tout un projet basé sur une coopération économique, il n'est pas étonnant de constater que la question de la protection des données personnelles au service du développement de l'économie n'échappe pas à la règle.

Dès lors, il s'agissait de fortifier le marché européen des technologies de l'information, de faciliter le développement d'acteurs européens dans les systèmes d'information et, plus récemment, dans le numérique, de stimuler la croissance, la compétitivité et l'emploi. Tous ces éléments expliquent la politique de droit des données personnelles menée par l'Union européenne sur les

---

[270] COMMISSION EUROPÉENNE, *The European Community and Data Processing -- Government Development Aids Permitted*, Information, 21/72, coll. Competition, Bruxelles, Commission européenne, 1972, p. 1.
[271] *Id.*, p. 2.
[272] COMMISSION EUROPÉENNE, *Communication by the Commission of the European Communities concerning a Community policy for data processing*, Communication, P-63/73, coll. Information Memo, Bruxelles, Commission européenne, 1973, p. 13.
[273] Voir, Gloria González FUSTER, « The Beginning of EU Data Protection », dans Gloria González FUSTER (dir.), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, coll. Law, Governance and Technology Series, n°16, Cham, Springer, p. 111. Les initiatives européennes alliant protection et libre circulation des données y sont très bien détaillées, si bien qu'un simple renvoi est plus efficace qu'une explication fastidieuse dans le corps de texte, qui n'est pas la priorité dans le cadre du présent mémoire.

flux intracommunautaires de données, mais également les flux sortants depuis les 25 dernières années.

En ce qui concerne le modèle de règles extraterritoriales pour réguler les flux sortants de données, on peut assez facilement admettre l'existence d'entraves implicites à la libre circulation plutôt qu'une protection des données assumée. Et au vu du contexte et des politiques menées, ce n'est guère surprenant. Les outils prévus par la directive pour transférer des données personnelles hors du territoire de la communauté sont tout d'abord assez larges. Plusieurs mécanismes sont prévus pour assurer des standards de protection des données.[274] Mais ces mécanismes complexes et alambiqués concernent également les possibles dérogations ayant pour but de transférer les données vers un pays tiers et d'assurer *in fine* une libre circulation. On peut dégager du chapitre de la directive consacré à ce régime, trois situations dans lesquelles il est possible de transférer des données personnelles hors de l'Union européenne.[275] Premièrement, le pays tiers doit faire l'objet d'une décision d'adéquation de la Commission européenne, qui lui reconnaît alors un niveau de protection adéquat autorisant les transferts.[276] Deuxièmement, le transfert peut avoir lieu même si le pays tiers n'assure pas un niveau de protection adéquat dans le cas où il remplit au moins un critère dérogatoire fixé à l'article 26 § 1.[277] Troisièmement, le transfert peut avoir lieu si le responsable de traitement se trouvant dans un pays n'assurant pas un niveau de protection adéquat offre des garanties suffisantes de protection des données personnelles.[278] Cette dernière catégorie

[274] *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*, 24 octobre 1995, J.O. 23 novembre 1995 [*Directive 95/46/EC*], art. 25 et suiv.
[275] Lingjie KONG, « Data Protection and Transborder Data Flow in the European and Global Context », (2010) 21-2 *The European Journal of International Law* 441, 443.
[276] *Directive 95/46/EC*, préc., note 274, art. 25 § 6.
[277] Les critères dérogatoires du texte sont les suivants : « 1. Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué, à condition que : a) la personne concernée ait indubitablement donné son consentement au transfert envisagé ; ou b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ou ; c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ou ; d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ou ; e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou ; f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier. *Id*., art. 26.
[278] *Id.* art. 26 § 2.

est à l'origine des clauses types permettant de régler la question des flux transfrontières de manière contractuelle. Cela traduit une volonté de faire peser sur les acteurs privés la responsabilité quant à la légalité des transferts qu'ils opèrent.

Le problème est que très peu de décisions d'adéquation ont été rendues par la Commission. Or, ces décisions constituent, parmi les possibilités offertes pour autoriser les flux sortants, le seul moyen fiable de s'assurer de l'existence d'un droit protégeant les données des citoyens européens. Par conséquent, le régime dérogatoire prévu par la directive, favorise significativement la libre circulation des données au détriment du niveau de protection, du fait de la rareté des décisions d'adéquation. En effet, le contrôle sur l'effectivité des mesures mises en place se fait majoritairement *a posteriori*, dans le cas où il n'y a pas de décision d'adéquation reconnaissant un régime de protection des données conformes aux standards européens. Cela peut poser des problèmes en matière de responsabilité et *in fine* de recours pour les personnes concernées. Encore une fois, il est utile de rappeler que l'on est dans une logique de droit à la protection comme réparation et non comme une fin en soi. De plus, les autorités n'ont que peu de moyens de contrôle concernant les flux sortants, et notamment lorsqu'elles n'ont pas d'homologue dans le pays où les données sont transférées. Ainsi, si l'on peut comprendre la création d'une libre circulation des données intracommunautaire basée sur une protection harmonisée à l'intérieur du territoire de l'Union, il est plus difficile de justifier de si nombreuses dérogations aux règles de protection pour les flux sortants, si ce n'est pour consacrer un régime de libre circulation distinct de celui concernant les flux intracommunautaires. Pour réglementer les flux sortants, on se base par conséquent sur les standards de la directive pour transférer des données vers des pays tiers auxquels on assortit des dérogations suffisantes pour assurer la libre circulation.

Mais, le même modèle est également transposable au *RGPD*, bien que le contexte diffère un peu. Avec la croissance exponentielle de l'économie numérique et le retard de l'UE en la matière, la question de la libre circulation des données à caractère personnel est devenue cruciale, compte tenu notamment du manque de grands acteurs numériques capables de concurrencer les géants américains de la technologie.[279] Le *RGPD*, de la même façon que la directive, reflète les enjeux de la politique économique de l'Union européenne en matière de développement numérique. C'est probablement une des raisons pour laquelle un règlement qui est d'application

[279] S. LONGHAIS, préc., note 228, p. 92.

directe pour les États membres a été préféré à la directive, pour laquelle les États n'avaient pas tous des règles uniformes, créant alors des barrières économiques dans l'espace communautaire et nuisant de ce fait à la volonté de renforcer la libre circulation des données.

Ce sont d'ailleurs autant les impacts économiques du texte que l'étude de la protection des données en soi qui ont fait l'objet de débats en doctrine. Sur le plan économique, la question était notamment de savoir si les standards de protection allaient engendrer une compétitivité plus forte ou, au contraire, se présenter comme une entrave au développement économique du marché de la donnée.[280] Les avis sont partagés : certains considèrent que le niveau de protection est trop élevé pour ne pas entraver la libre circulation et les intérêts économiques qui en découlent[281], d'autres voient dans la protection des données personnelles, l'opportunité de créer de nouveaux marchés autour de la donnée.[282] La cristallisation des débats autour de l'impact sur le plan économique que peut avoir la protection des données prévue par le *RGPD* est un indicateur fort de l'importance de la libre circulation des données. En ce qui concerne la libre circulation sur les flux sortants, les plus véhéments sont même allés jusqu'à dire que le texte européen constituait une barrière non tarifaire qui viole les dispositions du *General Agreement on Trade in Services* (*GATS*).[283] Cette perspective, qui reprend dans les grandes lignes, les premières critiques de protectionnisme économique par la protection des données émanant d'auteurs américains, peut s'entendre. La protection des données peut théoriquement être utilisée à des fins protectionnistes. Mais en l'espèce, cette critique nous semble juridiquement infondée. En effet, si la Commission européenne ne cache pas les ambitions économiques derrière le texte et l'importance capitale de la libre circulation des données au service du développement du marché unique numérique,[284] il est difficile d'analyser le texte comme une barrière non tarifaire : il y a trop de dérogations possibles pour que le texte soit considéré comme tel. C'est ce que nous allons maintenant étudier.

---

[280] Jean-Luc SAURON, « Le RGPD : outil ou entrave de la société d'information ? », (2018) 2018 *Dalloz IP/IT* 17.
[281] *Id.*, 19.
[282] Darcy W. E. ALLEN, Alastair BERG, Chris BERG, Brendan MARKEY-TOWLER et Jason POTTS, « Some Economic Consequences of the GDPR », (2019) 39-2 *Economics Bulletin* 785, 786.
[283] Elisabeth MEDDIN, « The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services », (2020) 35-4 *Am U Int'l L Rev* 997, 1036.
[284] Léo LICTEVOUT et Vincent LEQUEUX, « La politique numérique de l'Union européenne », *touteleurope.eu*, 16 décembre 2020, en ligne : <https://www.touteleurope.eu/economie-et-social/la-politique-numerique-de-l-union-europeenne/>.

En effet, pour ce qui est des standards de protection garantissant la liberté de circulation des flux sortants, le *RGPD* conserve le mécanisme de décision d'adéquation, mais pour le reste, il laisse le soin aux entreprises d'adopter des garanties appropriées qui sont souvent longues, complexes et coûteuses à mettre en œuvre (que ce soit les clauses contractuelles ou les règles d'entreprises contraignantes[285] par exemple).[286] Encore plus que dans la directive, on retrouve des dérogations aux termes ambigus qui permettent de transférer des données vers un pays tiers alors que le pays n'offre pas un niveau de protection adéquat ou que le responsable de traitement n'apporte pas de garanties appropriées.[287] En effet, l'article 49 du *RGPD* fournit une liste de dérogations particulières pour lesquelles les transferts peuvent avoir lieu : « en l'absence de décision d'adéquation […], ou de garanties appropriées […], y compris des règles d'entreprise contraignantes […] ».[288] Ainsi, les transferts peuvent s'opérer dans les cas où :

> « a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ; b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ; c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ; d) le transfert est nécessaire pour des motifs importants d'intérêt public ; e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ; f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ; g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre,

---

[285] Selon la CNIL : « Les règles d'entreprise contraignantes (communément appelées *BCR*) permettent à des groupes d'entreprises d'encadrer juridiquement leurs transferts de données hors de l'Union européenne (UE) tout en leur offrant la possibilité d'engager une démarche de mise en conformité globale à l'échelle de tout le groupe. Les BCR constituent un outil d'encadrement global des transferts hors UE. C'est une alternative à d'autres outils permettant d'encadrer des transferts tels que les Clauses Contractuelles Types. », voir, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Ce qu'il faut savoir sur les règles d'entreprise contraignantes (BCR) », *www.cnil.fr*, 7 février 2020, en ligne : <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr>.
[286] S. LONGHAIS, préc., note 228, p. 86.
[287] *R.G.P.D*, préc., note 265, art. 44 et suiv.
[288] *Id.*, art. 49

est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce. »[289]

On en conviendra, le texte est proche de l'article 26 § 1 de la directive de 1995, bien qu'il recèle quelques subtilités de langage de nature à influer sur l'interprétation que l'on peut en faire, mais sur lesquelles nous ne nous attarderons pas, préférant nous concentrer sur l'essentiel. Les dérogations de l'article 49 portent sur un transfert ou un ensemble de transferts[290] permettent de transférer des flux de données assez conséquents dans une kyrielle de cas possibles, allant du consentement jusqu'à la justification de nature contractuelle en passant par l'intérêt légitime de l'organisation effectuant le transfert.[291] Cette dérogation d'intérêt légitime est une nouveauté apportée par le *RGPD* par rapport à l'article 26 § 1 de la directive et autorise une interprétation large, étant donné le flou entourant la notion. En plus de ces dérogations, le *RGPD* dispose qu'un transfert peut avoir lieu même s'il ne remplit pas les conditions vues précédemment, dans le cas où : « ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. »[292]

Dans ses lignes directrices sur l'article 49, le G29 (nouvellement CEPD)[293] est tout de même venu apporter quelques limites à ces dérogations[294]. Les deux limites générales sur lesquelles insiste le CEPD sont le caractère occasionnel, non répété des transferts et la nécessité d'opérer le transfert. Sur le caractère occasionnel, le CEPD reconnaît cependant que pour ce qui est des critères

[289] *Id.*, art. 49
[290] *Id.*
[291] *Id.*
[292] *Id.*
[293] Le G29 ou Groupe de travail « article 29 » était un organe consultatif européen indépendant, institué par l'article 29 de la directive de 1995 et dont les missions étaient notamment de conseiller, de donner des avis et des recommandations à la Commission quant à l'interprétation de la directive. Avec l'entrée en vigueur du RGPD, ce groupe a été remplacé par le Comité européen de la protection des données (CEPD), qui exercent entre autres des missions similaires.
[294] *Guidelines on Article 49 of Regulation 2016/679*, WP 261, Brussels, WP29.

dérogatoires de l'article 49 § 1a) à 49§1 g), ce caractère occasionnel n'est pas expressément reconnu.[295] Il indique que même si ce n'est pas le cas, ces dérogations devraient être interprétées comme étant un régime d'exception revêtant alors un caractère occasionnel.[296] Pour ce qui est de l'exception de nécessité, elle prend la forme d'un test afin d'évaluer si le test est nécessaire aux fins du critère dérogatoire. Ce test ne concerne cependant pas toutes les dérogations. Notamment, les dérogations de consentement et d'intérêt légitime en sont écartées.[297] Les lignes directrices du CEPD sur l'article 49 reprennent ensuite une à une chaque dérogation, en les interprétant, en les clarifiant ou en les expliquant. Par exemple, pour l'exception de consentement, le CEPD rappelle que ce dernier doit être exprès, spécifique à un transfert ou un ensemble de transfert, et éclairé.[298] Pour ce qui est de l'intérêt légitime, il doit être utilisé en dernier ressort et à des conditions particulières. Le CEPD prend l'exemple de petites et moyennes entreprises qui ne peuvent pas en pratique, opérer de transferts sous l'égide de règles d'entreprise contraignantes et qui pourraient donc utiliser ce type de dérogations. [299]

Le CEPD est venu clarifier et cadrer ce régime d'exception, non pas pour interdire les transferts de données, mais pour interpréter des règles larges et parfois ambiguës. Malgré cette interprétation des dérogations de l'article 49 par le CEPD, il en ressort que les règles du *RGPD*, en matière de flux transfrontières, peuvent s'avérer complexes et dispendieuses, mais ne sont jamais impossibles à mettre en œuvre, même pour qui ne respecte pas nécessairement les règles de protection des données. Or, une barrière non tarifaire peut être définie comme un : « ensemble de mesures restrictives non tarifaires mises en place par un pays et visant à protéger son marché de la concurrence extérieure ».[300] Dans le cas du *RGPD*, ces dérogations existent justement pour permettre l'accès au marché. Elles ne sauraient non plus être considérées comme des mesures restrictives. En effet, elles n'ont pas, par exemple, pour objet de défavoriser un opérateur étranger au profit d'un opérateur européen, ce dernier étant soumis au *RGPD*, souvent de manière plus contraignante. Tout au plus, on peut donc y voir une régulation de la concurrence par la Commission au moyen de la protection des données. Mais à notre sens, cette régulation a

[295] *Id.*, p. 4
[296] *Id.*
[297] *Id.*
[298] *Id.*, p.6 et p.7.
[299] *Id.*, p. 15
[300] GLOSSAIRE-INTERNATIONAL, « Définition de Barrière non tarifaire », *https://www.glossaire-international.com*, en ligne : <https://www.glossaire-international.com/pages/tous-les-termes/barriere-non-tarifaire.html>.

simplement pour but de mettre les opérateurs européens et étrangers sur le même pied d'égalité et non d'empêcher ou de décourager les opérateurs étrangers de pénétrer le marché ou d'y rester. Après tout, le *RGPD* n'a pas remis en question la présence d'acteurs étrangers sur le marché européen des technologies de l'information.

Quoi qu'il en soit, ce modèle de règles à portée extraterritoriale de protection des données dans le but de préserver la libre circulation permet d'assurer un certain contrôle économique sur les flux transfrontières de données. Ce contrôle économique semble être la volonté principale de l'Europe depuis les années 1990. Comme nous l'avons déjà relevé, le temps passe, mais les problématiques n'évoluent que peu. Finalement, le même modèle juridique est privilégié que l'on soit en présence de l'envoi d'une disquette ou d'un flux de données entre un établissement en Europe et une ferme de serveurs aux États-Unis.

À l'étude des modèles canadien et européen, peut-on alors raisonnablement prétendre que la protection des données personnelles relève toujours d'un fondement et d'une fin en soi plutôt que d'un moyen de légitimer une libre circulation internationale ? Nous ne le croyons pas puisqu'il s'agit davantage d'appliquer des standards européens à une conception de *privacy* américaine fondée sur les *torts*, dans le but de préserver la libre circulation consacrée en droit international public et à des fins de commerce. Par conséquent, il est nécessaire de s'intéresser au droit du commerce international consacrant le principe de libre circulation des données et contraignant les États sur le fondement du droit international public. Nous avons pu étudier la donnée comme caractéristique fondamentale de l'économie et l'émergence d'un véritable marché international de la donnée dans un environnement dérégulé et libre de toute contrainte relative à la circulation. Comme nous allons l'étudier, le droit du commerce international est venu s'immiscer relativement tôt dans les questions de droit des données, afin de protéger le marché international des données, garantie par la libre circulation des données. La question à laquelle on tentera alors de répondre dans le chapitre suivant est la suivante : assistons-nous à une convergence entre droit des données personnelles et droit du commerce international, voire une domination du droit du commerce international sur le droit des données ?

Chapitre 2 : La convergence entre droit des données personnelles et le droit du commerce international

On peut à ce stade, affirmer que la consécration de la vision américaine de *privacy*, le développement de politiques économiques favorisant la libre circulation des données personnelles depuis les années 1990 avec l'arrivée d'internet, l'essor des technologies de l'information et la place de la donnée au sein d'un marché global ont naturellement conduit la problématique des données personnelles sur le chemin du commerce international. Le fait que de plus en plus de règles sur la circulation des données personnelles sont conçues à un niveau supranational dans le contexte du droit du commerce international et, notamment, dans le cadre des accords de commerce international en est un bon indicateur (Section 1). Plus récemment, des voix s'élèvent même en faveur d'une règlementation des données personnelles par l'Organisation mondiale du commerce (Section 2).

Section 1 : Le droit des données dans les accords de commerce international

Depuis les années 2000, avec une forte progression pendant les dix dernières années, on assiste à l'émergence d'une règlementation de la circulation des données personnelles dans des outils de droit commercial international et, notamment, dans les accords de commerce international. Il s'agit alors d'étudier dans un premier temps la genèse de ce droit des données dans les accords de commerces internationaux, qui est un pur produit de l'OMC, avant de s'intéresser plus spécifiquement aux différentes approches d'intégration de clauses de données personnelles dans ces accords.

De la genèse du droit des données dans les accords de commerces internationaux

Nous avons pu constater que les premiers outils internationaux de régulation des flux transfrontières de données sont apparus au début des années 1980, avec principalement deux textes qui étaient les *Lignes directrices de l'OCDE* et la *Convention 108 du Conseil de l'Europe*. Ces textes résolument en faveur d'une libre circulation des données personnelles, quoiqu'enrobés d'intentions de protection, étaient des textes de droit des données. Par-là, on entend qu'une

approche *ad hoc* centrée sur le droit des données était privilégiée.[301] Dès lors, ces textes de droit international venaient s'ajouter à un droit des données national. On pourrait à cet égard, faire une distinction entre droit national des données et droit international des données. Mais les choses ont changé dans les années 1990 et, depuis, la tendance a été de faire converger droit international des données et droit du commerce international. Ce qui est certain, c'est que la conséquence pour les États reste la même, à savoir une restriction de leurs compétences en droit des données, du fait d'outils juridiques de droit international public, les obligeant.

Cette nouvelle impulsion a surtout été rendue possible avec les accords de Marrakech donnant naissance à l'Organisation mondiale du commerce en 1994. Cette dernière a toujours embrassé une vision libérale basée sur un principe fort de non-discrimination des États. À ce titre, on peut citer les obligations de la *nation la plus favorisée* et du *traitement national* figurant dans les premiers textes multilatéraux sur le commerce international comme le *GATT* et ayant notamment favorisé la création d'infrastructures des technologies de l'information.[302] On retrouve ces mêmes principes dans un texte qui nous intéresse davantage, figurant en annexe des accords de Marrakech et instaurant l'accord général sur le commerce des services, plus connu sous son acronyme anglais *GATS* pour *General Agreement on Trade in Services*.[303] Comme nous l'avons étudié, le transfert de données est encore bien souvent rattaché à une transaction principale, et dont le transfert est perçu comme l'accessoire. Plus précisément la fourniture de services est souvent liée à la nécessité de collecter et de traiter des données personnelles. Et lorsque cette fourniture de service a lieu en dehors des frontières d'un État, il y a un transfert transfrontière de données personnelles. Une autre raison invoquée pour rattacher les transferts de données au *GATS*, c'est simplement le fait que la donnée s'échange sans qu'il y ait recours à un transfert d'un support physique,[304] et échapperait alors à la qualification de commerce de biens, qui est régie entre autres par le *GATT*. Dans une optique de libéralisation du marché des services, objectif poursuivi par le *GATS*, il a été jugé bon d'insérer dans ce texte une clause visant à empêcher les États de prendre

[301] Par approche centrée sur le droit des données personnelles, on entend des textes spécifiques sur les données personnelles rejoignant la branche du droit des données, contrairement à des problématiques de données intégrées dans d'autres branches du droit, comme celle du droit du commerce international. Si l'on prend le cas des lignes directrices ou de la convention 108, ces textes sont des outils juridiques *ad hoc* avant tout.
[302] Mira BURRI, « The Regulation of Data Flows Through Trade Agreements », (2017) 48-1 *Georgetown Journal of International Law* 407-448, 411.
[303] *Accord général sur le commerce des services de 1994*, préc., note 247.
[304] Andrew D. MITCHELL et Jarrod HEPBURN, « Don't Fence Me In: Reforming Trade and Investment Law To Better Facilitate Cross-Border Data Transfer », (2018) 19-1 *Yale Journal of Law & Technology* 182, 190.

des mesures trop restrictives en matière de protection des données.[305] Une telle mesure permettait d'assurer la libre circulation des données personnelles entre les États et donc la continuité des services auxquels ces flux sont rattachés.[306] Ainsi, l'article XIV dispose que :

> « Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: […] (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: […] (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; »

Les règles du *GATS* laissent la possibilité aux États de prendre des mesures de protection des données personnelles, sous une forme négative puisque c'est seulement si la libre concurrence (impliquant une libre circulation) est respectée, que des mesures de protection des données peuvent être adoptées. *A contrario*, des règles de protection des données déjà prises par les États pourraient être considérées comme violant les dispositions du G.A.T.S dans le cas où elles attenteraient trop à la liberté d'échanges de service. À ce titre, certains auteurs se sont même demandé si le *RGPD* serait considéré comme en violation de cette disposition au regard de la jurisprudence de l'OMC en matière de balances d'intérêts.[307]

Un exemple plus concret est celui d'un État qui obligerait une organisation à stocker des données sur son territoire. De telles mesures pourraient être jugées comme étant en violation de la section XIV du *GATS*, puisque cela engendrerait des coûts conséquents pour les organisations voulant s'y implanter.[308] Il a même pu être avancé que de telles mesures contribueraient à saborder des objectifs de protection de la vie privée et de sécurité en empêchant ce que l'on appelle le « sharding »[309] et dès lors s'exposer à des attaques malveillantes entraînant de plus grandes

[305] C. KUNER, préc., note 235, p. 52.
[306] *Id.*, p. 52.
[307] Mira BURRI, « The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation », (2017) 51 *UC Davis Law Review* 65, 92.
[308] A. D. MITCHELL et J. HEPBURN, préc., note 304, 195.
[309] Le *Sharding* consiste à partitionner les données en fragmentant les bases de données. Voir, Gaëtan RAOUL, « Qu'est-ce que le sharding ? Définition et avantages de cette méthode de distribution des données », *lebigdata.fr*,

conséquences du fait d'une centralisation des données trop importante.[310] Des règles étatiques seraient alors contreproductives et ne devraient être perçues que comme des barrières non tarifaires au commerce. L'argument est plus que discutable, mais quoi qu'il en soit, on retrouve de telles clauses d'interdiction de stockage des données dans certains accords impliquant les États-Unis.[311]

Dans un premier temps, cette clause de l'article XIV du *GATS* a servi de modèle dans les accords de commerces internationaux pour régler des questions de flux transfrontières de données. Ensuite, la lettre du texte a évolué au fur et à mesure en fonction des intérêts des parties fortes, signataires des traités.

