SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Quelles mesures spécifiques les États-Unis, l'UE et la Chine pourraient-ils prendre pour encourager et faciliter les flux de données transfrontaliers ?

Veronica Arroyo, Karin Hess

Nicole Grünbaum & Gustavo Ribeiro

Approche comparative de la réglementation des grandes entreprises technologiques (printemps 2023)

Professeur Florence G'sell

Avril 2023

Table des matières

LISTE DES ABRÉVIATIONS

Abréviation	Définition
API	Interfaces de programmation d'applications
BCR	Règles d'entreprise contraignantes
CAC	Administration du cyberespace de la Chine
CCP	Parti communiste chinois
CCPA	Loi californienne sur la protection de la vie privée des consommateurs
CFIUS	Commission sur les investissements étrangers aux États-Unis
CISA	Agence pour la cybersécurité et la sécurité des infrastructures
CLGISI	Groupe pilote central pour la sécurité et l'informatisation de l'Internet
CJUE	Cour de justice de l'Union européenne
COPPR	Règle sur la protection de la vie privée des enfants en ligne
CSL	Droit de la cybersécurité
DFI	Déclaration sur l'avenir de l'internet
DLR	Exigences en matière de localisation des données
DSL	Loi sur la sécurité des données
EDPB	Conseil européen de la protection des données
L'UE	Union européenne
EO	Décret exécutif
FISA	Loi sur la surveillance du renseignement étranger
FTA	Accord de libre-échange
FTC	Commission fédérale du commerce
FTZ	Zone de libre-échange
GDPR	Règlement général sur la protection des données

HIPAA	Loi sur la portabilité et la responsabilité en matière d'assurance maladie
PETs	Technologies d'amélioration de la protection de la vie privée
PIPL	Loi sur la protection des données personnelles
RPC	République populaire de Chine
RCEP	Partenariat économique régional global
CCN	Clauses contractuelles types
SIGINT	Renseignement sur les signaux
TEU	Traité sur l'Union européenne
TFUE	Traité sur le fonctionnement de l'Union européenne
É-U / USA	États-Unis
USTR	Bureau du représentant américain au commerce

Résumé

Cette note politique s'adresse aux ministres de l'économie numérique du G20 et aborde la question principale : **quelles mesures spécifiques les États-Unis, l'Union européenne et la Chine pourraient-ils prendre afin d'encourager et de faciliter les flux de données transfrontaliers ?** Pour ce faire, ce travail explore les principes et les logiques qui influencent la réglementation des flux de données et examine les instruments qui permettent aux données de circuler à travers les frontières de la République populaire de Chine, de l'Union européenne et des États-Unis d'Amérique.

Ce faisant, il fait le constat de points de convergence et de divergence. Les chevauchements entre l'UE et les États-Unis en matière de réglementation de la protection des données et de la vie privée sont limités. En outre, les deux politiques divergent de la Chine en ce qui concerne la sécurité nationale, car cette dernière dispose de moyens juridiques pour restreindre les flux de données transfrontaliers pour des raisons de sécurité. Le commerce des biens et services numériques est une priorité pour les trois pays.

Cette note politique conseille aux ministres de l'économie numérique du G20 d'**adopter des mesures stabilisatrices** telles que des référentiels, des normes et des clauses contractuelles types, et d'**explorer des mesures transformatrices** telles que des technologies renforçant la protection de la vie privée, des centres de données juridiquement adéquats dans les zones de libre-échange, et un tribunal ayant une compétence transnationale.

Introduction

Dans un monde de plus en plus numérique, les données sont devenues un atout stratégique pour les entreprises, les gouvernements et les organisations. Les entreprises s'appuient progressivement sur les données pour améliorer leurs opérations, gagner en efficacité et améliorer l'expérience des utilisateurs (The Economist, 2017), tandis que les gouvernements s'efforcent également de créer de la valeur publique grâce à des politiques publiques axées sur les données (OCDE, 2019 ; OCDE, 2014).