Des différentes approches d'intégration de clauses de données personnelles dans les accords de commerce international

Dans ce paragraphe, nous étudierons deux approches d'intégration de questions de droit des données personnelles dans les accords de commerce internationaux. Ces intégrations sont révélatrices de la convergence entre droit des données et droit du commerce international.

1. L'approche européenne

L'approche de l'Union européenne a consisté, dans un premier temps, à transposer cette clause dans les accords de libre-échange l'impliquant. Cependant, dans certains rares cas, les accords de libres échanges bilatéraux de l'UE notamment avec le Canada et avec la Corée du Sud semblent se détacher du modèle du *GATS* à certains égards et adoptent une approche positive.[312] En effet, et ce malgré de légères différences, ces accords contiennent tous deux des dispositions sectorielles, notamment en matière de services financiers, dans lesquelles chaque partie s'engage à prendre des mesures de protection de la vie privée en matière de transfert de données personnelles.[313] Dans *l'Accord économique et commercial global/Comprehensive Economic and Trade Agreement* (CETA) entre l'Union européenne et le Canada, une règle de territorialité, est

7 septembre 2017, en ligne : <https://www.lebigdata.fr/sharding-definition-avantage#:~:text=Le%20Sharding%20permet%20d%27organiser,aux%20coûts%20bien%20plus%20raisonnables.>.
[310] A. D. MITCHELL et J. HEPBURN, préc., note 304, 195.
[311] *Infra*, p. 104.
[312] Federica VELLI, « The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements », (2019) 4-3 *European Papers* 881, 890.
[313] *Id.*, 890.

ajoutée puisque la loi applicable est celle du territoire d'où le transfert s'opère,[314] ce qui constitue une manière de faire appliquer la loi européenne aux flux de données sortants. Bien que cette approche positive existe, elle reste bien souvent cantonnée au domaine des services financiers. Elle fait donc plutôt figure d'exception dans ces accords. L'approche générale est celle que l'on retrouve dans le volet du commerce électronique.

Dans les dispositions régissant le commerce électronique, les règles diffèrent, puisque l'accord de libre-échange entre l'Union européenne et la Corée du Sud (EUKOR) reprend les exceptions du *GATS* tandis que le CETA recommande simplement d'adopter ou de maintenir des règles de protection des données personnelles pour chaque partie.[315] Au titre de la confiance dans le commerce électronique, l'article 16.4 du CETA dispose que :

> « Chaque Partie devrait adopter ou maintenir des lois, des règlements ou des mesures administratives pour assurer la protection des renseignements personnels des utilisateurs du commerce électronique, en tenant dûment compte des normes internationales de protection des données établies par les organisations internationales compétentes dont les deux Parties sont membres. »[316]

L'article 7.48 de l'accord de libre-échange entre l'UE et la Corée du Sud[317] dispose quant à lui que :

> « 1. Les parties, reconnaissant que le commerce électronique génère des perspectives en matière de commerce et de croissance économique, qu'il importe de prévenir les obstacles à son utilisation et à son développement, […] conviennent d'encourager le développement du commerce électronique entre elles […] 2. Les parties conviennent que le développement du commerce électronique doit être pleinement compatible avec les normes internationales de protection des données, afin d'asseoir la confiance des utilisateurs dans le commerce électronique. »[318]

---

[314] *Accord économique et commercial global entre le Canada, d'une part, et l'Union européenne, d'autre part*, Can./U.E., 14 janvier 2017, J.O. 14 janvier 2017 (n° 22017A0114 (01) [*CETA*].
[315] *Id.*
[316] *Id.*, art. 16.4.
[317] *Accord de libre-échange entre l'Union européenne et ses États membres, d'une part, et la République de Corée, d'autre part*, Rep. Cor./U.E., 14 mai 2011, J.O. 14 mai 2011 (n° 22011A0514 (01)) [*EURKOR Agreement*].
[318] *Id.* Art. 7.48.

Ainsi, à l'étude de ces accords, on se rend compte que les mesures de protection des données sont vagues, puisqu'elles renvoient à chaque partie le soin d'adopter des règles dont les contours restent flous.[319] On constate que le principe de libre circulation des données est consacré par ces accords, mais que les standards de protection sont principalement l'affaire des parties tant que ces derniers n'entravent pas la libre circulation. Cependant, il est probable que la pleine gestion de ces standards de protection soit laissée aux mains des États, uniquement parce que le Canada et la Corée du Sud ont des réglementations de protection des données personnelles considérées comme fortes. Le constat doit être le même pour ce qui est de l'Union européenne et du Canada. En effet, l'article 16.6 du CETA prévoit par exemple un dialogue sur le commerce électronique entre les autorités européennes et canadiennes.[320] Notamment, la protection des renseignements personnels fait partie des questions pouvant faire l'objet d'un dialogue.[321] Ce dialogue peut : « prendre la forme d'un échange d'informations sur les lois, règlements et autres mesures respectifs des Parties afférents à ces questions, ainsi que d'un partage d'expériences concernant la mise en œuvre des lois, règlements et mesures en question. »[322] Cette même disposition, quand bien même elle ne vise pas expressément la protection des données, mais revêt un caractère plus général, existe également dans l'accord entre l'UE et la Corée du Sud.[323] Ce dialogue nécessite en amont d'avoir *a minima* des régimes de protections de données équivalents et des autorités de contrôle chargées de ces questions pour pouvoir faire naître un tel échange. Les dispositions de l'article 16.6 et leurs équivalents dans le traité UE/Corée du Sud, soutiennent, par conséquent, l'idée selon laquelle la gestion de la protection des données est laissée aux parties du fait de régimes équivalents ou, tout du moins, compatibles.

On pourrait également supposer que le contenu de ces accords reflète des négociations faites sous l'égide de la directive de 1995 et non du *RGPD*. C'est d'ailleurs ce qui tend à se vérifier dans une nouvelle génération d'accords *post RGPD* encore en négociation.[324] En effet, une approche positive et contraignante, en faveur d'un droit à la protection des données plus fort, semble émerger. Les premières moutures accessibles montrent le déploiement de règles de protection des données

[319] De surcroît, le degré de contrainte dans l'adoption de ces règles pour les États peut varier selon les secteurs visés comme nous avons pu le voir avec l'approche positive visant les services financiers.
[320] *CETA*, préc., note 314, art. 16.6.
[321] *Id.*
[322] *Id.*
[323] *EURKOR Agreement*, préc., note 317, art. 7.49.
[324] Au moment où nous écrivons ces lignes.

dans les flux transfrontières qui ne sont plus sectorielles, mais transversales.[325] En effet, l'accord en négociation avec l'Indonésie contiendrait un chapitre complet intitulé : « Cross-border data flows and protection of personal data and privacy ».[326] Parmi ces dispositions, on retrouve sans surprise la consécration du principe de libre circulation des données en matière de flux transfrontières.[327] Ce principe est notamment accompagné de quatre catégories d'interdictions portant sur des mesures qui empêcheraient trop la libre circulation.[328] Ces interdictions sont les suivantes :

> « a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party; b) requiring the localisation of data in the Party's territory for storage or processing; c) prohibiting storage or processing in the territory of the other Party; d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory. »[329]

En résumé, ces règles interdisent aux parties d'imposer aux responsables de traitement ou aux sous-traitants de traiter des données, ou de stocker des données sur leurs territoires, favorisant de ce fait la libre circulation des données.

Mais c'est en matière de protection des données que les choses sont plus intéressantes. On y retrouve notamment une approche européenne, qui consiste à faire de la protection des données un droit fondamental *relatif* au service de la libre circulation :

> « Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade. »[330]

---

[325] F. VELLI, préc., note 312, 892.
[326] Cela constitue un changement par rapport aux accords d'ancienne génération, intégrant des dispositions sur les données personnelles dans certains chapitres-thématiques du libre-échange.
[327] *EU proposal for provisions on Cross-border data flows and protection of personal data and privacy*, Brussels, European Union, en ligne : <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf>.
[328] *Id.*, art. 1.
[329] *Id.*
[330] *Id.*, art. 2.1.

Autre point important, la discrétion concernant le niveau de protection des règles établies est laissée aux États, et ces règles nationales ne peuvent être affectées par d'autres dispositions présentes dans les accords.[331] Cela signifie que les normes nationales mises en œuvre par les parties à des fins de protection des données et de protection de la vie privée devraient prévaloir sur les dispositions prévues par l'accord en cas de conflit de règles. Il est intéressant de noter ce renoncement d'une norme supraétatique au profit d'une norme nationale dans le cadre d'un litige. Reste à savoir comment les juges pourraient interpréter cette disposition, qui prend le contre-pied de la tendance observée en droit international en matière de données personnelles.

De surcroît, ces règles de protection des données personnelles sont renforcées par le fait qu'elles ne sont pas contestables devant le tribunal d'investissement.[332] En effet, le paragraphe 5 de l'article 2 de la proposition d'accord entre l'UE et l'Indonésie dispose que le système du tribunal d'investissement prévu ne s'applique aux dispositions sur les données personnelles.[333] La volonté de soustraire la protection des données personnelles au domaine de l'investissement international constitue de notre point de vue une bonne nouvelle. En effet, les tribunaux d'arbitrage en matière d'investissements se sont multipliés dans les accords de libre-échange, et avec eux la possibilité d'aller à l'encontre du droit national dans le cadre d'une procédure judiciaire. Ces tribunaux font en effet prévaloir le droit international du commerce sur les normes étatiques afin de permettre la pérennité des investissements à travers le monde, en éliminant les barrières que constitueraient des règles étatiques jugées trop contraignantes. Cependant, ces décisions vont bien souvent à l'encontre du bien-être de la population : on pense notamment à des décisions remettant en cause des normes étatiques de sauvegarde de l'environnement.[334] Le fait que le droit des données personnelles puisse échapper au règne des règles internationales sur l'investissement est une avancée en faveur d'une protection plus forte des individus.

Cependant, tout n'est pas gagné. L'accord en négociation avec l'Australie reprend certes les mêmes règles de protection de données que l'on retrouve dans les nouveaux modèles d'accords

[331] *Id.*, art. 2.2.
[332] *Id.*, art. 2.5.
[333] *Id.*
[334] Kintxo FREISS, « Protection de l'environnement et expropriation indirecte dans les accords mega-régionaux », (2018) 31-1 *Revue québécoise de droit international* 38, 49.

post-RGPD.[335] Mais, on suppose que ces règles restent contestables devant un tribunal d'arbitrage, ce point n'étant pas expressément mentionné dans le texte.[336]

Entre les anciens accords établis et les nouveaux accords en préparation, on perçoit alors une mutation des dispositions du droit des données personnelles. Dans les nouveaux accords, on consacre des principes de protection directement dans le texte de l'accord. C'est une différence notoire, là où on se contentait de mettre en balance protection et libre circulation dans les anciens accords sans inscrire les principes de protection à respecter dans le corps du texte. L'intégration de ces principes au sein des accords peut alors être vue comme un progrès relatif, certes, mais qui doit tout de même être souligné. La qualification de la protection des données personnelles comme droit fondamental (*relatif*) dans ces propositions d'accords est le premier de ces nouveaux principes, et peut-être même le plus important. On doit également souligner la prévalence de normes nationales de protection des données sur les dispositions de l'accord en cas de conflit de normes. Ce second principe constitue sans doute une avancée de taille dans la protection des données transfrontières au sein des accords de libre-échange. Cela permettrait aux États de récupérer une partie de leurs prérogatives pour protéger les données de leurs ressortissants des violations induites dans le cadre du commerce international. La lecture combinée de ces deux principes de protection des données permet de dégager deux hypothèses :

- La première hypothèse est celle dans laquelle un pays n'est pas doté d'un régime de protection permettant d'assurer la protection des données personnelles comme un droit fondamental. Dans ce cas de figure, cet État devrait se doter de standards de protection équivalents à ceux de l'UE pour se conformer aux dispositions du traité.

- La deuxième hypothèse est celle selon laquelle un État a déjà un droit protégeant efficacement les données personnelles ou consacre la protection des données comme un droit fondamental. Dans ce cas-là, du fait de la prévalence des normes

[335] À savoir : les quatre interdictions de mesures empêchant la libre circulation (art. 5), la protection des données comme droit fondamental relatif au service de la libre circulation (art. 6 § 1), la prévalence du droit national sur les dispositions de l'accord en matière de protection des données (art. 6 § 2), voir : *European Union's (EU) proposal for the EU-Australia FTA*, Brussels, European Union, 2018, en ligne : <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf>.
[336] *Id.*

nationales de protection des données sur les dispositions du traité[337], cet État devrait pouvoir assurer le niveau de protection prévu par son droit national, sans y renoncer au détriment de la norme supraétatique contenue dans le traité.

L'approche de l'UE dans la négociation des accords de libres échanges s'inscrit en faveur d'une protection des données plus forte, garante de la libre circulation depuis l'entrée en vigueur du *RGPD*. On note également une émancipation européenne des règles issues du commerce international (on pense à l'article XIV du *GATS*), par rapport aux accords ratifiés sous la directive. De manière générale, il y a moins, voire pas de renvois explicites vers les normes internationales de protection des données. Mais entendons-nous bien : cette approche contient certains aspects novateurs et consacre une protection des données internationale plus forte. Cependant elle n'est pas non plus de nature à remettre substantiellement en cause la libre circulation des données personnelles (qui reste la priorité) au détriment de la protection des données. Mais ces nouvelles règles ouvrent certaines portes pour remettre la protection des données dans les mains des États, tout en imposant la mise en œuvre d'un régime juridique avec de hauts standards de protection pour les États qui n'en seraient pas dotés. C'est la distinction majeure que l'on pourrait faire avec les accords d'anciennes générations qui, eux, se contentent d'appeler les parties à se conformer aux normes internationales. Dès lors, dans les accords *pré-RGPD*, on ne s'occupe pas du contenu des règles nationales de protection des données tant que la libre circulation de celles-ci est assurée sur le plan international. Tel n'est pas le cas dans les nouvelles propositions d'accords qui adoptent une position beaucoup plus positive et contraignante. En somme, on passe d'une approche passive à une approche plus active de la question de la protection des données dans les accords de libre-échange impliquant l'Europe.

2. L'approche états-unienne

Les États-Unis sont coutumiers des règles à portée extraterritoriales leur permettant d'accéder aux données partout sur le globe. Ainsi, des textes comme le *Patriot Act*[338] (expiré depuis

[337] Reste à voir comment cette prévalence pourrait s'articuler avec les interdictions pour les parties d'imposer le stockage ou le traitement sur leurs territoires.

[338] Au moment des révélations Snowden, l'article 215 du texte prévoyait que le gouvernement américain pouvait sur simple autorisation de la cour de surveillance du renseignement étranger, ordonner à un tiers de transmettre n'importe

2020), le *FISA*[339] ou encore le *Cloud Act*,[340] permettent au gouvernement américain de jouir d'un arsenal juridique conséquent en matière d'accès extraterritorial aux données de toute nature. Il n'est alors pas surprenant que ces dispositions aient été complétées sur le plan supranational, avec des règles permettant de contrôler la circulation des données, en s'assurant paradoxalement qu'elle soit le plus libre possible, en s'appuyant juridiquement sur les règles libérales prévues par l'OMC.

Pour ce faire, on retrouve des clauses d'interdiction de localisation des données sur le territoire d'un État dans des accords de libre-échange impliquant les États-Unis, clause qui nous l'avons vu, ne pose aucun problème, étant donné les exceptions prévues par le *GATS*. Ainsi, dans le nouvel accord États-Unis–Canada-Mexique, on retrouve une section dans le chapitre sur le commerce numérique qui dispose que :

> « Une Partie n'exige pas d'une personne visée qu'elle utilise ou situe des installations informatiques sur le territoire de cette Partie comme condition à l'exercice des activités commerciales sur ce territoire »[341].

Cette disposition est à lier avec l'article 19.11 § 1 qui dispose que :

> « Aucune Partie n'interdit ni ne limite le transfert transfrontière de renseignements, y compris de renseignements personnels, par voie électronique si cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée. »[342] [343]

---

quel enregistrement (ou « chose tangible ») jugé pertinent dans le cadre d'une investigation en matière de terrorisme international, de contre-espionnage et de renseignement étranger. Voir : BRENNAN CENTER, « Are they allowed to do that? A breakdown of selected government surveillance programs », *https://www.brennancenter.org*, en ligne : <https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf> (consulté le 1 avril 2022).

[339] Le Foreign Intelligence Surveillance Act prévoit à son article 702 que le Procureur général des États-Unis et le Directeur du renseignement national à autoriser conjointement, le ciblage de personnes dont on peut raisonnablement croire qu'elles se situent en dehors des États-Unis, dans le but d'obtenir des informations de renseignement extérieur.

[340] Dans le Cloud Act qui vient mettre fin à la sage judiciaire *Microsoft Ireland* c. *U.S.*, le texte clarifie le fait que l'opérateur de services numériques doit communiquer aux autorités toutes les informations qu'il détient, dont il a la garde ou le contrôle, peu importe la localisation de la donnée, pourvu que l'autorité demanderesse soit munie d'un mandat à son encontre. Pour l'affaire *Microsoft Ireland* v. *U.S,* voir : S. LONGHAIS, préc., note 228, p 76 et suiv.

[341] *Accord Canada-États-Unis-Mexique*, Can./Mex./É.-U., 30 novembre 2018, (entré en vigueur le 1er juillet 2020), art. 19.12.

[342] *Id.*, art.19. 11.

[343] Une exception d'objectif de politique publique est prévue à condition que cette dernière : « ne soit pas appliquée de façon à constituer un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce ; […] d'autre part, n'impose pas de restrictions sur les transferts de renseignements qui soient plus importantes que celles qui sont nécessaires pour atteindre cet objectif », *Id.* art. 19.11. On pense notamment aux politiques de modernisation des lois sur les renseignements personnels au Canada pourrait par exemple entrer dans cette catégorie de politique publique.

Ces deux clauses prévues dans l'accord multilatéral de libre-échange entre les États-Unis, le Mexique et le Canada assurent une libre circulation entre ces trois pays de toutes les données, y compris personnelles, pour ce qui est du commerce électronique, en cassant une dynamique de protectionnisme de l'information, d'une part, et en consacrant le principe de libre circulation des données dans un texte supranational contraignant, d'autre part. Ainsi, les leviers à la disposition du gouvernement américain sont très importants, puisque la prééminence des acteurs du numérique américain leur permet *in fine* de s'arroger un contrôle sur tous les flux de données transfrontières tombant sous le coup de cet accord. En effet, dans cet accord, la grande majorité des acteurs du numérique susceptibles de transférer des données concernant des utilisateurs des États parties à l'accord sont américains. On aura vu que le gouvernement américain possède des règles à portée extraterritoriale redoutables pour récupérer les données collectées par ces compagnies. Dès lors, un accord consacrant un principe de libre circulation des données leur permet encore plus facilement d'obtenir un contrôle très important sur les flux transfrontières s'opérant sous l'égide de cet accord.

Dans un des accords bilatéraux impliquant les États-Unis, on notera le constat de l'importance d'une protection des données personnelles à titre assez indicatif, comme s'il s'agissait de le mentionner de manière informative. On retrouve cet aspect indicatif de la protection des données dans le traité entre la Corée du Sud et les États-Unis, à l'article 15.8 du texte dans le chapitre sur le commerce électronique :

> « Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders. »[344] [345]

Dans la formulation, il y a pour commencer, un accent qui est mis sur la libre circulation au détriment de la protection des données. Contrairement aux accords de première génération impliquant l'Union européenne dans lesquels on retrouvait certaines recommandations de prendre

[344] *EURKOR Agreement*, préc., note 317, art. 15.8.
[345] Traduction libre, le texte n'a pas de traduction officielle en français : *reconnaissant l'importance de la libre circulation des données en vue de faciliter le commerce et prenant acte de l'importance de protéger les données personnelles, les parties devraient s'abstenir d'imposer ou de maintenir des barrières non-nécessaires aux flux transfrontières d'informations électroniques.

des mesures de protection, les modèles d'accords bilatéraux états-uniens ne s'embarrassent pas de garde-fous, aussi légers soient-ils. Ici, on est typiquement dans le schéma dans lequel on consacre une libre circulation externe des données personnelles, sans prévoir de dispositions visant à protéger les données. Jusqu'ici, on pourrait penser que cela ne fait pas réellement de différence. Cependant, un raisonnement a *contrario* permet de s'apercevoir que c'est une libre circulation sans limites qui est prévue. En effet, si une telle protection n'existe pas sur le territoire des parties, les données sont libres de circuler. Rien dans les accords n'empêche l'absence de protection des données dans les États parties. Et force est de constater que la situation des États-Unis en matière de réglementation de l'usage des données personnelles ne progresse que très lentement. Pour ne rien arranger, la majeure partie des partenaires commerciaux des États-Unis ne se retrouvent pas en situation d'obtenir des garanties de protection des données personnelles de la part de ces derniers.

Et pourtant, c'est le « mieux » que l'on puisse trouver dans les accords bilatéraux entre les États-Unis et ces différents partenaires commerciaux. En effet, la question n'est pas abordée davantage dans les autres traités, tous fabriqués dans le même moule. Il faut donc se contenter d'un simple constat de l'importance de la protection des données dans les accords de libre-échange entre les États-Unis et leurs partenaires commerciaux. Ainsi, la libre circulation des données est consacrée comme un principe inébranlable, puisque très souvent rattaché à la circulation de services au travers du respect des règles de l'OMC,[346] interdisant les discriminations au commerce électronique de services,[347] même si formellement il n'y a pas d'interdiction de prendre des mesures de protection des données personnelles.[348] Il est tout de même utile de mentionner que le traité de libre-échange entre les États-Unis et Singapour mentionne vaguement la protection des données comme étant une compétence du *Financial Services Comitee.*[349] Le *Financial Services Commitee* est un organe de contrôle instauré par ce traité. Il a pour mission de veiller à la bonne application des règles sur les services financiers présentes dans l'accord. Ce comité a

[346] Sacha WUNSCH-VINCENT et Arno HOLD, « Towards coherent rules for digital trade: Building on efforts in multilateral versus preferential trade negotiations », *World Trade Institute Papers* 2012.251, p. 14.
[347] *United States-Morocco Free Trade Agreement*, É.-U./Mar., 15 juin 2004, art. 14. ; *United States-Bahrain Free Trade Agreement*, É.-U./Bar., 14 septembre 2004, art. 13.4. ; *United States-Peru Free Trade Agreement*, É.-U./Per., 12 avril 2006, art. 15.3. ; *United States-Australia Free Trade Agreement*, É.-U./Aus., 18 mai 2004, art. 16.4.
[348] S. WUNSCH-VINCENT et A. HOLD, préc., note 346, p. 22.
[349] *United States-Singapore Free Trade Agreement*, É.-U./Sing. 6 mai 2003.

principalement des mandats de supervision, de consultation et d'arbitrage.[350] À ce titre, il a notamment la compétence d'étudier, à la demande d'une des parties, les questions relatives à la protection de la vie privée des individus dans le traitement et la dissémination des données personnelles, ainsi que la protection de la confidentialité des dossiers et comptes individuels.[351] Ce comité a une compétence plus générale sur les transferts d'informations effectués à l'intérieur et en dehors du territoire des parties par des institutions financières, pour des traitements de données effectués nécessaires à l'exercice de la profession.[352] Cependant, cette exception est noyée dans une myriade d'accords prônant une libre circulation sans limite.

Concernant l'absence de protection des données personnelles dans les accords américains, le propos doit être nuancé lorsque les États-Unis négocient des accords avec des partenaires plus privilégiés ou plus puissants économiquement. À ce titre, l'ACEUM prévoit un article sur la protection des renseignements personnels au chapitre du commerce électronique. En substance, chaque partie peut adopter ou maintenir un cadre juridique assurant la protection des renseignements personnels dans le respect des standards internationaux.[353] On y reconnaît également les « grands » principes de la protection moderne des données, tels que la limitation de la collecte, la finalité de la collecte, la limitation dans l'utilisation ou encore les garanties de sécurité.[354] Cependant, en adéquation avec l'article 19.11, il faut que les États fassent en sorte que toute restriction sur les flux transfrontières de données soit « nécessaire et proportionnée aux risques associés ».[355] Si les applications extraterritoriales de mesure de protection semblent exclues,[356] chaque partie assure aux usagers des recours dans leurs juridictions, et des moyens de contraindre les entreprises à se conformer aux exigences en vigueur dans le pays.[357]

Cet article inséré dans le nouvel ALENA est notamment empreint des standards de protection des données qui existent dans les lois canadiennes de protection des renseignements personnels, dont on ressent l'influence dans le texte. Preuve que les négociations ont été plus

[350] *Id.*, art. 10.6.
[351] *Id.*, Annex 10 D.
[352] *Id.*
[353] Ici, on renvoie aux lignes directrices de l'OCDE ou aux lignes directrices de l'APEC (pour ces dernières, *infra*, p. 114).
[354] *Accord Canada-États-Unis-Mexique*, préc., note 341, art. 19.8.
[355] *Id.*
[356] *Id.*
[357] *Id.*

équilibrées et ne relèvent pas du simple contrat d'adhésion que les États-Unis fournissent normalement à leurs partenaires commerciaux. Par ailleurs, on retrouve un article rédigé dans les mêmes termes au sein du *Trans Pacific Partnership*, l'accord multilatéral de libre-échange réunissant l'Australie, Brunei, le Canada, le Chili, le Japon, le Mexique, la Nouvelle-Zélande, le Pérou, Singapour et le Viêt Nam signé en 2016 et dont les États-Unis se sont retirés en 2017. Il convient de le citer, car même si les États-Unis s'en sont retirés, ils avaient, dans un premier temps, négocié et signé cet accord. Cependant, il ne s'agit pas d'être dupe, puisque le *lobbying* américain des grandes entreprises du numérique vise à promouvoir une économie numérique libre et sans contraintes, à laquelle la libre circulation des données personnelles est nécessaire, ainsi qu'en atteste *The Digital 2 Dozen* qui gouvernent le TPP.[358]

Selon les parties en présence, il existe alors plusieurs manières d'assurer une libre circulation des flux transfrontières de données personnelles, par le biais du droit du commerce international. Cependant, les règles issues de l'OMC restent encore très présentes avec l'esprit libéral qu'on lui connaît. Pour cette raison plusieurs voix militent pour une réglementation des flux transfrontières de données au niveau de l'OMC.

[358] Ce sont des principes obligatoires promouvant un Internet libre, ouvert et sans frontières visant à favoriser le développement de l'économie numérique. Un des principes est de permettre aux flux transfrontières de circuler librement tout en cassant les mesures trop protectrices vues comme des barrières au commerce et un désavantage pour les entreprises américaines. U.S. GOV., « The Digital 2 Dozen », *ustr.gov*, en ligne : <https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf>.

Tableau récapitulatif de la protection des données des accords de libres échanges

	UNION EUROPÉENNE (accords d'ancienne génération)	**UNION EUROPÉENNE (accords de nouvelle génération)**	**ÉTATS-UNIS**
Influence de la clause de l'article XIV du *GATS*	**OUI**	**NON**	**OUI**
Consécration de la libre circulation des données	**OUI**	**OUI**	**OUI**
Protection des données prévues dans l'accord	**OUI** (Passive) (Laissée aux États à condition de ne pas contrevenir aux dispositions des accords)	**OUI** (Active)	**NON**
Dispositions sectorielles concernant la protection des données	**OUI** dans certains accords sur les services financiers	**NON** (Dispositions transversales)	**NON** (Exception pour l'accord E.U./Singapour et les missions du Financial Services Committee)
Dispositions spécifiques sur les flux transfrontières de données	**NON**	**OUI** (Consécration d'un chapitre entier sur le sujet)	**NON**
Prévalence des règles nationales de protection des données sur les règles de l'accord	**NON**	**OUI**	**NON**
Interdiction pour une partie d'imposer la localisation des données sur son territoire	**NON**	**OUI**	**OUI**

Section 2 : Les voix en faveur d'une régulation internationale des données par l'OMC

Du fait de la règlementation internationale sur le commerce provenant de l'OMC et couvrant les questions de données personnelles, de la présence de nombreux traités de libre-échange s'emparant de ces questions et de la tendance à assimiler la circulation de données personnelles au commerce électronique, il existe des arguments en faveur d'une réglementation internationale des données par l'OMC. Tout d'abord, l'OMC est dotée de règles juridiques protégeant la libre circulation des données. Il s'agira ici de les détailler. De plus, la modernisation de ces règles est, à l'heure actuelle, encouragée par une volonté politique en faveur d'une libre circulation au sein de l'OMC.

Les règles juridiques de l'OMC en faveur d'une libre circulation des données

Nous l'aurons vu, l'OMC a joué un rôle dans la libre circulation des données en permettant via un mécanisme d'exception prévu dans le *GATS* d'insérer des clauses dans les accords de libre-échange réduisant la marge de manœuvre des États en matière de droit de la protection des données personnelles. Cependant l'influence de l'OMC sur la libéralisation de la circulation internationale de données va au-delà de la section XIV du *GATS*. En réalité, elle s'arroge la compétence sur les données dès 1998, lorsque le conseil général de l'instance cette année-là instaure le programme de travail sur le commerce électronique. Au titre de ce programme, l'OMC définit le commerce électronique comme :

> « The production, distribution, marketing, sale or delivery of goods and services by electronic means ».[359]

Si cette définition était originellement applicable à la vente de biens ou de services en ligne, on peut tout à fait imaginer que la circulation des données entre dans cette définition.[360] En effet, comme nous l'avons vu, il y a eu progressivement une scission entre la donnée comme accessoire à une transaction principale — typiquement la vente de biens ou de services — et la donnée comme bien économique ayant une valeur intrinsèque. Ces deux types d'exploitation économique des

[359] ORGANISATION MONDIALE DU COMMERCE, « Le commerce électronique », *wto.org*, en ligne : <https://www.wto.org/french/tratop_f/ecom_f/ecom_f.htm>.
[360] Cédric LETERME, « Qui captera l'"or du XXIe siècle" ? Bataille autour des données numériques », *monde-diplomatique.fr*, novembre 2019, en ligne : <https://www.monde-diplomatique.fr/2019/11/LETERME/60937>.

données trouvent tout à fait à entrer dans la définition adoptée par l'OMC du commerce électronique. Certes, les problématiques de circulation de données à l'OMC sont réglementées par les dispositions sur les services, du fait du développement de l'économie de services. Mais les infrastructures physiques permettant le transport de l'information (cruciales pour pérenniser la circulation des données) auraient tendance à tomber sous le coup de la règlementation sur les biens. On pense notamment à l'*Information Technology Agreement* ayant favorisé le développement d'infrastructures mondiales de télécommunications.[361] En matière de service, on vise également à assurer une libre circulation. En pratique, le *GATS* permet la circulation des données par la libéralisation des services à l'échelle mondiale. En effet, les principes tels que celui du *traitement national* et celui de la *nation la plus favorisée,* formulés dans le *GATS* restreignent considérablement la marge de manœuvre étatique sur le commerce de service[362] et préservent ainsi la libre circulation de données. Plus précisément, l'action étatique est freinée du fait des règles du *GATS* sur les services informatiques et les services connexes prévus dans la liste exhaustive de services encadrés par l'OMC, W/120 Classification.[363] À ce titre, l'Union européenne s'est engagée à ne pas limiter l'accès à son marché et à respecter les principes de *traitement national*, notamment en ce qui concerne la sous-catégorie sur les services de traitement de données.[364] Dès lors, ces engagements pourraient être contredits par les différentes règlementations existant sur les données en Europe même si pour l'heure aucun panel de l'OMC n'a eu l'occasion de se pencher sur ce sujet.[365] En matière de supériorité de la règle dictée par l'OMC, réduisant la capacité des États a pouvoir dire le droit, ce qui est visible en droit des données, concourt d'un phénomène plus vaste que le Professeur Benyekhlef qualifie d'« axiologie du droit commercial international ».[366] En substance, cela renvoie à la supériorité des règles internationales de commerce sur le droit interne des États, mais également sur d'autres règles de droit supraétatiques des droits de la personne ou de l'environnement.[367] En matière de droit des données, on constatera que l'hypothèse selon laquelle le principe de libre circulation des données est consacré par l'OMC au détriment du

[361] M. BURRI, préc., note 307, 76 à 78.
[362] *Id.*, 83.
[363] Nivedita SEN, « Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path? », (2018) 21-2 *Journal of International Economic Law* 323, 332.
[364] M. BURRI, préc., note 307, 84.
[365] *Id.*, 85.
[366] Karim BENYEKHLEF, *Une possible histoire de la norme, les normativités émergentes de la mondialisation*, 2e éd., Montréal, Thémis, 2015, p. 304.
[367] *Id.*

droit interne se vérifie. C'est le cas du fait des règles du *GATS*, mais c'est également le cas dans la plupart des accords de commerce international qui en font application en copie conforme, retirant *ipso facto* la possibilité de freiner la libre circulation des données à des fins de protection. Au point de vue du droit international, pour l'heure, aucune règle supraétatique ne semble aller à l'encontre des règles prescrites par le *GATS*, à savoir vers une remise en cause du principe de libre circulation à des fins de protection.

Certains auteurs considèrent même que les principes de vie privée et de sécurité notamment sont compatibles avec les missions de l'OMC de développement du commerce international.[368] Ces considérations rejoignent le discours général dont nous avons déjà pu faire état, à savoir que les mesures de protection des données personnelles permettent de légitimer la libre circulation en suscitant une certaine confiance de la part des utilisateurs[369], libre circulation par essence bonne pour le commerce électronique. Pour ces auteurs, les principes généraux du *GATS*, bien qu'étant apparus dans un contexte préinternet, permettent une interprétation par le panel de l'OMC, qui prendrait en compte des principes de vie privée de nature à répondre aux enjeux de protection des données.[370]

Dès lors, au niveau commercial, les outils existent à l'OMC pour réguler, ou plutôt déréguler la circulation des données de toute nature et s'inscrivent dans une mouvance plus globale de prévalence des règles de droit du commerce international.[371] Cependant les procédures sont longues et complexes et le résultat escompté n'est pas forcément à la hauteur des espérances. Par exemple, aucune sanction n'a été prise à l'encontre d'un État au niveau international, au regard d'une loi sur la protection des données qui serait trop protectrice, puisqu'aucun panel n'a jamais été saisi dans ce type d'affaires. À la fin 2020, l'OMC s'inquiétait même de la tendance de certains États à exercer un protectionnisme numérique.[372] Pour autant, la volonté politique de sacraliser la

[368] Neha MISHRA, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, NUS Centre for International Law Research Paper, 19/09, Singapore, NUS Centre for International Law, 2018, p. 498.
[369] *Id.*, p. 503.
[370] *Id.*, p. 504.
[371] K. BENYEKHLEF, préc., note 366, p. 241 et suiv.
[372] Julien BOUISSOU, « L'OMC s'inquiète du protectionnisme numérique », *lemonde.fr*, 23 novembre 2020, en ligne : <https://www.lemonde.fr/economie/article/2020/11/23/l-omc-s-inquiete-du-protectionnisme-numerique_6060808_3234.html>.

question de la circulation des données comme composante essentielle du commerce électronique semble intacte.

La volonté politique de l'OMC pour la libre circulation

Cette volonté de placer l'OMC au cœur de la dérégulation du commerce électronique a pris une nouvelle dimension en 2015. Devant la suspension des négociations du cycle de Doha en 2006 qui paralyse les discussions sur la libéralisation du commerce international et l'absence d'avancée du programme de travail sur le commerce électronique, la conférence ministérielle de Nairobi en 2015 est marquée par la volonté de certains États de se détacher des travaux du cycle de Doha et de repartir sur de nouvelles bases en explorant de nouvelles approches.[373] À cet égard, les ministres reconnaissent dans la déclaration de fin de session que : « D'autres Membres ne réaffirment pas les mandats de Doha, car ils estiment que de nouvelles approches sont nécessaires pour obtenir des résultats significatifs dans les négociations multilatérales ».[374] Un an plus tard en 2016, un atelier sur le commerce électronique est tenu à l'OMC par le groupe MIKTA[375], ce dernier étudiant notamment la question des flux et de la localisation des données.[376] En 2017, les initiatives politiques s'intensifient. Un groupe de pays appelé *Friends of e-commerce for development*, tient une réunion sur l'avenir du *e-commerce* et soulève sept questions principales, qu'il juge nécessaire d'intégrer dans les travaux de l'OMC, parmi lesquels on retrouve l'accès aux infrastructures et aux services de TIC ou encore la sécurité juridique et les cadres règlementaires concernant le commerce électronique.[377] Sur la base de discussions concernant le programme de travail sur le commerce électronique (et relatif notamment aux flux et à la protection des données)[378], et à l'initiative des États-Unis, du Japon et de l'UE, à la onzième conférence ministérielle de Buenos Aires, 71 pays produisent une déclaration conjointe. Elle prendra en réalité la forme d'une initiative plurilatérale conjointe. Dans cette déclaration, ils annoncent engager des travaux exploratoires sur le commerce

[373] Yasmin ISMAIL, *Le commerce électronique au sein de l'Organisation mondiale du commerce : Historique et dernières avancées des négociations dans le cadre de la déclaration conjointe*, Winnipeg, International Institute for Sustainable Development, 2020, p. 12.
[374] *Déclaration ministérielle de Nairobi WT/MIN (15)/W/33/Rev.3*, Genève, Organisation mondiale du commerce, 2015, en ligne : <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=r:/WT/MIN15/W33R3.pdf&Open=True> §30 .
[375] Composé du Mexique, de l'Indonésie, de la Corée du Sud, de la Turquie et de l'Australie.
[376] Y. ISMAIL, préc., note 373, p. 13.
[377] *Id.*
[378] *Id.*

électronique en vue de négociations futures,[379] ainsi que la création d'un groupe de travail[380] ; on ne sait pas si ce groupe est créé en marge ou bien adoubé par l'OMC. Toujours est-il que les discussions relatives à ce groupe se font sous l'égide de l'organisation internationale. Trois camps se distinguent alors :

- Les États et entités favorables au commerce électronique dérégulé (États-Unis, Union européenne)

- Les États opposés à ces négociations (Inde, Afrique du Sud) ; ces derniers craignant que l'on se détourne des problèmes soulevés lors des cycles de Doha tout en leur imposant des contraintes spécifiques en matière de commerce électronique,[381]

- Les États favorables, mais prudents sur le contenu (Thaïlande, Bangladesh, Chine).[382]

Des réunions régulières entre les États signataires de l'initiative ont suivi en 2018 et les nombreuses questions soulevées incluaient notamment la protection de la vie privée, la localisation de données[383] et autant de points que l'on retrouve dans les *digital dozen,*[384] qui permettent aux États-Unis d'assurer une circulation des données fluide au niveau international afin de favoriser leurs champions du numérique. Cependant, l'initiative comprenant des pays en voie de développement, on retrouve également des questions relatives à leurs intérêts.[385]

Cette initiative accueillant de nouveaux membres et les discussions ayant eu lieu entre 2017 et 2019 seront confirmées lors du forum de Davos en 2019, dans une déclaration conjointe par

[379] *Déclaration conjointe sur le commerce électronique WT/MIN (17)/60*, Genève, Organisation mondiale du commerce, 2017, en ligne : <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=r:/WT/MIN17/60.pdf&Open=True>.
[380] *Programme de travail sur le commerce électronique WT/MIN (17)/15/Rev.1*, Genève, Organisation mondiale du commerce, 2017.
[381] Y. ISMAIL, préc., note 373, p. 13.
[382] C. LETERME, préc., note 360.
[383] Y. ISMAIL, préc., note 373, p. 16.
[384] Les *Digital Dozen* sont une liste de 12 principes qui a gouverné la politique numérique de l'administration Obama. Ces principes ont officiellement pour but de protéger l'innovation, de conserver un internet libre et ouvert et de maintenir un commerce sans barrière. Pour en savoir plus, voir : U.S. GOV., « The Digital Dozen », *ustr.gov*, en ligne : <https://ustr.gov/sites/default/files/USTR-The_Digital_Dozen.pdf>.
[385] Y. ISMAIL, préc., note 373, p. 16.

laquelle les partenaires entendent lancer les négociations.[386] Ce n'est pas moins de 6 rondes de négociations qui se sont déroulées au cours de l'année 2019, autour de quinze thèmes différents, dont les flux d'informations et la protection des données personnelles.[387] En matière de protection des données, la direction qui semble être privilégiée est celle de l'adoption et du maintien de cadres règlementaires harmonisés par les États.[388] Pour des raisons de confiance envers le commerce électronique, il est alors question de mettre en œuvre des cadres de protection des données harmonisés et respectueux des règles en matière de commerce international. Les pistes de réflexion sont notamment l'harmonisation des termes employés et des définitions de ces termes : par exemple les différences de sens, entre « donnée » et « information » personnelles.[389] De la même façon, les parties se sont interrogées sur l'utilisation d'un langage contraignant versus un langage non contraignant[390] : pour résumer, doit-on contraindre ou inciter ? On comprend que ces mesures devraient permettre à terme de fonder la libre circulation des données personnelles sur la base de mesures de protection équivalentes entre les États. Ces équivalences se traduisant par des standards de protection internationaux sont la piste la plus probable afin de légitimer les transferts à l'avenir. Cependant, certaines questions relatives aux flux transfrontières agitent encore les débats. Il s'agit notamment des questions de localisation pour lesquelles les États n'arrivent pas à un consensus.[391] Notamment, les négociations semblent particulièrement houleuses entre les États-Unis, la Chine et l'Union européenne sur ces questions de flux transfrontières et de localisation des données. Les négociations sont également mouvementées, concernant les questions de vie privée qui pourrait affecter les objectifs de libre circulation des données.[392] Sur les questions de vie privée, la Chine et l'Union européenne semblent faire front commun contre les États-Unis en militant pour un cadre règlementaire imposant un « haut » degré de protection des données personnelles,[393] bien que les deux entités défendent des intérêts assez différents, l'UE centrant son argumentaire sur des questions de droits des personnes alors que la Chine joue sur le volet de la sécurité.[394] Concernant

[386] Cédric LETERME, *Quelle régulation mondiale pour l'économie des données ? Le « commerce électronique » dans les nouveaux accords commerciaux internationaux*, Conférence, Laboratoire de Cyberjustice, Montréal, 6 avril 2021.
[387] Y. ISMAIL, préc., note 373, p. 17.
[388] *Id.*, p. 20.
[389] *Id.*
[390] *Id.*
[391] *Id.*, p. 19.
[392] *Id.*, p. 28.
[393] Gary Clyde HUFBAUER et Lu ZHIYAO, *Global E-Commerce Talks Stumble on Data Issues, Privacy, and More*, Policy Brief, 19-14, Washington, D.C., Peterson Institute for International Economics, 2019, p. 6.
[394] *Id.*

la circulation des données de toute nature, c'est la Chine qui doit faire face aux États-Unis et aux Européens qui prônent tous deux, un principe de libre circulation.

De premiers résultats sont attendus pour la douzième conférence ministérielle de l'OMC qui devait initialement se tenir au Kazakhstan et qui a été reportée à cause de la pandémie de Covid-19.[395] Quoi qu'il en soit, il existe une volonté forte de la part de certains États de replacer la question de la libre circulation des données, y compris personnelles dans les mains de l'OMC. Est notamment recherché un cadre règlementaire plus clair et plus adapté que les règles actuellement en vigueur qui revêtent une portée très générale. L'OMC dispose déjà de règles pouvant court-circuiter les tentatives législatives étatiques de protection des données, surtout en ce qui concerne les pays en voie de développement. Ces dispositions permettent surtout de le faire par le biais d'accords de libre-échange, transposant en leur sein les doctrines libérales de l'organisation. La prochaine étape est par conséquent, l'adoption d'un cadre règlementaire global où l'on scellerait définitivement dans le marbre le caractère commercial de la donnée et son corollaire que représente le principe de libre circulation.

Ainsi, après une dizaine d'années régies par un principe de protection des données comme fin, protection assurée par les États eux-mêmes, on assiste depuis les années 1980 à une libéralisation du droit des données, du fait notamment de l'émergence d'un droit international des données. En conséquence, la liberté sur les flux transfrontières de données a été consacrée sans que les États ne puissent/veuillent la remettre en cause. L'apogée de cette libre circulation se traduit par la volonté de placer la protection des données sous la coupe du droit international commercial. On aura vu que c'est une bataille idéologique menée sur le plan juridique et sur le plan économique qui est à la base des politiques libérales en matière de flux transfrontières de données.

Or, la libre circulation n'a pas que des effets positifs, c'est le moins que l'on puisse dire. Que ce soit la régression de la protection des données au sein des États ou bien les conséquences néfastes de ce que l'on appelle capitalisme de surveillance, c'est autant de raisons militant pour la remise au centre des débats de la notion de protection de la vie privée telle que conçue et appliquée en Europe dans les années 1970 et la sortie de la libre circulation à outrance sous l'égide de « l'axiologie du droit du commerce international ».

[395] Elle se tiendra en juin 2022 au siège de l'organisation à Genève.

Partie 3 : Les effets délétères de la libre circulation internationale des données sur la protection des données personnelles

Jusqu'ici, nous avons eu l'occasion de démontrer comment le droit des données personnelles à des fins de protection a cédé sa place au principe de la libre circulation des données internationale. De nombreux facteurs ont contribué à ce basculement, au premier rang desquels figure, l'avènement de l'économie néo-libérale et la victoire de la doctrine de *privacy* américaine, conditionnant la protection des données personnelles à l'existence d'un dommage et des outils de droit international public venant consacrer le principe de libre circulation de manière internationale. Cette conjoncture a entraîné des réactions étatiques en faveur de la libre circulation matérialisées par des cadres juridiques adaptés. Ces cadres juridiques sont notamment le fruit d'une domination du droit du commerce international et du traitement des questions de données personnelles sous l'égide de ce dernier. Cela se matérialise par des règles contraignantes pour l'État au niveau de l'OMC et par un principe de libre circulation sanctifié jusque dans les accords de libre-échange. Plus, qu'une simple contrainte, nous allons maintenant observer plus en détail l'hégémonie du droit du commerce international sur les questions de données personnelles et l'abaissement des objectifs de protection des données qui en découlent au niveau des États (Chapitre 1). Puis, nous nous attarderons sur les dérives de l'exploitation des données que la libre circulation à outrance des données a induites, pour finalement proposer modestement des pistes pour enrayer le principe de libre circulation international des données (Chapitre 2).

Chapitre 1 : La consécration internationale du principe de libre circulation à des fins commerciales : vers une régression de la protection des données au sein des États ?

Nous l'avons abordé, les cadres juridiques dans les ordres internes, qu'ils s'agissent du Canada ou bien de l'Union européenne, ne font que retranscrire l'idée d'une protection des données au service de la libre circulation. C'est d'autant plus le cas, depuis que les outils de droit international public, contraignant les États, se constituent sous l'égide du droit du commerce international. On pense à ce titre aux accords de commerce international et aux règles de l'OMC. À côté de ça, les règles internationales *ad hoc* comme les *Lignes directrices de l'OCDE* et la *Convention 108* sont loin de prendre la tangente. Au contraire, elles sont venues adouber les politiques résolument libérales de l'époque et n'ont jamais servi à empêcher la convergence entre droit des données et commerce international, puis la domination du dernier sur le premier. Le commerce est devenu l'élément central du droit des données personnelles, tant et si bien que l'on assiste à l'appréhension sous l'égide du droit du commerce international, des problématiques de droit des données, ce qui conduit *ipso facto* à une logique du législateur-scribe[396] (Section 1). On verra ensuite que cette appréhension a dans les faits entraîné un abaissement des objectifs de protection au sein du droit des États (Section 2).

Section 1 : L'appréhension du droit des données par le droit du commerce international et la logique du législateur-scribe

De plus en plus, l'appréhension du droit des données par le droit du commerce international se traduit par des initiatives *ad hoc* au sein des partenariats économiques, régionaux notamment. Cela concourt à ce que l'on pourrait qualifier de logique de législateur-scribe, c'est-à-dire, des États qui viennent adouber la norme réglementant les données et qui émanent directement d'organisations régionales de coopération économique. Ainsi, l'influence du droit commercial se retrouve à tous les niveaux. En ce sens, nous considérons que cela participe à l'hégémonie du droit du commerce international sur la protection des données.