Les chaînes de valeur mondiales, dans lesquelles les processus sont fragmentés, sont également transformées par les données. Non seulement les biens et les services circulent au sein de ces chaînes de production mondiales, mais les données sont également inévitablement échangées. Comme le soulignent Casalini et al. (2021), "il est de plus en plus difficile pour une transaction commerciale internationale de se dérouler sans un quelconque transfert de données transfrontalier" (p.6). Les transferts de données deviennent vitaux pour les organisations, tant pour leurs fonctions commerciales internes que pour leurs interactions avec les fournisseurs, les prestataires et les clients. C'est pourquoi les flux transfrontaliers de données soulèvent des préoccupations en matière de respect de la vie privée, de sécurité et de protection des données, entre autres. Au cours des deux dernières décennies, les gouvernements ont réagi à ces tendances et un ensemble disparate de réglementations, de cadres juridiques et d'accords a créé un paysage difficile à naviguer pour les entreprises et les gouvernements.

D'une part, le pouvoir de marché de l'Union européenne (UE) associé à son règlement général sur la protection des données (RGPD, règlement (UE) 2016/679) l'a amenée à devenir une pionnière mondiale en matière de réglementation des données (Bradford, 2020). Sur le plan interne, la Commission européenne a lancé Une stratégie européenne pour les données (Commission européenne, 2020) dans le but de "concrétiser la vision d'un véritable marché unique des données" (p.11). D'autre part, les États-Unis "adoptent une approche décentralisée axée sur le marché pour leur stratégie numérique" (OCDE, 2017, p. 34). En effet, il manque encore un cadre fédéral, mais une forte pression citoyenne a conduit à des réglementations au niveau des États, plus particulièrement en Californie, au Colorado, au Connecticut, en Virginie et dans l'Utah (Desai, 2023). La République populaire de Chine (RPC) est un troisième acteur majeur, mais souvent négligé, de la scène internationale en matière de réglementation des données. Au cours des cinq dernières années, la RPC a introduit un certain nombre de nouvelles réglementations, notamment la loi sur la cybersécurité (CSL), la loi sur la protection des informations personnelles (PIPL), la loi sur la sécurité des données (DSL) et les dernières mesures relatives à l'évaluation de la sécurité des transferts transfrontaliers de données, dans le but d'établir un cadre de gouvernance des données contrôlé de manière centralisée.

Le débat sur le rôle de l'utilisation des données et des transferts de données est incontestablement urgent, contemporain et pertinent car "l'élaboration de règles sur les flux de données est difficile à séparer de la rivalité géopolitique" (WEF, 2023). En effet,

"[l]a propriété et le contrôle des flux de données sont devenus un domaine primordial de la concurrence entre les États-Unis et la Chine pour la supériorité économique et géopolitique" (Torreblanca, 2021, p.43). De même, le Digital Trade Restrictiveness Index révèle "que de nombreuses économies de premier plan imposent des restrictions significatives au commerce numérique" (Ferracane et al., 2018, p.4). En outre, ces derniers mois, l'application chinoise TikTok s'est retrouvée au cœur d'une bataille entre les États-Unis et la Chine concernant son utilisation des données (Criddle et al., 2023), et certains pays européens ont interdit à leurs fonctionnaires de l'utiliser (Le Monde, 2023). Alors que les entreprises tentent d'opérer dans les différents cadres réglementaires mis en place par la triade des pouvoirs, les gouvernements continuent de répondre à un scénario en constante évolution. En particulier, le nouveau cadre établi par la Chine limite les flux transfrontaliers sur la base de l'intérêt public et des préoccupations de sécurité nationale et, par conséquent, adopte une approche réglementaire de plus en plus restrictive.

À la lumière de ces nouveaux développements réglementaires et compte tenu de l'engagement pris par les ministres de l'économie numérique du G20 de "travailler à l'identification des points communs, des complémentarités et des éléments de convergence entre les approches et les instruments réglementaires existants permettant aux données de circuler en toute confiance" (G20 Indonésie, 2022), la présente note d'information examine la question suivante : quelles mesures spécifiques les États-Unis, l'Union européenne et la Chine pourraient-ils prendre afin d'encourager et de faciliter les flux de données transfrontaliers ?

Ce rapport vise à i) clarifier la fragmentation réglementaire qui est apparue en relation avec les flux de données transfrontaliers, ii) évaluer les enjeux pour chacune des trois politiques, iii) identifier les convergences ainsi que les divergences, et iv) fournir des recommandations sur les actions que le groupe de travail du G20 sur l'économie numérique peut envisager afin de faciliter les flux de données transfrontaliers.