[396] *Intra*, p. 117.

Les initiatives ad hoc en droit des données au sein des partenariats économiques régionaux : le parachèvement de l'hégémonie du droit du commerce international

Il n'existe pas, à ce jour, de règlementation mondiale, de cadre normatif mondial ou encore d'institution mondiale de droit public, spécifique en droit des données personnelles. À notre sens, l'inexistence d'un cadre normatif international spécifique au droit des données personnelles à des fins de protection, est symptomatique de la deuxième partie de l'« axiologie du droit du commerce international », à savoir que les règles supraétatiques en droit des données ont été happées par les règles de droit du commerce international ; la première partie du problème étant la dépossession de la capacité et l'absence de volonté des États à rétablir un droit des données personnelles protecteur faisant fi des considérations économiques. Nous l'avons vu dans la première partie, la tendance à libéraliser les flux de données est apparue avec les premiers instruments juridiques internationaux sur le sujet. Nous avons illustré notre propos avec les *Lignes directrices de l'OCDE* et la *Convention 108* du Conseil de l'Europe pour démontrer comment le glissement d'un droit des données personnelles protecteur vers un droit des données personnelles libéral s'est opéré. Au moment de l'émergence de la nouvelle économie dans les années 1990, nous avons pu constater que cette harmonisation libérale s'est faite au fur et à mesure sous l'égide du droit du commerce international. À ce titre, on aura pu constater que la théorie de l'« axiologie du droit commercial international »[397] trouve également à s'appliquer en matière de droit des données.

En une vingtaine d'années, au gré des développements technologiques concomitants aux thèses néolibérales de l'époque, les différents instruments internationaux successifs, traitant du droit des données personnelles ont d'abord vanté une libre circulation des données internationale comme vecteur d'une croissance vertueuse, puis instauré un droit des données personnelles au service d'une commercialisation des données vue comme le moteur principal de l'économie actuelle. Pour autant, ils n'ont jamais vraiment participé à une cohérence juridique internationale en la matière. La raison est triple. Premièrement, les règlementations internationales *ad hoc* de protection des données sont régionalement fragmentées. Deuxièmement, les règles de protection

[397] Comme expliqué à la page 99, l'axiologie du droit commercial international renvoie en substance à la supériorité des règles internationales de commerce sur le droit interne des États, mais également sur d'autres règles de droit supraétatiques des droits de la personne ou de l'environnement. Voir, K. BENYEKHLEF, préc., note 366, p. 304.

sont pour la plupart non contraignantes, car au service de la libre circulation. Troisièmement, ces règlementations *ad hoc* sont régies par des organisations régionales de libre-échange et de coopération économiques. À ce sujet, il convient de dire quelques mots pour compléter le panorama de la consécration internationale de la libre circulation des données personnelles sous l'égide du droit du commerce international.

Les règles internationales qui nous intéressent, sont celles dont l'objet principal est le droit des données personnelles, mais qui émanent d'organisations de coopération économique. En effet, outre les premiers outils internationaux *ad hoc* en droit des données, émanant de l'OCDE (organisation de coopération économique et de libre-échange au demeurant) et du Conseil de l'Europe, il existe des initiatives plus récentes concernant la réglementation des flux externes de données. Ces initiatives sont régionales et émanent de partenariats économiques, de zones d'échanges. On abordera successivement les principes de vie privée de l'APEC (Asia-Pacific Economic Cooperation) et les règles de protections des données de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO).

- Le modèle libéral de l'*Asia-Pacific Economic Cooperation*

Le cadre pour la vie privée de l'APEC a vu le jour en 2005 et provient d'une initiative d'un groupe de travail créé au sein de l'organisation en 2003, chargé de se pencher sur les questions de vie privée, soulevées dans le cadre des échanges économiques entre les pays de l'APEC.[398] Ces principes de vie privée ont largement été influencés par les *Lignes directrices de l'OCDE* de 1981.[399] Ces principes sont non contraignants et ne nécessitent pas de ratification de la part des États partis à l'organisation.[400] Les principes de vie privée de l'APEC ont été mis à jour en 2015 en vue de l'adoption du *RGPD*. Parmi, ces principes, on retrouve les grands axes du droit des données personnelles, à savoir, la transparence, par un mécanisme de notification, la limitation de la collecte de données, des limitations quant à l'utilisation des données, le consentement libre et éclairé de la personne concernée, la sauvegarde, l'intégrité des données, ainsi que des garanties de

[398] Ellyce R. COOPER, Alan Charles RAUL et Sheri PORATH, « The Privacy, Data Protection and Cybersecurity Law Review: APEC Overview », *www.thelawreviews.co.uk*, 26 octobre 2021, en ligne : <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/apec-overview> (consulté le 9 mai 2022).
[399] *Id.*
[400] *Id.*

sécurité à la charge du responsable de traitement.[401] On retrouve également certains droits d'accès et de corrections et un principe de responsabilité des responsables de traitements,[402] à la manière de ce que l'on peut observer dans le *RGPD*.

Pour ce qui intéresse les flux transfrontières de données, il y a un système spécialement prévu, sous le nom de « *Cross-border Privacy Rules System* » (CBPR). En substance, il s'agit de lier les différentes règles en vigueur dans les pays de l'organisation afin d'assurer la fluidité des transferts par une « harmonisation » des règles étatiques. Pour être éligibles à ce programme et permettre à ces acteurs économiques de transférer des données sous l'égide de ce système, les États doivent montrer patte blanche sur un certain nombre d'aspects[403] qui ne semblent pas non plus fabuleusement contraignants. À la manière d'un « *Privacy Shield* », les organisations sont tenues pour transférer des données d'un pays à un autre de l'APEC, de mettre en place des politiques de protection et de respecter des bonnes pratiques. Ces organisations se retrouvent alors certifiées par un mécanisme de vérification effectuée par des agents de responsabilité (*accountability agent*), qui proviennent du secteur privé et dont la mission est de contrôler si l'organisation respecte les standards du système CBPR.[404] Enfin, une instance, le secrétariat CBPR, chapeaute l'intégralité du dispositif. Pour ce qui est du système CBPR, tout se fait sur la base du volontariat et les pays qui ont un degré de protection supérieur en matière de protection de la vie privée conserve ce niveau sans devoir y renoncer au nom des règles du CBPR.

Par rapport à tout ce qui existe et a pu exister en matière de réglementation des flux transfrontières, il est clair que les principes de vie privée de l'APEC et le mécanisme de régulation des flux transfrontières, sur la base de ces principes, ne réinventent pas la roue. En réalité, nous sommes comme toujours dans une optique d'optimisation de la libre circulation des données pour nourrir des intérêts économiques, en se fondant sur les principes consacrés par l'OMC. Au surplus, il ne faut pas oublier le caractère non contraignant des principes de vie privée de l'APEC, et le fait que le système du CBPR n'est pas non plus obligatoire. Les organisations peuvent très bien s'en passer pour transférer des données d'un pays à un autre. C'est un mécanisme de certification facultatif, qui servirait plutôt de vitrine commerciale, tout au mieux. L'avantage d'un tel modèle,

[401] *Id.*
[402] *Id.*
[403] *Id.*
[404] *Id.*

c'est que les États les mieux protégés semblent garder la main mise sur les questions de réglementations. Le désavantage, c'est que les pays qui ne sont pas dotés d'un tel droit en la matière ne sont qu'encouragés à le faire pour des intérêts économiques, ce qui n'a pas pour objectif de tirer le niveau de protection vers le haut. Intéressons-nous maintenant au modèle africain qui fait plutôt vieille école en comparaison aux règles de l'APEC.

- Le modèle de la *Communauté économique des États de l'Afrique de l'Ouest* : l'exception en matière de règlementation des données en droit du commerce international

Sous la forme d'un acte additionnel de la 37e session de la conférence de la CEDEAO, des règles sur la protection des données dans cet espace économique ont été adoptées en 2010. Cet acte additionnel a une force obligatoire et contraignante pour les États membres puisque, comme en dispose son article 48, il est annexé au traité de la CEDEAO, duquel il fait partie intégrante.[405] Ce texte est assez proche de ce que l'on peut trouver dans les textes européens, en ce qui se rapporte à la forme et à la structure. L'article 1 dévoile une longue liste de définitions, tandis que les articles suivants s'attellent à en délimiter l'objet et le champ d'application.[406] Dans la teneur, la lecture du texte nous fait l'effet d'un bond dans le passé. On y retrouve un système déclaratif des traitements de données personnels, devant remplir des formalités plutôt contraignantes comme en atteste l'article 7 qui énumère une longue liste d'éléments à mentionner allant de l'identité du responsable de traitement jusqu'aux politiques prévues pour assurer la sécurité des données personnelles traitées.[407] On retrouve ici aussi les principes habituels de protection, d'influence européenne, pré-*RGPD*. En ce qui concerne les flux internationaux de données, la position pour ce qui est du transfert de données personnelles vers un pays non membre est beaucoup plus tranchée qu'elle ne l'a jamais été en Europe. À ce titre, l'article 36 dispose que :

> « 1) Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un pays non membre de la CEDEAO, que si cet État assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet. 2) Avant tout transfert des

[405] *Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO*, 16 février 2010, en ligne : <https://www.afapdp.org/wp-content/uploads/2018/06/CEDEAO-Acte-2010-01-protection-des-donnees.pdf>, art 48.
[406] *Id.*
[407] *Id.*

données à caractère personnel vers ce pays tiers, le responsable de traitement doit préalablement informer l'autorité de protection. »[408]

Le constat est clair. En dehors du niveau de protection équivalent assuré par le droit d'un État non membre, il n'y a pas d'exception. Et que l'on soit en présence de flux internes ou de flux externes, le système déclaratif subsiste. Pour rappel, l'Europe des années 1990 avait déjà dans la directive de 1995, prévu beaucoup d'exceptions afin d'assurer les transferts en dehors de l'Union européenne. Ce texte africain relativement récent contraste alors avec la *doxa* occidentale en place depuis les années 1980.

Ce qui est intéressant avec ce texte est qu'il semble constituer une réminiscence de ce qui a pu exister dans le passé et rappelle étrangement les politiques strictes sur la protection des données personnelles dans la réglementation des flux transfrontières de données des années 1970, que nous avons pu étudier. Évidemment, le texte date de 2010, mais il est tout de même encore en vigueur. Une étude plus approfondie sur son fonctionnement, son efficacité et ses résultats serait intéressante, et pourrait constituer un point d'ancrage pour un retour à plus de protection au détriment de la libre circulation.

Cependant, l'émergence de plusieurs standards *ad hoc* en droit des données, émanant de zones d'échanges et de partenariats économiques démontrent encore davantage comment le droit du commerce international s'est globalement emparé des questions des droit des données.

La recrudescence d'outils juridiques internationaux en droit des données et la logique de l'État-scribe

Avant d'aborder les conséquences néfastes de l'exploitation à outrance des données personnelles, il convient tout de même de dresser un constat. Depuis les années 1980 et le développement des premiers outils internationaux en droit des données, on a assisté à une explosion de l'utilisation de ces cadres juridiques. Aujourd'hui, un grand nombre d'États, à commencer par les États membres de l'Union européenne, ne font que transposer des règles en matière de droit des données personnelles, émanant d'institutions internationales, ou bien de traités régionaux et autres traités bilatéraux relatifs au commerce. Les règles en droit des données des États européens ne sont guère plus que l'application des dispositions du *RGPD*. Les règles de l'APEC, bien qu'elles ne

[408] *Id.*

soient pas contraignantes, doivent servir de cadre à la rédaction de lois sur la protection des données personnelles dans les États membres qui n'en sont encore pas dotées. L'Acte additionnel sur la protection des données de la CEDEAO revêt une force obligatoire et a dû, à ce titre, être transposé dans le droit des États membres. Plus largement, les règles de l'OMC fixent la limite à ne pas dépasser en ce qui concerne ce que les États peuvent faire ou ne pas faire en matière de transferts internationaux de données, ce qui vient soutenir la thèse de la prédominance du droit du commerce international sur le droit des données. Dès lors, comment peut-on légitimement penser que les États assureraient la protection bec et ongles, des données de leurs ressortissants, lorsqu'ils ne font qu'appliquer des règles supra-étatiques qui prônent (à l'exception du modèle africain peut-être, ainsi que des accords de nouvelle génération de l'UE), une libre circulation quasi sans limites.

On est ici dans la logique du législateur scribe, expression de Lê-My Duong, empruntée par Boris Barraud pour expliquer comment en droit de l'internet, les législateurs ne sont plus cantonnés qu'à un rôle de transcription formelle de recommandations et de propositions provenant de sources informelles.[409] On peut appliquer le même raisonnement pour ce qui est des règles internationales de protection des données applicables aux États, qui se doivent de les transposer en ayant de moins en moins de marge de manœuvre. Comme certains diraient que : « ce sont les acteurs concernés qui font la loi »,[410] il convient ici de dire que ce sont les instances protégeant les acteurs concernés et portant leurs voix, qui font la loi. D'aucuns expliqueront cependant que c'est la raison même du droit international public, de fixer un cadre juridique international s'appliquant aux États. Nous pensons que régir les relations entre les États et contraindre les États de légiférer d'une certaine façon pour assurer que le commerce international, au service d'acteurs privés n'en soit pas altéré, sont deux enjeux différents.

L'hégémonie du droit commercial international sur la protection des données

Les États sont alors liés par des contraintes internationales qui, paradoxalement, les empêchent de contraindre. La répercussion des règles de droit international sur le droit interne des données des États eux-mêmes est tangible. On l'a vu, que ce soit dans les accords de libre-échange,

[409] Boris BARRAUD, *Repenser la pyramide des normes à l'ère des réseaux : pour une conception pragmatique du droit*, coll. logiques juridiques, L'Harmattan, 2013, p. 205.
[410] François OST et Michel VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, coll. Droit, Bruxelles, Facultés Universitaires Saint-Louis Bruxelles — F.U.S.L., 2010, p. 111.

dans les instruments conventionnels d'entités internationales, on pense à l'OMC ou mêmes à l'Union européenne, l'étau se resserre sur la protection des données. Si les mesures visant à assurer la pérennité des flux internationaux de données ne concernent théoriquement que ces flux internationaux, il ne faut pas négliger les effets délétères de ces mesures sur les législations étatiques de protection de données.

Quand nous parlons de protection des données au service de la libre circulation, nous ne sommes ni plus ni moins dans une logique d'assujettissement de la chose publique à l'utilité privée décrite si justement par Alain Supiot dans *la gouvernance par les nombres*,[411] lorsqu'il aborde le dépassement de l'État. Il s'agit de faire des règles de protection des données, une force qui va accompagner le marché et non le restreindre. Le constat que l'on adresse dans le domaine de la protection des données personnelles s'inscrit dans un panorama plus global, comme nous avons déjà pu le mentionner.[412] Les thèses économiques néolibérales développées dans les années 1970 soutiennent que les forces du marché entraînent naturellement un « ordre spontané » qu'elles seules sont capables d'apporter.[413] Là où la logique d'après-guerre à la fin des années 1940 était « d'assujettir les échanges économiques à la réalisation des droits sociaux », nécessitant « la réhabilitation du rôle des États »[414], la tendance actuelle est largement inversée. Depuis les années 1980 et les premières mesures supranationales en matière de droit des données personnelles, on assiste à un délitement de la capacité de l'État à protéger efficacement les données personnelles et la vie privée de ses ressortissants. Plus que jamais, placer les droits sociaux au service de l'activité économique entraîne des inégalités et des fractures dans nos sociétés et des discriminations entre les individus eux-mêmes. Comme nous le verrons dans le chapitre suivant, un contrôle algorithmique basé sur une masse de données personnelles est désormais rendu possible. Les grandes plateformes et même les États abusent largement de la position dominante qu'elles détiennent en la matière. Que l'on soit dans le cas de la discrimination entre les utilisateurs du fait de leur bonne ou mauvaise notation, mise en exergue par la plateforme Uber, jusqu'au système de crédit social chinois, on se base sur une surveillance massive des individus pour prendre des décisions automatisées à leur endroit.

[411] Alain SUPIOT, *La gouvernance par les nombres*, Fayard, coll. Pluriel, Paris, 2020, p. 379.
[412] *Supra*, p. 105.
[413] A. SUPIOT, préc., note 411, p. 387.
[414] *Id.* p. 387.

L'évolution du droit des données personnelles dans les trente dernières années n'a pas su prévenir les dérives que l'on connaît aujourd'hui. Dans une logique néolibérale désormais protégée par l'OMC, on s'est contenté dans nos démocraties occidentales d'ouvrir les vannes de flux de données personnelles de manière libre et sans grande contrainte. De l'abandon de la conception de la vie privée à l'européenne jusqu'à la consécration d'une libre circulation internationale des données à laquelle les États ne peuvent apporter que très peu de restrictions, on doit constater un droit de la protection des données personnelles qui se limite à ce que les conventions internationales, surtout en matière de commerce, autorisent et n'autorisent pas. Néanmoins, les projets européens de traité de libre-échange[415] peuvent donner un peu d'espoir en faveur d'un cadre normatif plus contraignant. Il en est de même du texte de la CEDEAO que nous avons présenté. On est cependant en droit de craindre que ce soit la même idéologie de l'assujettissement de la chose publique à l'utilité privée, qui régit la rédaction de ces textes, et non une prise de conscience soudaine de l'importance de la protection sociopolitique que devrait revêtir la protection des données.

Que faire par conséquent, si ce n'est tirer un constat d'impuissance du droit des données personnelles à protéger efficacement la vie privée des individus, lorsque la compétence est mise pour partie hors de portée des États et qu'elle est bien souvent traitée internationalement sous l'égide du droit du commerce ? Plus encore, y a-t-il une réelle volonté des États de récupérer une telle compétence et de défendre un droit fondamental comme celui à la vie privée, lorsque ce sont les mêmes idéologies de prééminence du marché qui gouvernent les politiques étatiques dans les États démocratiques occidentaux ? Le serpent se mord la queue : l'abandon étatique palpable de la protection des données comme un droit fondamental et éminemment sociopolitique, au profit du droit international et des considérations économiques, ne fait qu'entraîner plus de règles internationales sanctifiant la libre circulation des données au détriment de la protection des individus. Pour autant, un cadre normatif en droit international des données n'existe pas et n'est pas souhaitable,[416] puisque c'est sous l'égide du droit du commerce international que ces questions sont réglées. Par conséquent, une remise en cause du système actuel ne serait pas à l'ordre du jour.

[415] Nous faisons ici référence aux nouvelles moutures de traités européens dont nous avons fait état dans la deuxième partie. *Supra*, p. 87.
[416] *Infra*, p. 146.

Pour autant, tous ces éléments contribuent à abaisser les objectifs de protection des données en droit domestiques.

Section 2 : L'abaissement des objectifs de protection des données en droit domestique

Cet abaissement des objectifs de protection des données en droit domestique se traduit tout d'abord par un constat de cet abaissement dans les textes de lois récents. Il se traduit ensuite par une tendance vérifiable quant aux effets. À cet égard, nous étudierons le cas de la France comme illustration de notre propos.

Le constat de l'abaissement des objectifs de protection dans les textes de lois récents

La consécration du principe de la libre circulation internationale des données par des instances internationales ou bien au sein d'outils juridiques internationaux a forcément entraîné des conséquences sur le droit des données personnelles des États et des effets tangibles. Le degré de protection accordé par le droit des données personnelles des États s'arrête désormais là où la libre circulation internationale des données commence. Il est plus aisé de mesurer cet effet dans des États qui s'étaient déjà dotés de réglementation de protection avant que ces questions ne soient autant règlementées sur la scène internationale. Au Canada, on a très clairement observé cette tendance avec le *projet de loi C-11* qui deviendrait la *Loi sur la protection de la vie privée des consommateurs* et qui abrogerait au moins pour partie la *Loi sur la protection des renseignements personnels et les documents électroniques,* à savoir la première partie sur la protection des renseignements personnels dans le secteur privé. Ainsi, doit-on comprendre par ce changement de sémantique que tout ce qui touche au secteur privé est par définition commercial ? Ce que l'on sait pour sûr, c'est que l'objectif de cette loi est bien de viser : « à faciliter et à promouvoir le commerce électronique au moyen de la protection des renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales ».[417] On considérera l'objectif comme rempli puisque la collecte, l'exploitation est la communication des données ne peut se faire qu'à des fins acceptables, aux éléments de caractérisation flous, permettant peu ou prou de laisser à la discrétion de l'entreprise « responsable des données » ce qu'elle considère comme étant « acceptable ». Une fois n'est pas coutume, ce n'est qu'après les scandales que l'on ramassera les pots cassés,

[417] *Projet de loi C-11*, préc., note 232.

conséquence directe de la consécration de la doctrine de *privacy* à l'américaine appréhendée par le truchement des *torts*.[418] Les limites à la collecte sont également floues et criblées d'exceptions, tout comme le « principe » de consentement qui souffre de pas moins de cinq catégories d'exceptions au sein desquelles s'énumèrent 47 exceptions différentes, pour passer outre le consentement de la personne concernée[419] : cela fait beaucoup pour soutenir que le consentement de la personne reste le principe. Mais que l'opinion publique soit rassurée : le projet de loi prévoit que l'organisation doit prendre des mesures de sécurité pour assurer la protection des données, plus de transparence et un droit d'accès et de rectification pour les individus concernés. Les données sont sauves et avec elles, la vie privée des individus… jusqu'au prochain incident.

Mais le nouveau projet de loi canadien n'est pas un cas isolé. Dans une moindre mesure, les règles européennes ont également contribué à abaisser la protection des données personnelles dans les pays de l'Union. On a pu souligner que le *RGPD* se révélait finalement assez permissif en ce qui concerne les flux de données externes à l'Union européenne. À ce propos, la tendance semble se poursuivre avec le nouvel accord annoncé, entre l'Union européenne et les États-Unis pour les transferts de données, visant à remplacer le *Privacy Shield*.[420] Les inquiétudes croissent quand bien même les États-Unis clament que le prochain accord : « assurera un accès aux données proportionné et mettra en place un système de recours ».[421]

Cependant, le *RGPD* est tout aussi permissif pour ce qui est des flux internes. La raison d'être du texte est l'harmonisation du droit des États par un règlement d'application directe, afin de permettre aux données de circuler le plus librement possible, ce n'est pas un scoop de l'annoncer, ni une aberration que de soutenir une telle hypothèse. Néanmoins, nous sommes conscients que cette vision va à contre-courant d'une doctrine majoritaire qui encense les initiatives comme le *Règlement européen sur la protection des données personnelles*, puisqu'elle questionne *in fine* l'objectif de la protection des données, et par conséquent, le degré de protection apporté par la loi. On peut dégager certains aspects que la doctrine majoritaire en droit de la protection des données personnelles a salué avec l'arrivée du *RGPD*. Par exemple, ce texte semble plus adapté

---

[418] *Supra*, p. 32.
[419] *Projet de loi C-11*, préc., note 232.
[420] Alexandre PIQUARD, « Données numériques : le nouvel accord entre l'Europe et les Etats-Unis suscite des interrogations », *www.lemonde.fr* (12 avril 2022), en ligne : <https://www.lemonde.fr/economie/article/2022/04/12/donnees-numeriques-un-nouvel-accord-europe-etats-unis-suscite-des-interrogations_6121798_3234.html> (consulté le 6 juin 2022).
[421] *Id.*

aux réalités concrètes à propos de l'usage des données personnelles, de leur nature ubiquitaire et volatile, ainsi que des technologies utilisées pour les traiter et des nouveaux types de traitement qui vont de pair. À ce titre, on peut citer, par exemple, le droit de ne pas faire l'objet d'une décision automatisée.[422] Cette disposition est le parfait exemple d'une adaptation du droit à un « nouveau » contexte technologique. Cependant, bien que présentée comme une nouveauté, cette disposition existait déjà dans la loi française de 1978.[423] De la même façon, l'accent positif des observateurs est bien souvent mis sur la possibilité des individus de faire valoir leurs droits sur les données les concernant de manière plus complète. Ici, le mot « droit » doit s'entendre comme une action mise à la disposition de l'individu sur le traitement de ses données par une organisation. Il faut comprendre que les droits accordés par le *RGPD* sont calqués sur le « cycle de vie » des données. Ainsi, on a un éventail d'actions plus large et plus complet, ce qui permettrait théoriquement une amélioration de la protection des données.

À notre sens, la hausse du degré de protection des données des individus ne se retrouve que de manière assez éparse. On peut, par exemple, mentionner l'ajout d'un alinéa sur le traitement sécuritaire des données même contre le traitement illicite, non autorisé ou contre la perte de données, à l'article 5 du *RGPD*[424], qui est par ailleurs un calque de l'article 6 de la Directive de 1995. Une autre amélioration que l'on peut noter concerne la protection des données des enfants de moins de 16 ans qui n'est pas abordée par la Directive. On est finalement assez loin de la révolution en matière de protection des données personnelles, tant annoncée avant l'entrée en vigueur du texte, la faute peut-être aux campagnes de lobbying au Parlement européen des grands acteurs privés du numérique.[425] La force du texte réside surtout dans la possibilité pour un individu d'agir *a posteriori*. Deux points sont importants à ce sujet. Le premier est que les organisations doivent prévenir les autorités de contrôle en cas d'incidents et doivent au-delà d'un certain degré de gravité prévenir les individus concernés. Cela permet certes, une plus grande réactivité dans l'exercice des droits et dans les sanctions applicables à une organisation. On reste cependant dans un règlement *a posteriori* en cas de dommages. Le deuxième point important est que les individus disposent d'actions en tout temps à l'encontre des organisations traitant des données personnelles

[422] *R.G.P.D*, préc., note 265, art. 22.
[423] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, préc., note 78, art. 2.
[424] *R.G.P.D*, préc., note 265, art. 5.
[425] Romain HOUEIX, « Le lobbying de Facebook en Europe dévoilé par des mémos internes », *www.france24.com*, 4 mars 2019, en ligne : <https://www.france24.com/fr/20190304-europe-lobby-facebook-rgpd-sheryl-sandberg-memo>.

les concernant.[426] En théorie, on serait tenté de dire que c'est un progrès. Dans les faits, c'est loin d'être évident du fait de l'opacité et de l'effet « usine à gaz » des procédures de gestion des données propres à chaque organisation et du fardeau que cela suppose pour un individu.

Encore une fois, tout dépend de ce que l'on considère être comme un progrès. Nos travaux se placent résolument en faveur d'une protection des données qui soit une fin en soi et non pas un recours en cas de dommages, afin de permettre aux individus d'obtenir réparation. Dès lors, le *RGPD* ne constitue pas à notre sens, un progrès marquant en matière de protection. C'est un outil qui, tout au mieux, permet de définir les règles du jeu de la circulation des données et d'établir un régime de responsabilité. Définissant alors ce cadre de responsabilité, on comprend mieux la mise en place d'un système d'actions ouvertes aux individus à l'encontre des responsables de leurs données. Dès lors, un dommage dont l'organisation est responsable ouvre le droit à une action en réparation. Mais, ce droit à l'action en réparation ne produit pas nécessairement les effets escomptés. Nous allons maintenant constater que l'abaissement des objectifs de protection se vérifie en pratique, au travers du cas de la France.

[426] *R.G.P.D*, préc., note 265.

Une tendance vérifiable quant aux effets : le cas de la France

La tendance des quatre dernières années semble être à la hausse en ce qui concerne les plaintes reçues. C'est en tout cas ce qui transparaît dans les rapports de la CNIL puisqu'on passe de 7703 et 8360 plaintes auprès de la CNIL, pour les années 2016[427] et 2017[428] respectivement à 11077, 14137 et 13585 pour les années 2018[429], 2019[430] et 2020[431], soit après l'entrée en vigueur du *RGPD*. De plus, une étude réalisée en 2019 par le cabinet d'études de marché européen *IntoTheMinds*, sur les effets du *RGPD* après son entrée en vigueur montre une forte augmentation du nombre de plaintes avec une hausse moyenne de 86 %[432]. Cependant, cette hausse est à relativiser pour deux raisons. La première raison c'est que des pays comme la Suède ou l'Autriche culminent à 479 % et 564 % d'augmentation relative du nombre de plaintes[433], ce qui n'est pas forcément représentatif d'une tendance européenne plus globale. La deuxième raison est qu'en termes de chiffrage absolu, cela ne représente qu'une augmentation moyenne de 1899 plaintes et le taux moyen n'est que de 2.99 par 10000 habitants[434]. Il convient de mentionner que ces chiffres n'apportent que des éléments partiels de réponse, puisque pour chiffrer l'exercice par les individus concernant leurs droits, il faudrait également étudier le nombre de réclamations directement enregistrées auprès des organisations responsables du traitement des données.

Si l'on prend encore une fois le cas de la France, la hausse des plaintes s'accompagne paradoxalement d'une baisse des vérifications effectuées par la CNIL. On passe de

---

[427] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2016*, Rapport d'activité, 37, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf>.
[428] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2017*, Rapport d'activité, 38, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2018, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf>.
[429] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2018*, Rapport d'activité, 39, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2019, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-39e_rapport_annuel_2018.pdf>.
[430] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2019*, Rapport d'activité, 40, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2020, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf>.
[431] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2020*, Rapport d'activité, 41, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2021, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf>.
[432] Pierre-Nicolas SCHWAB, « Statistiques RGPD Europe : évolution du nombre de plaintes par pays », *www.intotheminds.com*, 4 mai 2020, en ligne : <https://www.intotheminds.com/blog/statistiques-rgpd-europe/> (consulté le 21 mars 2022).
[433] *Id.*
[434] *Id.*

8297 vérifications effectuées par l'autorité de protection française en 2017[435] à 3286 en 2020[436], soit une réduction de plus de la moitié de ces vérifications. De la même façon, le nombre de contrôles des organisations par le gendarme à la protection des données français est à la baisse depuis l'entrée en vigueur du *RGPD*. On passe de 341 contrôles en 2017[437] à 247 contrôles en 2020[438]. Le même constat peut être fait pour ce qui est du nombre de mises en demeure de 79 en 2017[439] et qui stagne entre 40 et 50, les années suivantes[440]. Cependant, l'année 2021 fait office d'exception avec une explosion des mises en demeure de la CNIL (135)[441]. Le nombre de sanctions reste quant à lui stable, allant de 11 à 14 par année.[442] C'est le même son de cloche du côté de l'Irlande, qui concentre les sièges européens des géants de la Tech avec environ 10000 plaintes en 2020 pour 2 sanctions.[443]

Ainsi, on constate qu'il y a une hausse des plaintes depuis l'entrée en vigueur du texte européen, mais très peu de sanctions qui suivent, corrélées à une baisse du nombre de contrôles. Ces données attestent du changement qui s'est opéré avec l'entrée en vigueur du *RGPD*. On est passé d'une logique de contrôle *a priori* à une logique de contrôle *a posteriori*[444] et d'*accountability*, reprenant la philosophie américaine du « tant qu'il n'y a pas de dommage, il n'y a pas de problèmes ». En France, la Quadrature du Net qui milite pour le droit à la protection des données personnelles déplorait l'absence de réaction de la CNIL, allant même jusqu'à qualifier l'autorité de protection de « coupable » et de « complice » dans le cadre d'une action collective contre Apple, pour laquelle selon l'organisation, la CNIL a volontairement refusé d'agir en

[435] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 428.
[436] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 431.
[437] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 428.
[438] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 431.
[439] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 428.
[440] Voir, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 429. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 430. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 431.
[441] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Journée de la protection des données : focus sur une année record pour l'action répressive de la CNIL », *https://www.cnil.fr*, 28 janvier 2022, en ligne : <https://www.cnil.fr/fr/bilan-sanctions-mises-en-demeure-2021>.
[442] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 427. ; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 428. ; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 429. ; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 430. ; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, préc., note 431.
[443] Philippe RICHARD, « RGPD : un bilan mitigé », *https://www.techniques-ingenieur.fr*, 28 mai 2021, en ligne : <https://www.techniques-ingenieur.fr/actualite/articles/rgpd-un-bilan-mitige-93755/>.
[444] *Id.*

n'utilisant pas tous les rouages du *RGPD* pour contrer une décision de la DPC irlandaise, favorable à Apple et empêchant toute condamnation.[445]

Parallèlement, certaines données montrent que la régulation par l'*accountability* a du mal à prendre. En effet, le bilan quant à la conformité des organisations au texte européen est mitigé. Dans une étude du cabinet KPMG, portant sur la mise en conformité du règlement européen par les entreprises en France, plusieurs données montrent que le niveau d'avancement n'est pas encore optimal. Seulement 39 % des entreprises estiment leurs plans d'action vers une conformité, complétés à 75-100 %.[446] La mise en place de registres de traitement est à la hausse ; en revanche les analyses d'impact relatives à la protection des données, qui sont la clé de voûte de la « co-régulation » voulue par l'Europe, est en retard.[447]

Évidemment, une étude bien plus poussée de la situation en Europe serait nécessaire et il y a clairement un manque de chiffrage sur le sujet. Seulement, existe-t-il ? Si oui, il n'est pas forcément rendu public et on peut épingler, à ce titre, le manque de transparence du Comité européen à la protection des données personnelles, qui ne publie que très peu de données sur la situation dans l'ensemble de l'Union européenne. Reste qu'avec les données disponibles, on constate que le système mis en place par le *RGPD* ne tend pas à augmenter significativement la protection des données des Européens. Ce n'est résolument pas le cas en France. Plus encore, on peut y voir des signes d'abaissement de cette protection. Cet abaissement est avant tout idéologique. Le passage d'une philosophie de vie privée à l'américaine et la logique du « tort » et la consécration de la libre circulation des données mènent *de facto* à un appauvrissement de la protection des individus. Avec le *RGPD*, les individus sont livrés à eux-mêmes. En d'autres termes, les individus peuvent agir plus et les autorités de protection agissent moins. Ainsi qu'en attestent les chiffres de la CNIL vus précédemment, les autorités sont réduites à une mission d'information et d'éducation, plutôt que de contrôle et de répression. Ne nous méprenons pas, le volet éducatif est très important, mais on ne peut raisonnablement penser que la protection de la vie privée des individus découlera de ce dernier (en tout état de cause, pas avant longtemps).

---

[445] LA QUADRATURE DU NET, « Les GAFAM échappent au RGPD, la CNIL complice », *www.laquadrature.net*, 25 mai 2021, en ligne : <https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/>.
[446] KPMG, *Baromètre RGPD, 3 ans après, où en êtes-vous ?*, Baromètre, Paris, France, KPMG, Juillet 2021, p. 23.
[447] *Id.*, p. 26.

Comme nous le soutenons, depuis les années 1980, la tendance est à l'américanisation de la vie privée et à la libre circulation des données personnelles. Le *RGPD* n'est qu'une étape supplémentaire vers la prééminence de la libre circulation des données. C'est précisément cette libre circulation pour des considérations économiques libérales, qui entraîne un recul de la protection des données personnelles comme fin en soi, dont le *RGPD* est le parfait exemple. Ainsi que le démontre la teneur des futurs textes canadiens ou bien les effets au mieux mitigés du *RGPD*, on risque d'assister dans nos pays occidentaux à un abaissement du niveau de la protection des données, ce qui peut paraître paradoxal pour des outils juridiques qualifiés de progrès. Les textes législatifs, toujours plus empreints de libéralisme et l'absence de réactions des régulateurs, font que l'on se retrouve avec des cadres normatifs non efficaces, en ce qu'ils ne répondent qu'à des atteintes *a posteriori* et qu'en plus de ça, tendent à faire reposer le poids de leur propre protection sur les individus eux-mêmes. Les objectifs de protection des données comme fin en soi sont délaissés et seul le profit que l'on peut en dégager, compte. Finalement, cette conséquence de la subtilisation des questions de protection des données personnelles, par le droit du commerce international prônant le « laisser-faire », se retrouve finalement assez bien dans les récents cadres de règlementation des données personnelles.

Évidemment, cet abaissement de la protection des données « venant d'en haut », si l'on peut dire, phagocyte la capacité des États à pouvoir légiférer en faveur des réglementations poursuivant un objectif de fin en soi concernant la protection des données personnelles et ces derniers s'en accommodent très bien. Les États ne militent que mollement contre les mesures édictées par le droit du commerce international sous l'hégémonie des règles de l'OMC. Ce qui est vrai pour le droit des données personnelles l'est également pour d'autres branches du droit au premier rang desquels figure le droit de l'environnement. Cet abaissement de la protection des données a entraîné des dérives induites par la libre circulation des données. C'est ce que nous aborderons dans le chapitre suivant, non sans proposer quelques pistes prospectives de solutions.

Chapitre 2 : Les dérives de l'exploitation des données personnelles induites par le principe de libre circulation des données et les pistes de solutions

Les dérives provenant de l'exploitation des données personnelles dans le cadre d'un marché international de la donnée, elle-même induite par la consécration de la libre circulation sont nombreuses. Elles sont tellement nombreuses, qu'il n'est pas possible de tout traiter dans le présent chapitre. Nous avons alors choisi de traiter celles qui découlent directement du principe de libre circulation qui gouverne le droit des données depuis les 40 dernières années et qui nous paraissent les plus révélatrices pour notre démonstration. Il s'agit du capitalisme de surveillance, de l'hypothèse technoféodale et des dérives de surveillance publique du fait de la libre circulation (Section 1). La section conclusive suivant la description de ces dérives aura pour objectif de proposer quelques solutions et pistes de réflexion pour casser ce principe de libre circulation et élever le niveau de protection des données (Section 2).

Section 1 : Des dérives induites par la libre circulation des données : capitalisme de surveillance, technoféodalisme et surveillance public :

Un des éléments les plus couramment cités ayant entraîné des dérives majeures et qui a fait l'objet d'une recherche approfondie ces dix dernières années est ce que l'on appelle le capitalisme de surveillance. Cette notion que nous allons détailler découle, selon nous, très largement de la tendance juridique démontrée dans notre mémoire. Cependant d'autres dérives dont les conséquences néfastes revêtant un caractère plus collectif, sont également à analyser. Il s'agit principalement des conséquences du technoféodalisme et des conséquences de la surveillance par les gouvernements provenant directement de la libre circulation des données.

La notion de capitalisme de surveillance

Le capitalisme de surveillance ou capitalisme de l'attention a surtout été médiatisé par une professeure de la Harvard Business School, qui a publié un ouvrage intitulé *l'âge du capitalisme de surveillance*. Dans sa monographie, l'auteure, Shoshana Zuboff explique comment les grandes firmes américaines de la technologie ont tiré un avantage concurrentiel sans pareil sur le marché des données en développant des algorithmes et une architecture permettant de déduire « les

pensées, les sentiments, les intentions et les intérêts des individus et des groupes ».[448] Évidemment la libre circulation des données désormais sanctifiée en droit du commerce international et les politiques libérales depuis le début des années 1980 jusqu'à nos jours auront permis à ces firmes d'acquérir des jeux de données absolument colossaux. Ces quantités de données ont rendu possible la création d'architectures, de déductions de données personnelles et de créer de nouveaux points de données à propos d'individus, qui n'auraient donné leur consentement à aucun moment. Cet « habitat néolibéral » a fortement participé à l'émergence puis l'hégémonie du capitalisme de surveillance, 30 ans plus tard.[449]

Selon l'auteure, la capacité des sociétés du numérique à maîtriser des techniques de collecte et de tri des données, mais surtout la possibilité de le faire dans un environnement largement dérégulé, a permis ces prouesses en matière de prédiction et d'incitation des comportements. Cette maîtrise des technologies et, notamment de *Big Data,* a entraîné encore davantage une logique d'accumulation de données personnelles sur les individus qui est à la racine du capitalisme de surveillance.[450] Sur cette base, c'est une véritable régie publicitaire qui s'est organisée au fil des années en exploitant les données personnelles d'individus. Dans son ouvrage, Shoshana Zuboff définit le capitalisme de surveillance comme un nouvel ordre économique qui : « revendique unilatéralement l'expérience humaine comme matière première gratuite destinée à être traduite en données comportementales. »[451] Le terme « unilatéralement » renvoie à la notion que l'auteure baptise « Big Other », en référence au « Big Brother » imaginé par George Orwell dans *1984.* En effet, la notion quasi religieuse de « Big Other » reflète « une infrastructure computationnelle ubiquitaire, sensorielle et interconnectée ».[452] Cet infernal vortex à données, enregistre, modifie, traite, uniformise toutes les informations captées par le biais de n'importe quel appareil électronique connecté.[453] Plus qu'un simple outil au fondement du capitalisme de surveillance, il

[448] Shoshana ZUBOFF, « Un capitalisme de surveillance », *https://www.monde-diplomatique.fr*, janvier 2019, en ligne : <https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443#:~:text=L%27industrie%20numérique%20prospère%20grâce,doit%20se%20changer%20en%20certitude.>.
[449] L'auteure explique dans ce paragraphe intitulé « l'habitat néolibéral », comment les thèses radicales du libre marché développées par F. Hayek et M. Friedman ont constitué un terreau fertile pour l'émergence du capitalisme de surveillance. Voir, Shoshana ZUBOFF, *L'Âge du capitalisme de surveillance*, coll. Zulma Essais, Zulma, 2020, p. 62.
[450] Shoshana ZUBOFF, « Big other: Surveillance Capitalism and the Prospects of an Information Civilization », (2015) 30 *Journal of Information Technology* 75, 77.
[451] S. ZUBOFF, préc., note 449, p. 24.
[452] *Id.*, p. 45.
[453] S. ZUBOFF, préc., note 450, 81.

est vu par son auteure comme un nouveau régime souverain, complètement indépendant et incontrôlable qui « annihilerait » la liberté rendue possible par l'État de droit.[454] Ainsi, à l'ère du capitalisme de surveillance, on a affaire à un système qui fait fi de toutes les règles relatives à la vie privée et à la protection des données personnelles, qui obéit à ses propres règles, qui agit dans l'ombre et qui est complètement opaque. La prédiction des comportements par la compilation et la création de nouveaux de points de données, devient la norme, et sur cette base, les acteurs du capitalisme de surveillance, manipulent, influencent les comportements de millions d'utilisateurs à des fins de profit économique. Ainsi, selon S. Zuboff, on se retrouverait dans une société dans laquelle l'individu *a priori* libre et autonome perdrait complètement cette liberté. À cet égard, le capitalisme de surveillance participerait d'un processus antidémocratique dans lequel un pouvoir « instrumentariste »[455] décide en lieu et place des individus pour atteindre ses propres objectifs. Dès lors, au nom du marché et du profit, les individus voient leurs libertés et leur libre arbitre bafoués de manière insidieuse. Comme nous l'avons mentionné plus haut, l'émergence du capitalisme de surveillance concourt de plusieurs facteurs, parmi lesquels se trouvent les politiques néolibérales gouvernant nos sociétés depuis le début des années 1980.

La responsabilité du principe de libre circulation internationale dans l'émergence du capitalisme de surveillance

Pourtant, à propos du capitalisme de surveillance et de ses origines, Shoshanna Zuboff en dit assez peu sur les implications du principe de libre circulation des données. Elle dépeint un portrait du néolibéralisme comme terreau fertile de ce pan récent de l'économie des données, mais n'entre pas spécifiquement dans les détails de la place du droit des données. Elle aborde simplement dans un passage intéressant, le développement des technologies logicielles dite de « cookie » et l'intense lobbyisme ayant fait échouer une règlementation fédérale sur la question dans les années 1990.[456] De manière plus éparse et superficielle, on retrouve des références à la protection des données personnelles que l'on pourrait qualifier de contemporaines, ainsi que des problématiques liées à la libre circulation sans contrainte juridique.[457] Il est pour autant beaucoup question du droit à la vie privée et de ces nombreuses incompatibilités avec le capitalisme de surveillance. Dès lors,

[454] *Id.*
[455] L'auteur définit le pouvoir instrumentariste comme : « l'instrumentation et l'instrumentalisation du comportement à des fins de modification, de prédiction, de monétisation et de contrôle ». Voir : S. ZUBOFF, préc., note 449, p. 472.
[456] *Id.*, p. 125.
[457] *Id.*, p. 318.

la question de l'évolution du droit à la vie privée et du droit des données personnelles semble avoir toute sa place dans la problématique du capitalisme de surveillance.

Comme nous l'avons abordé, la vision de la vie privée à l'européenne et de la protection des données comme une fin en soi n'a perduré qu'une petite dizaine d'années. Elle a périclité, concomitamment à la victoire des thèses économiques néolibérales prônant un marché largement dérégulé dans lequel le rôle de l'État serait cantonné à celui d'ultime recours. Cela marque un tournant à la fin des années 1970 et au début des années 1980 et la fin de l'économie d'après-guerre marquée par les thèses keynésiennes prônant un fort interventionnisme de l'État.[458] Ce changement de paradigme économique est corrélé à l'avènement du droit à la vie privée à l'américaine comme réparation d'un dommage. La *Doxa* de l'époque, guidée par l'empêchement des États de limiter les interactions économiques s'est répercutée jusque dans le droit des données personnelles. Les premières initiatives internationales dans les années 1980 auront permis aux entreprises technologiques américaines de se développer en Europe en assurant la libre circulation internationale des données personnelles. De manière générale, tout le pôle occidental signataire de ces conventions se retrouvait pieds et poings liés, par une réglementation les incitant à retirer les régimes spécifiques de protection sur les flux transfrontières de données. Bien que dans un premier temps, cela n'ait pas eu nécessairement les effets escomptés, ces règles constituaient dans les années 1990, une porte ouverte à la captation des données personnelles sur les territoires des pays les plus informatisés et au rapatriement de ces données sur le territoire américain, par des firmes, qui, du fait d'une protection contre la concurrence aux États-Unis, dominaient le marché. Les politiques de libre circulation des données personnelles et la sanctification du principe au sein du droit du commerce international ont parachevé l'hégémonie des firmes américaines de la technologie, aujourd'hui acteurs majeurs du capitalisme de surveillance. En relayant la protection des données personnelles au rang de faire-valoir de la libre circulation des flux d'informations, les deux principaux effets ont été de :

- Consacrer la vision américaine de la *privacy* ne visant qu'à réparer un dommage et de fait, bien plus conciliable avec la libre circulation des données.

[458] Pierre DARDOT et Christian LAVAL, *La nouvelle raison du monde*, coll. Poche/Sciences humaines et sociales, Paris, La Découverte, 2010, p. 273.

- Empêcher la réglementation étatique jugée trop protectrice et, par conséquent, restrictive, dans une économie de l'information où les données y sont une caractéristique primordiale.

En premier lieu, l'avènement du concept de *privacy* américaine vient légitimer tous les traitements et les transferts de données qui découlent du principe de libre circulation. En effet, il ne s'agit plus pour les organisations de respecter les règles qu'imposerait d'emblée un régime juridique de protection des données comme une fin en soi. On part du principe selon lequel, tant qu'il n'y a pas de dommage, il n'y a pas de recours. Dès lors, il faudrait, dans un premier temps, que l'individu soit au courant que ses données sont exploitées par une firme à l'autre bout du monde, que cette exploitation lui cause un dommage afin qu'il ait une voie de recours contre l'organisation qui traite ses données, et qu'enfin, il aille faire valoir ses droits devant la juridiction compétente, sans qu'il sache vraiment devant quel pays la formuler. Résumons alors : depuis le début des années 1980, le principe de libre circulation des données personnelles est consacré dans des outils juridiques internationaux de protection des données personnelles que sont les *Lignes directrices de l'OCDE* et la *Convention 108* du Conseil de l'Europe. Depuis les années 1990 en Europe, la libre circulation des données internationale est assurée par les textes communautaires sur la protection des données personnelles. Depuis les mêmes années, le principe de libre circulation des données est consacré en droit du commerce international, dans les textes fondateurs de l'OMC ainsi que dans les traités de libre-échange. Pire encore, les initiatives régionales sur la réglementation des questions de vie privée, émanent d'organisations commerciales (à l'exception de l'Afrique qui bénéficie d'un régime à l'ancienne et de projets de traités européens), qui récitent la partition de la libre circulation des données dont les seules garanties seraient des garde-fous douteux. Le concept de vie privée à l'américaine dans le cadre de la circulation internationale de données échoue à protéger efficacement les données personnelles. Plus encore, il vient protéger l'exploitation des données, puisqu'en pratique et ce jusque dans les années récentes, du fait de nombreux scandales sur le sujet, les entreprises traitant des données en masse et les grands acteurs du capitalisme de surveillance n'ont pratiquement jamais été inquiétées sur le fondement de la protection des données personnelles.