À cette fin, le rapport est structuré comme suit. Le reste de la section 1 présente et fait suivre les définitions pertinentes. La section 2 présente le cadre de gouvernance des données de chaque pays, ainsi que les effets sur les flux de données transfrontaliers. La section 3 met en évidence les convergences et les divergences entre chaque pays dans trois domaines d'action qui influencent les flux de données transfrontaliers. La section 4 formule des recommandations au groupe de travail du G20 sur l'économie numérique sur la base des résultats précédents. La section 5 conclut.

1.1. Définitions

1.1.1. Flux de données transfrontaliers et gouvernance des données

La notion de "flux de données transfrontaliers" fait référence au "mouvement ou au transfert d'informations entre serveurs informatiques au-delà des frontières nationales" (Fefer, 2020, p.3). Les industries clés pour la croissance économique dépendent fortement des flux de données transfrontaliers, notamment les services d'information, la fabrication à haute valeur ajoutée, les services financiers et le commerce électronique, pour n'en citer que quelques-uns. Selon la dernière étude de McKinsey, "les flux de données ont atteint un niveau record" (Brishan et al, 2022) pendant et après

la pandémie de COVID-19 et ont augmenté de près de 50 % par an depuis 2010. Un secteur spécifique comme le commerce électronique transfrontalier a, selon le WEF (2023), été multiplié par 45 en dix ans pour atteindre un montant estimé à 2,7 billions de dollars.

Le concept de flux de données transfrontaliers est intrinsèquement lié à la notion de gouvernance des données. La gouvernance des données est définie comme "l'organisation et la mise en œuvre de politiques, de procédures, de structures, de rôles et de responsabilités qui définissent et appliquent des règles d'engagement, des droits de décision et des responsabilités pour la gestion efficace des actifs informationnels" (Ladley, 2012, p.11). Bien que les définitions puissent légèrement différer, la gouvernance des données suppose la mise en œuvre de politiques spécifiques par une autorité (gouvernements, entreprises ou organisations) afin de garantir la gestion adéquate de ses actifs de données. La réglementation des flux de données transfrontaliers s'inscrit donc dans le cadre de la gouvernance des données. Comme le montre le rapport, cette conceptualisation a un impact significatif sur les mesures prises par chaque entité politique[1] .

1.1.2. La classification des données

L'une des principales questions liées à la réglementation des données est la tâche difficile que représente leur classification. Comme le note l'OCDE, "les données sont parfois traitées comme une entité monolithique" (2020, p.12) mais, en réalité, elles sont hétérogènes. L'UE, les États-Unis et la Chine définissent les données de différentes manières, mais comme le montre la figure 1, des chevauchements peuvent être constatés. Il est essentiel de comprendre comment chaque État définit et classifie les différents types de données lorsque l'on tente d'interpréter les cadres de gouvernance.

[1] La notion de cybersécurité est un concept encore plus large, complexe et multidimensionnel. Comme le soulignent Craigen et al. (2014), le terme "est utilisé de manière large et ses définitions sont très variables, liées au contexte, souvent subjectives et, parfois, non informatives" (p.13). La loi américaine CISA la définit comme "l'art de protéger les réseaux, les dispositifs et les données contre un accès non autorisé ou une utilisation criminelle et la pratique consistant à assurer la confidentialité, l'intégrité et la disponibilité des informations". La loi sur la cybersécurité de l'UE (2019) la définit comme "les activités nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes concernées par les cybermenaces" (article 2.1). Enfin, la loi chinoise sur la cybersécurité l'entend comme un moyen de "prévenir les cyberattaques, les intrusions, les interférences, la destruction et l'utilisation illégale, ainsi que les accidents inattendus, de placer les réseaux dans un état de fonctionnement stable et fiable, et de garantir la capacité des données du réseau à être complètes, confidentielles et utilisables" (article 76). (Art. 76).