En second lieu, les objectifs de protection des données personnelles ont été revus à la baisse du fait de l'empêchement consenti de la part des États à légiférer trop strictement sur les données,

si chères et précieuses au développement économique. On a pu le constater, la lettre du texte dans les nouvelles lois de protection des données personnelles s'inscrit dans la même mouvance : libre circulation avant tout et pour ce qui est de la protection, elle est reléguée à un argument de confiance, comme on brandirait un argument marketing ; en atteste le projet de loi fédérale canadien. Le problème qui se pose est le suivant : comment protéger efficacement les données personnelles, si les textes de loi ne remplissent pas des objectifs de protection ? On ne réglemente plus les données personnelles, on réglemente leur libre circulation comme on poserait un dôme sur des pratiques déjà bien établies.

Cet échec sur le plan juridique a laissé carte blanche au développement des grandes firmes de l'internet et a participé à l'accumulation de grandes masses de données, au développement de technologies visant à trier, à recouper, à interpréter ces jeux de données et à les structurer pour faire du profit. Il ne s'agit pas de pointer cet échec comme étant l'unique responsable de phénomènes comme le capitalisme de surveillance. Il est évident qu'énormément de facteurs concourent : de l'émergence puis de l'hégémonie des firmes technologiques, sur la base de l'exploitation et du traitement de données.[459] Cependant, il ne faut pas négliger la responsabilité du changement de paradigme dans le droit de la protection des données personnelles comme constituant une pierre à l'édifice de la déconstruction du droit à la vie privée, puisque c'est finalement de ça dont il est question.[460] Dès lors, en consacrant la libre circulation des données personnelles internationale et en relayant de *facto* la protection des données en arrière-plan, le développement du capitalisme de surveillance n'a pas été entravé, mais au contraire, a été accompagné.

[459] Ces facteurs sont multiples et pluridisciplinaires. Des auteures comme S. Zuboff, C. Durand ou E. Morozov produisent des analyses exhaustives et pluridisciplinaires de ces questions.

[460] En illustration de ce propos, les mots du PDG de Meta, Mark Zuckerberg trouvent un certain écho lorsqu'il clamait en 2010 que la vie privée n'est plus une norme sociale. Voir, LE MONDE, « Pour le fondateur de Facebook, la protection de la vie privée n'est plus la norme », *www.lemonde.fr*, 11 janvier 2010, en ligne : <https://www.lemonde.fr/technologies/article/2010/01/11/pour-le-fondateur-de-facebook-la-protection-de-la-vie-privee-n-est-plus-la-norme_1289944_651865.html#:~:text=Technologies-,Pour%20le%20fondateur%20de%20Facebook%2C%20la%20protection%20de%20la%20vie,générations%20que%20pour%20leurs%20parents.&text=Lecture%201%20min.>.

Ce constat est transposable à beaucoup d'autres dérives qui sont tout aussi problématiques. Nous l'aurons vu, le capitalisme de surveillance est un mode de surveillance qui vise à faire du profit. Dans ce contexte, le principe de libre circulation des données et notamment des données personnelles trouve presque une certaine logique. En effet, notre étude démontre que le parti pris de ce principe est avant tout un parti pris économique, dans le sillage des thèses néolibérales de l'époque. Par conséquent, le capitalisme de surveillance est simplement une conséquence logique des politiques qui ont été menées depuis les années 1980. À la manière d'un *Frankenstein,* tout contrôle a été perdu sur la bête créée en partie par le fait de l'avènement d'une libre circulation des données à outrance. C'est ce qu'admet volontiers Cédric Durand lorsqu'il avance l'hypothèse du technoféodalisme.

L'hypothèse technoféodale décrite par C. Durand dans son ouvrage intitulé *Technoféodalisme* découle *ipso facto* du même terreau fertile duquel s'est élevé le phénomène du capitalisme de surveillance. De manière schématisée, les idéaux technophiles des années 1960 ont embrassé les doctrines économiques néolibérales en se basant sur les courants prônant un internet libre et ouvert.[461] En conséquence, un discours magnifié de cette nouvelle économie du numérique a émergé, revendiquant un écosystème idéal pour les entreprises voulant pénétrer le marché. Cette contextualisation temporelle de rigueur dans de nombreux ouvrages traitant des conséquences néfastes induites par l'ultralibéralisation de l'économie à l'ère d'internet est utile, en ce qu'elle permet de montrer à quel point les résultats n'ont pas été à la hauteur des promesses de l'idéologie californienne.[462] Ainsi, on s'est vite rendu compte que les start-ups étaient destinées à briller ou à s'éteindre. En ce qui concerne les géants du numérique : « les sympathiques start-up d'hier sont devenues de féroces monopoles ».[463] Cette férocité se retrouve jusque dans la gestion des travailleurs, laquelle repose sur des technologies avancées au service du contrôle de la productivité alors même que cette économie numérique n'a généré que peu de croissance.[464]

[461] C. DURAND, préc., note 198, p. 21 et suiv.
[462] *Id.*, p. 42 et suiv.
[463] *Id.*, p. 44.
[464] *Id.*, p. 55 et suiv.

Économiquement parlant, la puissance de ce système s'appuie sur des actifs intangibles dont la force est d'être consommés de manière ubiquitaire, permettant des rendements potentiellement infinis. Les rentes sur les actifs intangibles se trouvent décuplées du fait de l'accroissement du phénomène de monopolisation intellectuelle, qui permet de contrôler l'information et d'en capter la valeur. Cependant, ce phénomène se produit au détriment des acteurs dont l'activité est basée sur des actifs tangibles et qui dépendent de ces plateformes. Ainsi se fonde l'hypothèse technoféodale.[465]

Les fiefs du numérique basent notamment leur activité sur le capitalisme de surveillance et ses dérives. La réduction des comportements des individus à de simples probabilités, l'exploitation des données personnelles à des fins de prédictions des comportements des sujets est devenue l'activité principale de ces grands groupes. Dès lors, le modèle technoféodal est intimement lié au capitalisme de surveillance et à toutes les dérives que ce dernier engendre. Cependant, c'est bien plus qu'une menace pour les individus. La comparaison avec le modèle féodal du Moyen-âge est assez édifiante. Le féodalisme est un rapport de domination à la fois politique et économique et un jeu de pouvoir tant sur les hommes que sur la terre. Dans ce rapport, ce sont la contrainte et la prédation qui dominent. L'application du modèle féodal à l'économie actuelle produit un constat frappant : les grandes plateformes possèdent un vivier de données, d'informations et de connaissances, à partir duquel des entreprises développent leur activité économique en situation de dépendance vis-à-vis de ces nouveaux seigneurs. L'hypothèse technoféodale ne se borne pas à appliquer les thèses marxistes de concentration des moyens de production à l'économie du numérique, mais alerte sur l'appropriation et la capture de ces moyens de production par les GAFAM. Ces derniers sapent l'autonomie des individus pour fournir un vivier dont les acteurs économiques développant une activité dans leurs fiefs ne peuvent pas se passer.[466]

Les dérives découlant d'un modèle technoféodal fondé sur les données sont à souligner par la nature collective du danger qu'elles représentent. Dans le capitalisme de surveillance, Shoshanna Zuboff, pointe surtout des dérives pour les individus en cause. Ainsi, le principal effet négatif du capitalisme de surveillance c'est de saper l'autonomie, la liberté et le libre arbitre de l'individu en tant qu'un individu. À cet égard, le docteur en histoire des sciences Evgeny Morozov, reproche à

[465] *Id.*, p. 179 et suiv.
[466] *Id.*, p. 127 et suiv.

S. Zuboff, le manque de dimension collective dans son analyse des conséquences néfastes du capitalisme de surveillance. L'hypothèse technoféodale pointe justement des effets désastreux sur les collectivités du fait de ces fiefs fondés sur l'agrégation de données. En effet, il se crée des relations de dépendance des différentes couches du tissu économique envers les plateformes.[467] L'agrégation des données couvée par un principe de libre circulation international jamais remis en cause aura sûrement participé à l'émergence de cette nouvelle prédation remplaçant la production.[468]

Il est évident que la création de tels fiefs économiques rend désormais la tâche de la protection des données personnelles des plus ardues. En effet, la « data sphère »[469] existant par nature du fait de la libre circulation des données et l'abaissement de la protection de ces dernières, relève davantage d'une glèbe numérique[470] sur laquelle les plateformes exercent une domination sans pareil. Sur cette glèbe numérique[471] dominée par les plateformes, ces dernières se sont érigées en seigneuries. Les énormes avantages et bénéfices retirés par les plateformes de l'exploitation de cette glèbe numérique leur permettent de restituer de « puissants effets utiles ».[472] Tant et si bien que c'est un aspect collectif que revêt la domination. Les outils fournis par les plateformes sont rendus indispensables à la société. Dès lors, l'emprise n'est plus seulement cristallisée sur la capacité de la firme numérique à exercer une surveillance individuelle, mais bien de rendre indispensables les outils qu'elle fournit à une société dans son ensemble. Dès lors, les communautés d'individus s'en retrouvent dépendantes et ces dernières, matérialisées notamment par les États ne peuvent plus agir, sur les questions qui viendraient déranger les firmes numériques fournissant les services : les questions de protection des données personnelles et du maintien de la libre circulation quoiqu'il en coûte, en font partie. Un exemple récent s'en fait la parfaite illustration. Début 2022, la compagnie de Mark Zuckerberg, *Meta*, a menacé de retirer les réseaux sociaux Facebook et

[467] *Id.*, p. 227
[468] *Id.*, p. 227
[469] Thomas GOMART, *Guerres invisibles*, Tallandier, coll. Texto, Paris, p. 302.
[470] C. DURAND, préc., note 198, p. 123 et suiv.
[471] Selon C. Durand, cette glèbe numérique se fonde sur le concept de *potentia multitudinis,* notamment décrit par Frédéric Lordon. Voir, Frédéric LORDON, *Imperium, Structures et affects des corps politiques*, Paris, La Fabrique, 2015. Transposé au Big Data, les faits techniques deviennent des faits institutionnels de capture. En rétablissant une « puissance du social » augmentant l'individu (mouvement descendant), ce dernier se retrouve « capturé » du fait de la réduction de son autonomie (mouvement ascendant). Sous couvert d'un sentiment de puissance collective conféré à l'individu, les firmes numériques exercent un pouvoir sans précédent de capture et d'emprise sur les individus et les collectivités. Voir, C. DURAND, préc., note 198, p. 126.
[472] C. DURAND, préc., note 198, p. 129.

Instagram de l'Union européenne, si elle ne peut plus transférer les données des utilisateurs aux États-Unis. En effet, depuis l'annulation de l'accord *Privacy Shield*,[473] les grosses firmes américaines ont perdu un moyen de transférer de gros volumes de données à moindres coûts. Comme nous l'avons vu dans la partie précédente, le R.G.P.D, prévoit de nombreuses exceptions pour maintenir la libre circulation des données depuis l'Europe vers des pays tiers. Cette annulation fait craindre au groupe une étude plus poussée de ces exceptions, avec à la clé une entrave à la libre circulation des données produisant des effets dommageables à leur encontre.[474] En réponse à cela, la Commission européenne a annoncé l'intensification des négociations avec Washington en vue d'un nouvel accord.[475] Un nouvel accord a d'ailleurs été annoncé le 25 mars 2022 par le Président américain Joe Biden et la Présidente de la Commission européenne, Ursula von der Leyen.[476]

Dès lors, premièrement, ces dérives technoféodales sont directement liées à la consécration de libre circulation des données en droit du commerce international. Deuxièmement, les fiefs créés par les grandes entreprises du numérique prospèrent du fait du maintien du principe de libre circulation des données. Enfin, troisièmement, cette soumission collective rend très compliquée la remise en cause de ce principe et le retour à une protection des données personnelles et de la vie privée comme une fin en soi, tant les rapports de forces semblent maintenant déséquilibrés.

Les conséquences indirectes de la consécration de la libre circulation des données dans la surveillance par les gouvernements : les révélations Snowden

Quand on lie libre circulation des données à des fins commerciales et surveillance de la part de gouvernements, il faut être précautionneux et bien poser les termes du débat.

On a, d'une part, une surveillance qui résulte directement de la circulation des données entre les entités publiques, prévue par le droit des données personnelles. C'est, par exemple, le cas des dispositions du *RGPD*, qui régissent également ce qui relève du domaine public. Il en est de même

[473] Sylvain LONGHAIS, « Privacy Shield : Clap de fin pour l'accord transatlantique de transfert de données personnelles. Retour sur une saga juridique vieille de 20 ans », *cyberjustice.ca*, 22 septembre 2020, en ligne : <https://www.cyberjustice.ca/2020/09/22/blogue-privacy-shield-clapdefin/>.
[474] Jillian DEUTSCH et Stephanie BODONIE, « Meta Renews Warning to E.U. It Will Be Forced to Pull Facebook », *time.com*, 8 février 2022, en ligne : <https://time.com/6146178/meta-facebook-eu-withdraw-data/> (consulté le 3 mai 2022).
[475] *Id.*
[476] A. PIQUARD, préc., note 420.

s'il l'on prend la *directive (EU) 2016/680*, dite Directive Police/Justice,[477] ou bien les lois fédérale et provinciales au Canada sur la protection des renseignements personnels entre les pouvoirs publics et leurs administrés.[478] Leurs rôles sont d'assurer et de réglementer la communication entre les entités publiques des données, qu'elles ont elles-mêmes collectées : ces règles seront exclues de notre raisonnement.

On a d'autre part, les règles en droit des données s'appliquant au secteur privé, qui consacrent la libre circulation des données personnelles (en somme, toutes celles dont on a fait l'étude jusqu'ici) et qui sont exploitées par les gouvernements à des fins de surveillance. L'affaire des révélations d'Edward Snowden illustre parfaitement ce propos.

Le 6 juin 2013, dans ce qui deviendra l'un des plus grands scandales en matière d'atteinte à la vie privée, le journal britannique « The Guardian », explique sur la base des témoignages et des preuves du lanceur d'alerte Edward Snowden, comment la NSA collectait les enregistrements téléphoniques de millions de consommateurs de l'opérateur *Verizon*, aux États-Unis et dans le reste du monde.[479] Le lendemain, un autre scandale explose sur la base des révélations du même lanceur d'alerte, mais cette fois-ci, c'est le programme PRISM (*Planning Tool for Resource Integration, Synchronization, and Management*) qui indigne le monde entier. Pour cause, ce programme fournissait à la NSA, un accès direct aux données des géants du numérique américains.[480] On peut scinder ces accès aux données personnelles de millions de personnes en deux parties.

La première partie est celle des bases légales américaines à portée extraterritoriale, permettant l'accès aux autorités américaines aux données de ces compagnies. Bien que controversées pour certains et parfaitement scandaleuses pour d'autres, nous nous devons d'exclure l'étude de ces bases légales, ces dernières n'étant pas pertinente à notre propos, en ce qu'elles n'ont pas directement trait à l'abaissement de la protection de la vie privée induit par la libre circulation internationale des données.

---

[477] Voir, *Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil*, 27 avril 2016, J.O. 4 mai 2016 [*Directive Police/Justice*].
[478] Voir, *Loi sur la protection des renseignements personnels*, (1985), L.R.C. (1985), ch. P-21. Et *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*, (1982), A-2.1.
[479] S. LONGHAIS, préc., note 228, p. 15.
[480] *Id.*, p. 16.

La seconde partie est celle des bases légales permettant le transfert des données d'un pays à un autre, en l'occurrence, des pays du monde entier vers les États-Unis. Pour ce qui est de cette partie, le principe de libre circulation des données consacré en droit international et contribuant à abaisser la protection des données personnelles et de la vie privée doit être pointé du doigt. La libre circulation des données à des fins commerciales, comme nous l'avons démontré, ne peut être remise en cause du fait de sa sanctification en droit international et, plus récemment, en droit du commerce international. Ainsi, les géants du numérique bénéficiaient de toute la latitude possible pour transférer des données d'utilisateurs de pays tiers vers les États-Unis. Dès lors, les règles de libre circulation des données ont, d'une part, permis un accès beaucoup plus facilité aux données personnelles collectées par les acteurs privés américains, mais ont, d'autre part, empêché les États tiers de se prémunir contre les règles américaines à portée extraterritoriale, visant à mettre la main sur ces données.[481]

Dans le cadre de l'affaire *Snowden*, l'application de la section 215 du PATRIOT ACT et de la section 702 du FISA, qui fondait légalement l'accès aux données par les services de renseignements américains, n'était nullement empêchée par une quelconque restriction sur la libre circulation des données. Preuve en est : c'est sur cette base que la Cour de Justice de l'Union européenne a invalidé l'accord Safe Harbor, faire-valoir de la protection des données au service de la libre circulation transfrontière des données personnelles entre les États-Unis et l'Union européenne en 2015. Avant cela, la libre circulation des données pour des raisons économiques était assurée, quand bien même, les États-Unis avaient dicté leurs exigences en matière de sécurité nationale.[482]

Pour autant, la décision annulant l'accord *Safe Harbor* ne remet pas en cause le principe de libre circulation des données personnelles accordé aux opérateurs privés américains, ce principe tirant sa source de la directive de 1995 à l'époque et des règles de droit du commerce international. La libre circulation reste donc intacte quand bien même elle permet de faciliter la captation des données par des gouvernements à des fins de surveillance.

[481] À ce titre, les lois provinciales au Canada, concernant la protection des renseignements personnels dans le secteur privé prévoient des exceptions concernant la divulgation de renseignements personnels hors du canada, qui sont généralement assez larges pour permettre à ces transferts de s'opérer et de ne pas entraver la libre circulation des données, voir : K. BENYEKHLEF et P. — L. DEZIEL, préc., note 94, tableau 4.7, p. 327.
[482] S. LONGHAIS, préc., note 228, p. 19.

Section 2 : Des solutions pour enrayer le principe de libre circulation en faveur d'une meilleure protection des données personnelles ?

Faire de la protection des données personnelles une fin en soi, en finir avec la libre circulation sans limite, sanctifiée en droit du commerce international et rétablir l'équilibre entre les plateformes technoféodales et les institutions souveraines capables de dire le droit, voici à quoi ressemblerait les chantiers d'avenir pour redorer le blason de la protection des données personnelles. Nous vous proposons dans cette section conclusive de dresser une liste non exhaustive des pistes à explorer pour remettre en cause la libre circulation des données et élever un tant soit peu le niveau de protection des données personnelles.

Au fil de nos lectures, certains auteurs ont avancé, sur des problématiques concrètes de vie privée et de données personnelles ou bien sur des enjeux plus transversaux, des solutions qui viseraient à remettre au-devant de la scène la protection des données ou qui, par leurs effets, y contribueraient. Cette section peut être vue comme une synthèse de ces différentes propositions. Elle est également teintée de réflexions personnelles sur le sujet. Ces propositions suivent trois axes :

D'abord, il s'agirait de repenser la protection des données personnelles comme discipline à part entière du droit et non plus comme un sous-domaine du droit du commerce international. Ensuite, il est urgent que les États souverains, qui sont garants des libertés et des droits fondamentaux, retrouvent un rôle dans l'agencement international à l'œuvre. Enfin, et de manière plus large, il faut repenser la place des plateformes par lesquels transitent les grands flux de données personnelles. Cela passera par l'acceptation de l'hypothèse technoféodale et la manière dont les États peuvent y répondre.

Replacer la protection des données comme discipline à part entière du droit et non comme sous-domaine du droit du commerce international

Comme nous l'avons vu, les technologies évoluent, mais les problématiques relatives à la protection des données ne fluctuent que très peu. À ce titre, et comme nous avons donné un exemple lorsque nous avons abordé la doctrine américaine de vie privée, il n'est pas rare d'observer que certains problèmes relatifs à la vie privée, du fait de l'évolution des technologies dans les années 1800, sont transposables aux réalités technologiques d'aujourd'hui. Ainsi, lorsque Mark

Zuckerberg clame que la vie privée n'est plus une norme sociale, peut-être devrait-on lui opposer les travaux d'A. Westin, qui pointe justement que la vie privée comme norme sociale existe depuis la nuit des temps.[483] Mais A. Westin n'est pas le seul à avoir étudié ces questions sous un angle historique. Les historiens Philippe Ariès et George Duby ont également fait une étude très détaillée de l'histoire de la vie privée dans les années 1980 dans une série en 5 tomes intitulée *Histoire de la vie privée*.[484] De même, dans son ouvrage majeur, *Condition de l'homme moderne*, Hannah Arendt s'est également intéressée aux questions de vie privée dans la cité antique grecque.[485]

Dès lors, pour protéger la vie privée, peut-être serait-il bon de remettre au goût du jour les idéaux matérialisés par les premières lois européennes des années 1970 et de remettre en question la vision américaine de la « *privacy* » en ce qu'elle la cantonne à la survenance d'un dommage. De cette façon, cela casserait naturellement une dynamique fondée sur la libre circulation des données, puisque cette dernière serait empêchée dans la forme qu'elle revêt aujourd'hui. Cela induit nécessairement de s'opposer aux dispositions de droit des données prévues par le droit du commerce international et de faire en sorte que le droit des données redevienne une branche indépendante du droit et répondant à ses propres finalités sociopolitiques ; la vie privée n'en étant qu'une parmi d'autres.

Cette idée ne semble pas saugrenue. Après tout, les soubassements de la protection des données moderne au service d'une libre circulation internationale sont toujours fondés sur des règles juridiques, travesties certes, qui ont vu le jour dans les années 1970. Les règles instaurant une autorité de contrôle de la protection des données ne sont pas une invention du *RGPD*, mais de la toute première loi de protection des données personnelles de l'État de Hesse en Allemagne. Il en est de même pour les droits accordés aux individus sur le traitement de leurs données, qui datent également des années 1970. La protection des données personnelles moderne inféodée au droit du commerce international reprend ces codes qui ne sont pas préjudiciables pour la libre circulation des données, mais qui contribuent dans le même temps à légitimer les transferts internationaux. En quelque sorte, le droit des données moderne devient le vecteur de confiance en la libre circulation. Devant l'urgence sociale dans laquelle nos sociétés modernes se retrouvent du fait de l'exploitation à outrance des données à des fins de profits, il est plus que nécessaire de militer en faveur d'un

[483] A. F. WESTIN, préc., note 83.
[484] K. BENYEKHLEF et P. — L. DEZIEL, préc., note 94, p. 68.
[485] *Id.*, p. 66.

droit à la protection des données fort et répondant à cette urgence sociale. Les outils existent bel et bien. Mais qui pour insuffler ce second souffle ? Dans cette transformation juridique, le rôle de l'État nous semble fondamental.

Redéfinir le rôle de l'État dans un agencement international :

Nous l'avons constaté, la libre circulation internationale des données est garantie du fait du retrait de la compétence du droit des données des mains des États, sans que ces derniers ne militent vraiment pour la récupérer. Pourtant, il semble que les gouvernements doivent dans une certaine mesure retrouver toute leur place dans le règlement de ces questions afin d'assurer une protection plus forte. Dans *Léviathan*, Hobbes écrivait que l'État est le garant des libertés des hommes et les hommes doivent lui abandonner l'exercice entier de leurs libertés. En effet, l'homme est par nature un loup pour l'homme et seule la structure du souverain peut le protéger contre lui-même. Ces deux éléments sont importants pour notre raisonnement. Premièrement, Hobbes nous enseigne que pour préserver la paix et prévenir de la discorde, le souverain dispose de tous les moyens de droit.[486] Il appartient à chacun de juger ce que représentent les notions de paix et de discorde, mais lorsque les dérives que l'on a décrites, apparaissent du fait de l'exploitation des données personnelles et considérant l'impact qu'elles peuvent avoir sur les droits et libertés des individus dont le souverain est garant, on devrait admettre que ce dernier doit avoir la capacité par tout moyen de répondre aux menaces et atteintes que cela engendre. Deuxièmement, et c'est à notre sens le cœur du problème, quand on en vient à la libre circulation des données personnelles, les grandes firmes du numérique considèrent cette libre circulation des données comme étant une liberté naturelle, inaliénable alors même que cette dernière fait partie de la chose publique au sens *hobbesien* du terme.[487] Sur ce fondement, seul l'État souverain serait en mesure de décider de limiter cette liberté pour préserver

[486] T. Hobbes considérait qu' : « Il appartient de droit à tout homme ou assemblée qui a la souveraineté d'être à la fois juge des moyens de la paix et de la protection, et aussi de ce qui les empêche et les trouble, et de faire tout ce qu'il jugera nécessaire de faire, autant par avance, pour préserver la paix et la sécurité […] ». Voir, Thomas HOBBES, *Léviathan. Traité de la matière, de la forme et du pouvoir de la république ecclésiastique et civile*, traduit par Philippe FOLLIOT, Tome I, Londres, Andrew Crooke, 1651, en ligne : <http://classiques.uqac.ca/classiques/hobbes_thomas/leviathan/leviathan.html>, ch. VXIII.

[487] T. Hobbes a une vision critique dans l'exercice des libertés qu'il considère comme relevant de la chose publique : « Mais les hommes sont facilement trompés par la dénomination spécieuse de liberté, et, par manque de jugement pour faire des distinctions, ils prennent faussement pour leur héritage privé et leur droit de naissance ce qui est le droit de la seule chose publique. ». Voir, *Id.*, ch. XXI.

la paix et ainsi réduire la discorde qui pourrait résulter de l'exercice abusif de cette liberté.[488] Transposée à notre époque, la vision de Hobbes est intéressante en ce qu'elle permet de s'interroger sur le rôle que devrait avoir l'État sur la question de la libre circulation des données. Cependant, cette vision du droit édicté par le souverain, qui serait garant des droits et libertés et pourrait à ce titre par tout moyen, conserver la paix et la sécurité, s'intègre uniquement dans un cadre où l'État souverain seul dit la loi.

Seulement, nous sommes au XXIe siècle, l'ordonnancement du monde a changé et avec lui le droit a évolué, et cette vision est caduque. Les sources du droit se sont multipliées et les ordres normatifs se sont fragmentés. Ainsi, le souverain vu par Hobbes, et qui renvoie à l'État n'est plus le seul faiseur de droit. Le positivisme juridique caractérisé par l'association du droit avec l'appareil étatique, signifiant schématiquement que : « Seul l'État peut adouber la norme »[489] a largement été remise en cause. La doctrine soutenue par Carré de Malberg pour laquelle « il ne saurait y avoir de droit en dehors de l'État, ni antérieure à sa création »[490] et qui sous-tend *ipso facto* une conception moniste du droit international est aujourd'hui dépassée. Par nature, le modèle pyramidal Kelsenien, bien que trouvant un certain écho dans la norme interne et dans les ordres juridiques étatiques, se trouve petit à petit remplacé par une organisation plus horizontale du droit. La mondialisation aura joué un rôle dans ce changement de paradigme et la création et l'avènement d'internet également. Il semblerait cependant que ce soit toujours cet ordre pyramidal qui pose un problème quand on en vient à la question de la libre circulation des données et la capacité de l'État à la réglementer à des fins de protection des données de ses ressortissants. En effet, le droit commercial international n'a jamais été aussi contraignant envers les États, tant et si bien que ces derniers, dans un certain nombre de domaines, et notamment la protection des données personnelles n'ont qu'une marge de manœuvre limitée. Ainsi, l'entrave se situe principalement à ce niveau, et

---

[488] On pourrait d'ailleurs se demander si la libre circulation des données personnelles s'inscrit dans le principe de la liberté de circulation de l'information, eu égard à la nature des données échangées et l'objet de ces échanges qui est purement commercial. En effet, le principe de libre circulation de l'information est protégé directement ou indirectement par plusieurs textes concernant les droits et libertés fondamentaux (on pense à l'article 19 de la Déclaration universelle des Droits de l'Homme, à l'article de 10 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, à la Déclaration des Droits de l'Homme et du citoyen en France, ou encore à l'interprétation qui découle de l'article 2 b) de la Charte canadienne des droits et libertés). La question sous-jacente est bien évidemment : quels sont les types d'information concernés par cette liberté ? On trouve certains éléments de réflexion dans : Nicolas OCHOA, *Le principe de libre-circulation de l'information — Recherche sur les fondements juridiques d'Internet*, Paris, France, Archive ouverte HAL-SHS, 2016, en ligne : <https://halshs.archives-ouvertes.fr/halshs-01531301/document>.

[489] K. BENYEKHLEF, préc., note 366, p. 18.

[490] *Id.*, p. 37.

avec lui un mouvement descendant inspiré de la pyramide des normes, pour laquelle la norme internationale plus haute induit naturellement une soumission du droit interne. On a ici, volontairement, laissé de côté les influences politiques néolibérales et le fort lobbyisme des acteurs privés en faveur de la libre circulation pour se concentrer sur la théorie juridique, même si techniquement, les règles de droit du commerce international reflètent les intérêts des acteurs privés qui nourrissent le commerce. Dans les faits alors, la perte simultanée de pouvoir et d'influence de l'État sur ces questions de protection des données n'est pas forcément induite par de nouvelles formes récentes de normativités, mais concourt plutôt d'un schéma classique de droit moderne et de relations entre souveraineté interne et souveraineté externe.[491] Est-ce à dire pour autant que le rôle de l'État en matière de protection des données personnelles est définitivement enterré avec l'émergence de nouvelles normativités ? Nous ne le croyons pas.

Avec l'avènement d'Internet est arrivé l'avènement des réseaux. Il y aurait énormément à dire sur le paradigme du droit en réseau (droit postmoderne), mais nous nous contenterons, aux fins de la démonstration, aux interactions entre sphère privée et sphère publique dans les nouvelles normativités et qui ont contribué au fait que l'État a certes perdu du pouvoir dans sa capacité à légiférer, mais pas de son influence.[492] La théorie du droit en réseau implique nécessairement une multitude d'acteurs qui contribuent à faire le droit. Ainsi, l'État ne devient plus qu'un nœud du réseau et d'autres acteurs et notamment des acteurs privés, produisent également des normes. Selon Boris Barraud, une des fondations de ce « réseau » est la co-régulation.[493] La co-régulation est en fait une délégation volontaire du pouvoir normatif de l'État aux acteurs privés.[494] Cette dernière s'accompagne normalement d'un contrôle de la part de l'État.[495] La logique de « réseau » en droit relève de l'aveu de l'État de ne pas pouvoir imposer une logique unilatérale dans une société complexe et maillée. De ce fait, l'intégration d'une pluralité d'acteurs dans l'élaboration du droit relève d'une « nécessité fondamentale ».[496] Cette idée de co-régulation se retrouve souvent en droit contemporain des données personnelles. Si l'on prend par exemple le cas du *RGPD*, il y est laissé le soin à l'entreprise d'organiser son propre environnement sécuritaire pour les données, à la seule contrainte qu'elle doit respecter le cadre juridique que le texte met en place et qu'à ce titre, elle

[491] Voir, *Id.*, section 2 : la souveraineté dans le contexte de mondialisation, p. 49.
[492] *Id.*, p. 699
[493] B. BARRAUD, préc., note 409, p. 189.
[494] *Id.*
[495] *Id.*
[496] *Id.*, p. 191.

peut être soumis à des contrôles par une autorité de contrôle. La corégulation est, par conséquent, un compromis entre la règlementation étatique unilatérale et l'autorégulation dans laquelle, les acteurs privés se réguleraient indépendamment des États.[497] Sous la plume du Professeur Karim Benyekhlef, « la corégulation est une méthode et non une source normative ».[498] Cette méthode permet de « combiner réglementation étatique et régulation privée et de les rendre complémentaires. »[499] Dans ce cas de figure, la norme qui en résulte prend en compte les réalités contemporaines et en l'occurrence les réalités technologiques qu'une pratique législative unilatérale par l'État ne peut appréhender à elle seule. À la charge des acteurs privés, dans ce cas, d'opérer une gouvernance parfaitement respectueuse du droit étatique en matière de protection. Si l'on reprend le cas du *RGPD*, on aura constaté qu'il s'agit d'un outil juridique destiné avant tout à garantir à la libre circulation. Quand bien même il s'apparente à un outil issu de la corégulation, ce n'est pas la méthode qui doit être remise en cause, mais les objectifs. Le rôle de l'État peut être véritablement important dans la protection des données personnelles dans un cadre corégulatoire. Il le serait, une fois libéré de ces entraves issues du droit commercial international et à la condition de poursuivre des objectifs mettant en avant la protection des données, au détriment de la libre circulation des données. Cela passe par l'adoption d'une posture dans laquelle les droits fondamentaux prévalent sur les lois du marché. Cette méthode permettrait alors de reconnaître le pouvoir des grandes plateformes tout en laissant une place au moins aussi importante à l'État. Attention toutefois à ne pas tomber dans l'excès d'une domination par les compagnies privées dans l'adoption et la mise en œuvre de la norme. Pour cette raison, le rapport de force actuel entre plateformes et États doit être rééquilibré à la faveur des États. À ce titre, certains auteurs suggèrent aux États de repenser les plateformes comme des services publics. En effet, repenser la place des grands acteurs du numérique est primordiale pour une meilleure protection des données dans le sens où cela permettrait de redonner du pouvoir à l'État.

- Sur la création d'une organisation internationale de la protection des données

Certains auteurs en doctrine considèrent que le meilleur moyen d'assurer la protection des données personnelles serait de créer une organisation internationale sur la protection des données.

[497] K. BENYEKHLEF, préc., note 366, p. 743.
[498] *Id.*
[499] *Id.*

Pour soutenir cette création, les auteurs considèrent qu'elle viendrait combler un vide juridique puisqu'il n'y a à ce jour pas de perception globale de la protection des données.[500] Ainsi, une telle organisation contribuerait à unifier les standards de protection des données au niveau mondial. De plus, elle favoriserait la coopération internationale en matière de protection à la vie privée.[501] Enfin, cela contribuerait à la gouvernance internationale des données en érigeant une institution dédiée.[502]

Une organisation internationale des données présuppose une règlementation internationale prééminente. Pendant ces 50 dernières années, les outils issus du droit du commerce international dont nous avons fait état ont été utilisés en faveur d'une libre circulation des données quasi sans limites. De ce fait, ils ont largement contribué à l'abaissement de la protection des données personnelles. Créer une organisation internationale pour la protection des données, reviendrait à notre sens à sceller l'avenir de la protection des données sans retour en arrière possible. De plus, il y a fort à parier que le rapport de force entre cette organisation et l'OMC soit davantage à la faveur de cette dernière, ce qui contribuerait encore à accentuer l'hégémonie de la libre circulation des données ; l'organisation internationale des données agissant comme faire valoir de la libre circulation commerciale. Enfin, cela résulterait probablement en un immobilisme de la protection des données, comme c'est bien souvent le cas au sein des institutions internationales publiques. Dans un contexte où nous considérons que les États devraient se désentraver des règles de droit du commerce international en prérequis, pour élever le niveau de protection des données et pour les raisons précédemment citées, nous ne pouvons pas considérer que la création d'une organisation internationale des données soit une solution viable pour casser la libre circulation des données.

Repenser la place des plateformes par lesquelles transitent les grands flux de données personnelles

Sortir d'une logique de libre circulation des données et d'exploitation abusive des données passe également par la remise en question de l'hégémonie des grandes plateformes qui concentrent les flux transfrontières de données. Partant du principe que le droit de la concurrence ne peut plus rien pour contrer les citadelles imprenables qu'elles se sont constituées,[503] d'autres moyens de

[500] Paul DE HERT et Vagelis PAPAKONSTANTINOU, « Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency », (2013) 9-2 *Journal of Law and Policy* 271, 316.
[501] *Id.*
[502] *Id.*, 318.
[503] C. DURAND, préc., note 198, p. 229.

réguler les grandes plateformes sont parfois avancés. Parmi ces moyens, le démantèlement des plateformes fait partie des solutions qui sont parfois brandies. Loin d'être seulement une idée débattue en doctrine, cette idée commence à s'installer dans le débat public. À ce titre, le sujet s'est invité dans la campagne présidentielle française, par le biais surprenant du candidat libéral Emmanuel Macron qui, dans un entretien à un journal, déclarait qu'un démantèlement n'était pas une solution à exclure si cela était nécessaire.[504] Selon lui : « les plateformes viennent utiliser nos libertés antiques ou postrévolutionnaires pour les détourner de leur essence ».[505] Ce démantèlement passerait notamment par une restructuration profonde de ces acteurs privés par les régulateurs ou bien, par voie de justice, revenir sur certaines acquisitions d'autres services par le biais de fusions.[506] Cependant, si les bases légales existent aussi bien aux États-Unis qu'en Europe pour procéder à ces démantèlements, ils restent compliqués à mettre en œuvre.[507]

Pour autant, dans une logique de marché, ce démantèlement des plateformes s'apparente davantage à un rabattage des cartes sur le plan économique, avec pour finalité, la restauration d'une concurrence saine. Il ne semble pas qu'un démantèlement, qui ne poursuivent pas des objectifs plus ne change la donne. Alors, comment un tel démantèlement devrait-il s'accompagner ? Doit-on attribuer à ces plateformes une qualification de service public ? Combinée à une méthode de corégulation, cela permettrait probablement un meilleur contrôle de l'utilisation faite des données et de la circulation de ces dernières. Cela pourrait constituer un pas important dans la réhabilitation d'un rôle important pour l'État en matière de protection des données personnelles. Pour autant, cela freinerait-il la libre circulation à but commercial au profit d'une meilleure protection des données ? Pour cela, ne faudrait-il mieux pas s'atteler à retirer le profit de l'équation ? La piste des données comme bien commun au même titre que l'eau ou l'air pourrait être intéressante à cette fin.[508]

---

[504] Julien BALDACCHINO, « Numérique : Emmanuel Macron envisage "le démantèlement" des Gafam », *www.franceinter.fr*, 13 avril 2022, en ligne : <https://www.franceinter.fr/politique/numerique-emmanuel-macron-envisage-le-demantelement-des-gafam>.
[505] *Id.*
[506] Marc BOURREAU et Anne PERROT, « Plateformes numériques : réguler avant qu'il ne soit trop tard », (2020) 6-60 *Notes du conseil d'analyse économique* 1, 9.
[507] *Id.*, 10.
[508] Voir, Pricilla M. REGAN, « Privacy as a Common Good in the Digital World », (2002) 5-3 *Information, Communication & Society* 382.

CONCLUSION

Au cours de nos développements, nous aurons constaté que depuis les années 1970, on assiste à un glissement de la protection des données personnelles. Ce glissement est de deux ordres. Il est d'abord conceptuel. Il est ensuite territorial.

L'étude du droit des données personnelles des cinquante dernières années nous apporte des éclaircissements indispensables ainsi qu'une rétrospective capitale pour aborder les problématiques actuelles quant à la libre circulation des données personnelles. La philosophie européenne influencée par les idéaux des droits et libertés fondamentaux et par les traumatismes issus de la Seconde Guerre mondiale et des régimes totalitaires d'après-guerre prônait la protection des données personnelles et de la vie privée comme une fin en soi. Cette vision a été balayée par la conception américaine de la vie privée fondée sur les « *torts* ». C'est ce que l'on qualifiera de glissement conceptuel. Ce basculement s'est opéré concomitamment à l'avènement des thèses néolibérales des années 1980 dans l'économie des pays occidentaux. Le concept de vie privée à l'américaine fondé sur les « *torts* » est en effet beaucoup plus conciliable le principe de libre circulation des données qui s'insère dans le cadre d'un marché largement dérégulé, à l'ère où les technologies informatiques sont porteuses de promesses de jouvence pour l'économie.

Ce principe de libre circulation est d'ailleurs consacré à l'occasion du deuxième glissement de la protection des données, territorial donc. Les premiers outils internationaux de droit des données personnelles qui proclame le principe de libre circulation internationale des données ont également produit un effet confiscatoire de la compétence des États à légiférer en la matière. La création de l'OMC et l'entrée en vigueur du *GATS* auront non seulement parachevé de soustraire le droit des données personnelles à la compétence des États, de sanctifier le principe de libre circulation des données, mais surtout de placer le droit des données sous la houlette du droit du commerce international, signe que le droit des données s'inscrit parfaitement dans la thèse de l'« axiologie du droit commercial ».[509] Toutes ces mutations dans le droit positif des données sont impulsées par un contexte économique et politique dans lequel la protection des données est davantage vue comme un frein à l'économie, qu'une nécessité de protection des individus, individuellement et collectivement. Dès lors, les futures lois de protection des données qu'elles

[509] K. BENYEKHLEF, préc., note 366.

émanent d'États ou bien de l'Union européenne sont dans le moule de ce triptyque ne pouvant mener qu'à l'abaissement des objectifs de protection des données :

- Droit à la vie privée fondé sur les *torts*

- Principe de libre circulation sanctifié en droit international public

- Droit des données personnelles placé sous la houlette du droit du commerce international

Sous couvert de progrès, on ne fait, en réalité, qu'encadrer des pratiques d'atteintes à la vie privée et à bien d'autres droits et libertés, sans jamais les questionner. On fait de la protection des données personnelles un outil de légitimation de ces pratiques, comme c'est le constat qui est le nôtre lorsque nous abordons l'abaissement des objectifs de protection. Dans le modèle néolibéral qui caractérise nos sociétés modernes, le droit pour ce qui est des domaines touchant à la création de valeur économique, est mis au service de la recherche de profit. La protection des données personnelles n'échappe pas à ce constat. Les plateformes-citadelles et l'hégémonie qu'elles exercent sur les données résultent de choix idéologiques qui ont été consacrés en droit. C'est pour cette raison qu'un élèvement de la protection des données personnelles passera forcément par la remise en question de la libre circulation internationale de ces dernières. Cette remise en question devra s'appréhender par le truchement d'un droit à la protection des données comme branche indépendante du droit, d'un rôle fort de l'appareil étatique dans les questions de règlementation, de régulation par le biais d'une méthode de corégulation, par exemple, et enfin par le changement du statut des plateformes.

Retracer l'avènement du principe de la libre circulation des données aura permis de démontrer que d'autres visions mettant davantage l'accent sur la protection des données sont possibles, que la libre circulation des données est avant tout une construction juridique servant des intérêts économiques et qu'elle devrait dès lors être remise en question. En conséquence, notre mémoire se veut être un point de départ modeste à la réflexion vers un autre modèle plus respectueux des droits et libertés des individus fondés sur la protection des données, qu'ils soient exercés individuellement ou collectivement. De futures recherches pourraient dès lors imaginer de manière plus concrète la matérialisation de cette remise en cause de la libre circulation

internationale des données au profit d'un droit des données personnelles dont la fin en soi, est la protection des données.

TABLE DE LA LÉGISLATION

Textes fédéraux

Projet de Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois, C-11 (17 novembre 2020).

Loi sur la protection des renseignements personnels, (1985), L.R.C. (1985), ch. P-21.

Textes québécois

Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels, (1982), A-2.1.

Projet de loi modernisant des dispositions législatives en matière de protection des renseignements personnels, n° 64 (2020).

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

Textes américains

California Online Privacy Protection Act, 2018.

U.S. Const.

The Privacy Act, (1974) 5 U.S.C.

Communication Decency Act, (1996) 47 U.S. Code.

Textes européens

Constitución de la República Portuguesa [Constitution of the Portuguese Republic], (1976) Diário da República.

Constitución Española [Spanish Constitution], (1978) BOE, BOE-A-1978-31229.

Datalag [Data Act], (1973), SFS. 289.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (1978), J.O 7 janv. 1978.

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O. 7 août 2004.

Textes de l'Union européenne

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, (1995), J.O. 23 novembre 1995.

Directive du Parlement Européen et du Conseil du 6 octobre 1997 modifiant les directives 90/387/CEE et 92/44/CEE en vue de les adapter à un environnement concurrentiel dans le secteur des télécommunications, (1997), 97/51/CE.

Directive du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, (2000), 2000/31/CE.

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, (2016), J.O. 4 mai 2016.

Proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur, COM/98/0586 (23 décembre 1998).

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, (2016), J.O. 4 mai 2016.

Textes internationaux

Accord de libre-échange entre l'Union européenne et ses États membres, d'une part, et la République de Corée, d'autre part, (2011), 22011A0514(01).

Accord économique et commercial global entre le Canada, d'une part, et l'Union européenne, d'autre part, (2017), 22017A0114(01).

Accord Canada-États-Unis-Mexique, 30 novembre 2018.

Accord général sur le commerce des services de 1994, Annexe 1B de l'accord instituant l'OMC.

Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO, (2010), A/SA.1/01/10

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, (1950), S.T.E. n-° 5.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (1981), S.T.E. n-° 108.

Déclaration universelle des droits de l'homme, (1948), Rés. 217 A (III), Doc. off. A.G.N.U., 3e sess., suppl. n° 13, p. 17, Doc. N.U A/810.

Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980

Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Private Sector, (1973), (73)22.

Resolution on the Protection of the Privacy of Individuals Vis-A-Vis Electronic Data Banks in the Public Sector, (1974), (74)29.

United States-Singapore Free Trade Agreement, 6 mai 2003.

United States-Australia Free Trade Agreement, 18 mai 2004.

United States-Morocco Free Trade Agreement, 15 juin 2004.

United States-Bahrain Free Trade Agreement, 14 septembre 2004.

United States-Peru Free Trade Agreement, 12 avril 2006.

TABLE DE LA JURISPRUDENCE

Jurisprudence Canadienne

Jurisprudence américaine

Jurisprudence de l'Union européenne

BIBLIOGRAPHIE

Monographies et ouvrages collectifs

BARRAUD, B., *Repenser la pyramide des normes à l'ère des réseaux : pour une conception pragmatique du droit*, coll. logiques juridiques, L'Harmattan, 2013.

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992.

BENYEKHLEF, K., *Une possible histoire de la norme, les normativités émergentes de la mondialisation*, 2e éd., Montréal, Thémis, 2015.

BENYEKHLEF, K. et P.-L. DEZIEL, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Yvon Blais, 2018.

DARDOT, P. et C. LAVAL, *La nouvelle raison du monde*, coll. Poche/Sciences humaines et sociales, Paris, La Découverte, 2010.

DURAND, C., *Techno-féodalisme*, Paris, Zones, 2020.

FLAHERTY, D. H., *Protecting Privacy in Surveillance Societies*, Chapel Hill and London, The University of North Carolina Press, 1989.

FUSTER, G. G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, coll. Law, Governance and Technology Series, n°16, Cham, Springer.

GOMART, T., *Guerres invisibles*, Tallandier, coll. Texto, Paris.

GORDON, R. J., *The Rise and Fall of American Growth: The U.S. Standard of Living since the Civil War*, Princeton, NJ, Princeton University Press, 2016.

HOBBES, T., *Léviathan. Traité de la matière, de la forme et du pouvoir de la république ecclésiastique et civile*, traduit par Philippe FOLLIOT, Tome I, Londres, Andrew Crooke, 1651, en ligne : <http://classiques.uqac.ca/classiques/hobbes_thomas/leviathan/leviathan.html>.

HUWART, J.-Y. et L. VERDIER, *Economic Globalisation - Origins and Consequences*, coll. OECD Insights, Paris, France, OECD Publishing, 2013.

KUNER, C., *Transborder data flows and data privacy laws*, Oxford, UK, Oxford University Press, 2013.

LORDON, F., *Imperium, Structures et affects des corps politiques*, Paris, La Fabrique, 2015.

MARX, K., *Le Capital*, traduit par M.J ROY, Paris, Maurice Lacharte et Cie, 1872.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Policy issues in data protection and privacy : concepts and perspectives : proceedings of the OECD seminar 24th to 26th June 1974*, OECD Publications Center, coll. OECD Informatics studies, n°10, Paris, 1976.

OST, F. et M. VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, coll. Droit, Bruxelles, Facultés Universitaires Saint-Louis Bruxelles - F.U.S.L., 2010.

SUPIOT, A., *La gouvernance par les nombres*, Fayard, coll. Pluriel, Paris, 2020.

TUSSEL, J., *Spain: From Dictatorship to Democracy 1939 to the Present*, Oxford, Blackwell Publishing, 2007.

WESTIN, A. F., *Privacy and Freedom*, New York, Atheneum, 1967.

ZUBOFF, S., *L'Âge du capitalisme de surveillance*, coll. Zulma Essais, Zulma, 2020.

Articles de revues et études d'ouvrages collectifs

ALLEN, D. W. E., A. BERG, C. BERG, B. MARKEY-TOWLER et J. POTTS, « Some Economic Consequences of the GDPR », (2019) 39-2 *Economics Bulletin* 785.

BEUSCART, J.-S. et P. FLICHY, « Plateformes numériques », (2018) 2018/6-212 *Réseaux* 9.

BOHLOFF, K. et A. BAUMANNS, « Harmonising German Data Protection and the Council of Europe Convention », (1984) 12 *Int'l Bus Law* 175.

BOURREAU, M. et A. PERROT, « Plateformes numériques : réguler avant qu'il ne soit trop tard », (2020) 6-60 *Notes du conseil d'analyse économique* 1.

BRANDAO, P. R., « A brief history of Computation's in Portugal », (2018) 2-5 *Invention journal of Research technology in engineering & management* 01.

BURRI, M., « The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation », (2017) 51 *UC Davis Law Review* 65.

BURRI, M., « The Regulation of Data Flows Through Trade Agreements », (2017) 48-1 *Georgetown Journal of International Law* 407.

DALENIUS, T., « Data Protection Legislation in Sweden: A Statistician's Perspective », (1979) 142-3 *Journal of the Royal Statistical Society. Series A (General)* 285.

DE HERT, P. et V. PAPAKONSTANTINOU, « Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency », (2013) 9-2 *Journal of Law and Policy* 271.

DEDRICK, J., V. GURBAXANI et K. L. KRAEMER, « Information technology and economic performance: A critical review of the empirical evidence », (2003) 35-1 *ACM computing Surveys* 1.

EGER, J. M., « Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers », (1978) 10-4 *Law & Pol'y Int'l Bus* 1055.

EHRLICH, P., « Communications Decency Act § 230 », (2002) 17-1 *Berkeley Technology Law Journal* 401.

FREISS, K., « Protection de l'environnement et expropriation indirecte dans les accords mega-régionaux », (2018) 31-1 *Revue québécoise de droit international* 38.

FUSTER, G. G., « The Beginning of EU Data Protection », dans Gloria González FUSTER (dir.), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, coll. Law, Governance and Technology Series, n°16, Cham, Springer, p. 111.

GAVISON, R., « Privacy and the Limits of Law », (1980) 89-3 *The Yale Law Journal* 421.

GRAND, P., « Le Fichier Juif : un malaise », (1999) 1999/3-167 *Revue d'Histoire de la Shoah* 53.

GRATTON, É., « Dealing with Canadian and Quebec Legal requirements in the Context of trans-border Transfers of Personnal Information and Cloud Computing services », dans Jean CHARTIER

et BARREAU DU QUEBEC (dir.), *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels, les 30 ans de la Commission d'accès à l'information*, 358, Cowansville, Québec, Yvon Blais, 2012, p. 7.

GRYNBAUM, L., « La directive "Commerce électronique" ou l'inquiétant retour de l'individualisme juridique », (2001) 7-8-chron. 18 *Communication Commerce électronique*.

HAFLI, T., « Transborder Data Flows - The Scandinavian Solution », dans Jon BING et Knut S. SELMER (dir.), *A Decade of Computers and Law*, Oslo, Universitetsforlaget, 1980, p. 59.

HONDIUS, F. W., « Computers: Data privacy: The European community grapples with protecting individual rights in the midst of rampant computer progress », (1980) 17-3 *IEEE Spectrum* 67.

HONDIUS, F. W., « Data Law in Europe », (1980) 16 *Stan J Int'l L* 87.

JORGENSON, D. W. et K. VU, « Information Technology and the World Economy », (2005) 107-4 *Scandinavian Journal of Economics* 631.

JOURDAIN, L., « La Commission européenne et la construction d'un nouveau modèle d'intervention publique. Le cas de la politique de recherche et de développement technologique », (1996) 46-3 *Revue française de science politique* 496.

KIRBY, M. D., « Transborder Data Flows and the Basic Rules of Data Privacy », (1980) 16 *Stan J Int'l L* 27.

KONG, L., « Data Protection and Transborder Data Flow in the European and Global Context », (2010) 21-2 *The European Journal of International Law* 441.

KRAMER, I. R., « The Birth of Privacy Law: A Century Since Warren and Brandeis », (1990) 39-3 *Catholic University Law Review* 703.

MEDA-CALVET, I., « Playfulness and the Advent of Computerization in Spain: The National Club of ZX81 Users », dans Fabio GADDUCI et Mirko TAVOSANIS (dir.), *History and Philosophy of Computing : 3rd International Conference on History and Philosophy of Computing (HaPoC), on October 8th, 9th, 10th et 11th 2015*, Pisa, Italie, Springer, 2015, p. 228.

MEDDIN, E., « The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services », (2020) 35-4 *Am U Int'l L Rev* 997.

MITCHELL, A. D. et J. HEPBURN, « Don't Fence Me In: Reforming Trade and Investment Law To Better Facilitate Cross-Border Data Transfer », (2018) 19-1 *Yale Journal of Law & Technology* 182-237.

MOURON, P., « La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne », (2019) Hiver 2018-2019-49 *La revue européenne des médias et du numérique*.

ÖMAN, S., « Implementing Data Protection in Law », (2004) 47 *IT Law – Scandinavian Studies in Law* 389.

PARDAU, S. L., « The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States », (2018) 23-1 *J. Tech. L. & Pol'y* 68.

POSNER, R., « The Right of Privacy », (1978) 12-3 *Georgia Law Review*.

POSNER, R., « The Economics of Privacy », (1980) 71-2, Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association *The American Economic Review* 405.

POZNANSKI, R., « Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs », *Gazette des archives* 1997.177-178.250.

REGAN, P. M., « Privacy as a Common Good in the Digital World », (2002) 5-3 *Information, Communication & Society* 382.

SAMUELSON, P. et H. R. VARIAN, « The New Economy and information technology policy », dans Jeffrey A. FRANKEL et Peter R. ORZAG (dir.), *Economic Policy During the 1990s*, Cambridge (MA), MIT Press, 2002, p. 1131.

SAURON, J.-L., « Le RGPD : outil ou entrave de la société d'information ? », (2018) 2018 *Dalloz IP/IT* 17.

SEN, N., « Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path? », (2018) 21-2 *Journal of International Economic Law* 323.

TAVANI, H. T., « Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy », (2007) 38-1 *Metaphilosophy* 1.

VELLI, F., « The Issue of Data Protection in EU Trade Commitments: Cross-border Data Transfers in GATS and Bilateral Free Trade Agreements », (2019) 4-3 *European Papers* 881.

VON HAYEK, F. A., « The Use of Knowledge in Society », (1945) XXXV-4 *American Economic Review* 519.

WARREN, S. D. et L. D. BRANDEIS, « The Right To Privacy », (1890) 4-5 *Harvard Law Review* 193.

WASSERSTROM, R. A., « Privacy: some arguments and assumptions », dans FERDINAND D. SCHOEMAN (dir.), *Philosophical Dimensions of Privacy: an Anthology*, Cambridge, Cambridge University Press, 1984, p. 317.

WHEELER, W., « Economics of Information: a brief introduction », (2011) 36/37 *Progressive Librarian* 42

WUNSCH-VINCENT, S. et A. HOLD, « Towards coherent rules for digital trade: Building on efforts in multilateral versus preferential trade negotiations », *World Trade Institute Papers* 2012.251.

ZUBOFF, S., « Big other: Surveillance Capitalism and the Prospects of an Information Civilization », (2015) 30 *Journal of Information Technology* 75.

Mémoires et thèses

LONGHAIS, S., *Le Privacy Shield : cadre juridique efficace ou accord politico-économique ?*, Master of Laws Thesis, Aix-en-Provence, Aix-Marseille Université, 2019, en ligne : <http://www.iredic.fr/wp-content/uploads/2020/04/longhais-s.-macopymoire-privacy-shield-2018-2019.pdf>.

Documents gouvernementaux

COMMISSARIAT A LA PROTECTION DE LA VIE PRIVEE DU CANADA, *Traitement transfrontalier des données personnelles*, Lignes directrices, Ottawa (ON), Commissariat à la protection de la vie privée du Canada, 2009, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/aeroports-et-frontieres/gl_dab_090127/>.

COMMISSION DES COMMUNAUTES EUROPEENNE, *Vers la societé de l'information en Europe : un plan d'action*, Communication, C0M(94) 347, Bruxelles, Commission des communautés européenne, 1994.

COMMISSION EUROPÉENNE, *The European Community and Data Processing -- Government Development Aids Permitted*, Information, 21/72, coll. Competition, Bruxelles, Commission Européenne, 1972.

COMMISSION EUROPÉENNE, *Communication by the Commission of the European Communities concerning a Community policy for data processing*, Communication, P-63/73, coll. Information Memo, Bruxelles, Commission Européenne, 1973.

COMMISSION EUROPEENNE, *Croissance, compétitivité, emploi ; Les défis et les pistes pour entrer dans le XXIe siècle*, Livre blanc, Bruxelles, Commission Européenne, 1994.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2016*, Rapport d'activité, 37, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2017, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2017*, Rapport d'activité, 38, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2018, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2018*, Rapport d'activité, 39, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2019, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-39e_rapport_annuel_2018.pdf>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Ce qu'il faut savoir sur les règles d'entreprise contraignantes (BCR) », *www.cnil.fr* (7 février 2020), en ligne : <https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2019*, Rapport d'activité, 40, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2020, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, *Rapport d'activité 2020*, Rapport d'activité, 41, Paris, France, Commission Nationale de l'Informatique et des Libertés, 2021, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf>.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Journée de la protection des données : focus sur une année record pour l'action répressive de la CNIL », *https://www.cnil.fr* (28 janvier 2022), en ligne : <https://www.cnil.fr/fr/bilan-sanctions-mises-en-demeure-2021> (consulté le 21 mars 2022).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Donnée personnelle », *www.cnil.fr*, en ligne : <https://www.cnil.fr/fr/definition/donnee-personnelle> (consulté le 9 juin 2022).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, « Transfert de données », *www.cnil.fr*, en ligne : <https://www.cnil.fr/fr/definition/transfert-de-donnees> (consulté le 9 juin 2022).

WP29, *Guidelines on Article 49 of Regulation 2016/679*, Guidelines, WP 261, Brussels, WP29.

Rapports et conférences

BRENNAN CENTER, « Are they allowed to do that? A breakdown of selected government surveillance programs », *https://www.brennancenter.org*, en ligne : <https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf> (consulté le 1 avril 2022).

CASALINI, F. et J. L. GONZÁLEZ, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers, 220, Paris, France, OECD Publishing, 2019.

HEDLBOM, M. K. et W. B. GARRISON, *The Global Telecommunications Infrastructure: European Community (Union) Telecommunications Developments*, , Charleston, S.C., 1995.

HUFBAUER, G. C. et L. ZHIYAO, *Global E-Commerce Talks Stumble on Data Issues, Privacy, and More*, Policy Brief, 19-14, Washington, D.C., Peterson Institute for International Economics, 2019.

ISMAIL, Y., *Le commerce électronique au sein de l'Organisation mondiale du commerce : Historique et dernières avancées des négociations dans le cadre de la déclaration conjointe*, Winnipeg, International Institute for Sustainable Development, 2020.

KOMINSKI, R. et U.S DEPARTMENT OF COMMERCE, BUREAU OF THE CENSUS, *Computer Use in the United States: 1984*, Current Population Reports, 155, coll. Special Studies Series P-23, Washington, D.C., U.S Government Printing Office, 1988.

KPMG, *Baromètre RGPD, 3 ans après, où en êtes-vous ?*, Baromètre, Paris, France, KPMG, Juillet2021.

LETERME, C. *Quelle régulation mondiale pour l'économie des données ? Le « commerce électronique » dans les nouveaux accords commerciaux internationaux*, Conférence, Laboratoire de Cyberjustice, Montréal, 6 avril 2021.

LONGHAIS, S., « Privacy Shield : Clap de fin pour l'accord transatlantique de transfert de données personnelles. Retour sur une saga juridique vieille de 20 ans », *cyberjustice.ca* (22 septembre 2020), en ligne : <https://www.cyberjustice.ca/2020/09/22/blogue-privacy-shield-clapdefin/> (consulté le 3 mai 2022).

MISHRA, N., *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, NUS Centre for International Law Research Paper, 19/09, Singapore, NUS Centre for International Law, 2018.

NORA, S. et A. MINC, *L'informatisation de la societé*, Rapport à M. le Président de la République, B17970, Paris, 1978, en ligne : <https://www.vie-publique.fr/sites/default/files/rapport/pdf/154000252.pdf> (consulté le 17 mars 2021).

OCHOA, N. *Le principe de libre-circulation de l'information - Recherche sur les fondements juridiques d'Internet*, Paris, France, Archive ouverte HAL-SHS, 2016.

OECD, *Perspectives des technologies de l'information de l'OCDE*, coll. Technologies de l'information et des communications, Paris, France, OECD, 2004.

OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers, 176, coll. OECD Publishing, Paris, France, OECD, 2011.

OECD, *Perspectives des technologies de l'information de l'OCDE*, coll. Technologies de l'information et des communications, Paris, France, OECD, 2004.

SENAT FRANCE, « Étude de législation comparée n° 33 — janvier 1998 — La protection de la vie privée face aux médias », *senat.fr* (janvier 1998), en ligne : <http://www.senat.fr/lc/lc33/lc3312.html> (consulté le 17 mars 2021).

TRICOT, B., *Rapport de la Commission Informatique et Libertés*, Rapport de la commission informatique et libertés, 410, coll. La documentation française, Paris, Ministère de la Justice, 1975

Dictionnaires et encyclopédies

GOUJON, P., « Informatique – Évolution des systèmes de traitement de l'information », dans *Encyclopédie Universalis*, Corpus 12, Paris, France, Encyclopédie Universalis, 1989.

LAROUSSE, « Analyse de données », *www.larousse.fr*, en ligne : <https://www.larousse.fr/encyclopedie/divers/analyse_des_données/44425>.

LAROUSSE, « Télématique », *larousse.fr*, en ligne : <https://www.larousse.fr/dictionnaires/francais/télématique/77084#:~:text=Ensemble%20des%20techniques%20et%20des,les%20télécommunications%20et%20l%27informatique.>.

KRANZBERG, M. et M. T. HANNAN, « History of the Organization of Work Automation », *Britannica.com*, en ligne : <https://www.britannica.com/topic/history-of-work-organization-648000/Automation>.

REID, H., *Dictionnaire de droit québécois et canadien*, Version abrégée., Montréal, Wilson & Lafleur, 2016.

Sources journalistiques

BALDACCHINO, J., « Numérique : Emmanuel Macron envisage “le démantèlement” des Gafam », *www.franceinter.fr* (13 avril 2022), en ligne : <https://www.franceinter.fr/politique/numerique-emmanuel-macron-envisage-le-demantelement-des-gafam> (consulté le 4 mai 2022).

BOUISSOU, J., « L’OMC s’inquiète du protectionnisme numérique », *lemonde.fr* (23 novembre 2020), en ligne : <https://www.lemonde.fr/economie/article/2020/11/23/l-omc-s-inquiete-du-protectionnisme-numerique_6060808_3234.html>.

BUG BROTHER, « Safari et la (nouvelle) chasse aux Français », *Le Monde.fr* (23 décembre 2010), en ligne : <https://www.lemonde.fr/blog/bugbrother/2010/12/23/safari-et-la-nouvelle-chasse-aux-francais/>.

CHERIF, A., « Pourquoi l’Europe mise sur la libre circulation des données non personnelles », *www.latribune.fr* (4 octobre 2018), en ligne : <https://www.latribune.fr/technos-medias/pourquoi-l-europe-mise-sur-la-libre-circulation-des-donnees-non-personnelles-792766.html> (consulté le 8 juin 2022).

COOPER, E. R., A. C. RAUL et S. PORATH, « The Privacy, Data Protection and Cybersecurity Law Review: APEC Overview », *www.thelawreviews.co.uk* (26 octobre 2021), en ligne : <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/apec-overview> (consulté le 9 mai 2022).

DECEW, J., « Privacy », *plato.stanford.edu* (18 janvier 2018), en ligne : <https://plato.stanford.edu/entries/privacy/#PriResAcc>.

DEUTSCH, J. et S. BODONIE, « Meta Renews Warning to E.U. It Will Be Forced to Pull Facebook », *time.com* (8 février 2022), en ligne : <https://time.com/6146178/meta-facebook-eu-withdraw-data/> (consulté le 3 mai 2022).

FRANCE INFO, « Internet : des câbles sous-marins pour faire transiter les données », *francetvinfo.fr* (5 juillet 2016), en ligne : <https://www.francetvinfo.fr/internet/securite-sur-internet/internet-des-cables-sous-marins-pour-faire-transiter-les-donnees_1532971.html>.

GLOSSAIRE-INTERNATIONAL, « Définition de Barrière non tarifaire », *https://www.glossaire-international.com*, en ligne : <https://www.glossaire-international.com/pages/tous-les-termes/barriere-non-tarifaire.html>.

HISTOIRE CIGREF, « World Wide Web, toute une histoire ! », *cigref.fr* (12 août 2013), en ligne : <https://www.cigref.fr/archives/histoire-cigref/blog/world-wide-web-toute-une-histoire/#:~:text=Le%206%20août%201991%2C%20Tim,«%20n%27importe%20où%20»%20 !>.

HOUEIX, R., « Le lobbying de Facebook en Europe dévoilé par des mémos internes », *www.france24.com* (4 mars 2019), en ligne : <https://www.france24.com/fr/20190304-europe-lobby-facebook-rgpd-sheryl-sandberg-memo> (consulté le 9 mai 2022).

LA QUADRATURE DU NET, « Les GAFAM échappent au RGPD, la CNIL complice », *www.laquadrature.net* (25 mai 2021), en ligne : <https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/> (consulté le 21 mars 2022).

LE MONDE, « Selon le rapport de Martin Bangemann, vice-président de la Commission européenne La déréglementation des télécommunications faciliterait l'accès aux "autoroutes de l'information" », *lemonde.fr* (2 juin 1994), en ligne : <https://www.lemonde.fr/archives/article/1994/06/02/selon-le-rapport-de-martin-bangemann-vice-president-de-la-commission-europeenne-la-dereglementation-des-telecommunications-faciliterait-l-acces-aux-autoroutes-de-l-information_3833332_1819218.html>.

LE MONDE, « Pour le fondateur de Facebook, la protection de la vie privée n'est plus la norme », *www.lemonde.fr* (11 janvier 2010), en ligne : <https://www.lemonde.fr/technologies/article/2010/01/11/pour-le-fondateur-de-facebook-la-protection-de-la-vie-privee-n-est-plus-la-norme_1289944_651865.html#:~:text=Technologies-,Pour%20le%20fondateur%20de%20Facebook%2C%20la%20protection%20de%20la%20vie,générations%20que%20pour%20leurs%20parents.&text=Lecture%201%20min.>.

LETERME, C., « Qui captera l'"or du XXIe siècle" ? Bataille autour des données numériques », *monde-diplomatique.fr* (novembre 2019), en ligne : <https://www.monde-diplomatique.fr/2019/11/LETERME/60937>.

LICTEVOUT, L. et V. LEQUEUX, « La politique numérique de l'Union européenne », *touteleurope.eu* (16 décembre 2020), en ligne : <https://www.touteleurope.eu/economie-et-social/la-politique-numerique-de-l-union-europeenne/>.

MADIEGA, T., *Réforme du régime européen de responsabilité des intermédiaires en ligne : contexte de la future législation relative aux services numériques*, Analyse approfondie, PE. 649.404, Strasbourg, Service de recherche du Parlement européen, 2020, en ligne : <https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_FR.pdf>.

MOORE, S., « Gartner Says Worldwide Business Intelligence and Analytics Market to Reach $18.3 Billion in 2017 », *gartner.com* (17 février 2017), en ligne : <https://www.gartner.com/en/newsroom/press-releases/2017-02-17-gartner-says-worldwide-business-intelligence-and-analytics-market-to-reach-18-billion-in-2017>.

OECD, « À propos », *oecd.org*, en ligne : <http://www.oecd.org/fr/apropos/#:~:text=La%20mission%20de%20l%27Organisation,social%20partout%20dans%20le%20monde.>.

ORGANISATION MONDIALE DU COMMERCE, « Le commerce électronique », *wto.org*, en ligne : <https://www.wto.org/french/tratop_f/ecom_f/ecom_f.htm>.

PIQUARD, A., « Données numériques : le nouvel accord entre l'Europe et les Etats-Unis suscite des interrogations », *www.lemonde.fr* (12 avril 2022), en ligne : <https://www.lemonde.fr/economie/article/2022/04/12/donnees-numeriques-un-nouvel-accord-europe-etats-unis-suscite-des-interrogations_6121798_3234.html> (consulté le 6 juin 2022).

RAOUL, G., « Qu'est-ce que le sharding ? Définition et avantages de cette méthode de distribution des données », *lebigdata.fr* (7 septembre 2017), en ligne : <https://www.lebigdata.fr/sharding-definition-avantage#:~:text=Le%20Sharding%20permet%20d%27organiser,aux%20coûts%20bien%20plus%20raisonnables.>.

RICHARD, P., « RGPD : un bilan mitigé », *https://www.techniques-ingenieur.fr* (28 mai 2021), en ligne : <https://www.techniques-ingenieur.fr/actualite/articles/rgpd-un-bilan-mitige-93755/> (consulté le 21 mars 2022).

SCHULER, K., « Federal data privacy regulation is on the way — That's a good thing », *iapp.org* (22 janvier 2021), en ligne : <https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/>.

SCHWAB, P.-N., « Statistiques RGPD Europe : évolution du nombre de plaintes par pays », *www.intotheminds.com* (4 mai 2020), en ligne : <https://www.intotheminds.com/blog/statistiques-rgpd-europe/> (consulté le 21 mars 2022).

SENAT FRANCE, « Étude de législation comparée n° 33 — janvier 1998 — La protection de la vie privée face aux médias », *senat.fr* (janvier 1998), en ligne : <http://www.senat.fr/lc/lc33/lc3312.html> (consulté le 17 mars 2021).

SOLOW, R. M., « We'd Better Watch Out », *The New York Times*, éd. The New York Times Company, sect. New York times Book Review (12 juillet 1987), p. 36.

TRICOT, B., *Rapport de la Commission Informatique et Libertés*, Rapport de la commission informatique et libertés, 410, coll. La documentation française, Paris, Ministère de la Justice, 1975.

U.S. GOV., « The Digital 2 Dozen », *ustr.gov*, en ligne : <https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf>.

U.S. GOV., « The Digital Dozen », *ustr.gov*, en ligne : <https://ustr.gov/sites/default/files/USTR-The_Digital_Dozen.pdf>.

VIENNOT, L., « Internet, le conglomérat des réseaux », *Interstices.info* (17 novembre 2006), en ligne : <https://interstices.info/internet-le-conglomerat-des-reseaux/#:~:text=L%27internet%20est%20donc%20un,la%20destination%20%3A%20son%20adresse%20IP.>.

ZUBOFF, S., « Un capitalisme de surveillance », *https://www.monde-diplomatique.fr* (janvier 2019), en ligne : <https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443#:~:text=L%27industrie%20numérique%20prospère%20grâce,doit%20se%20changer%20en%20certitude.> (consulté le 28 avril 2022).

Documents internationaux

Déclaration ministérielle de Nairobi WT/MIN(15)/W/33/Rev.3, Organisation mondiale du commerce, 19 décembre 2015.

Déclaration conjointe sur le commerce électronique WT/MIN(17)/60, Organisation mondiale du commerce, 13 décembre 2017.

European Union's (EU) proposal for the EU-Australia FTA, Brussels, European Union, 2018, en ligne : <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf>.

EU proposal for provisions on Cross-border data flows and protection of personal data and privacy, Brussels, European Union, en ligne : <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf>.

Programme de travail sur le commerce électronique WT/MIN(17)/15/Rev.1, Organisation mondiale du commerce, 8 décembre 2017.