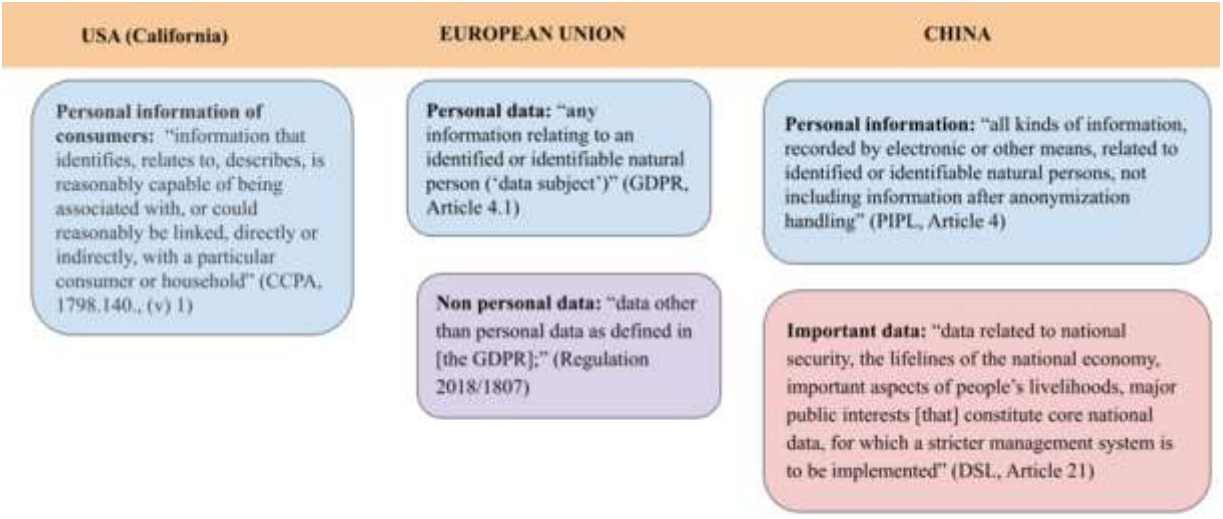


Figure 1: Definitions and classifications of data in the EU, US and China. Source: prepared by authors.

D'autres approches de la classification des données apportent plus de nuances qui pourraient faciliter la convergence des cadres de gouvernance. La classification de l'ISO (ISO/IEC 20889:2018), par exemple, propose un spectre de données comprenant les données identifiées, les données pseudonymisées, les données pseudonymisées non liées, les données anonymisées et les données agrégées. Comme le note l'OCDE, cette granularité peut "aider à évaluer le niveau de risque pour la vie privée et la confidentialité, qui à son tour peut aider à déterminer le degré auquel une protection juridique et technique peut être nécessaire, y compris le niveau de contrôle d'accès requis" (2020, p.14).

1.2. La fragmentation de la réglementation

1.2.1. Pourquoi les pays réglementent-ils les flux transfrontaliers de données ?

Les avantages économiques et sociaux des flux de données transfrontaliers sont largement documentés. Le Centre européen d'économie politique internationale explique qu'ils aident les entreprises à atteindre les marchés étrangers, à mieux accéder aux fournisseurs numériques et à accroître le bien-être des consommateurs en leur offrant un meilleur rapport qualité-prix et une plus grande variété de produits numériques (Ferracane et al., 2018, p.6). Néanmoins, les pays les réglementent de plus en plus, mais de manière fragmentaire. De nombreuses préoccupations sont en jeu, notamment la protection de la vie privée et des données, la sécurité nationale, les questions liées aux droits de propriété intellectuelle, "la portée réglementaire, la politique de la concurrence et la politique industrielle" (Casalini et al., 2021, p.4).

Les organisations et les forums internationaux ont tenté de relever les défis posés par cette prolifération et cette fragmentation réglementaires, mais des priorités concurrentes ont entravé la tâche[2] . L'OCDE a apporté quelques éclaircissements sur

[2] La difficulté de parvenir à un consensus s'est accrue dans les discussions de haut niveau, notamment dans le cadre du groupe de travail du G20 sur l'économie numérique. Le manque de clarté et de consensus a entraîné une duplication des termes, par exemple "Data Free Flow with Trust et Cross-Border Data Flows" dans les déclarations ministérielles. En outre, en 2022, la présidence indonésienne visait à rendre les concepts opérationnels et à convenir de "principes", mais les ministres se sont

ce sujet et publié deux rapports, "Mapping Approaches to Data and Data Flows" (2020) et "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers" (Casalini et al, 2021), dans le but d'identifier les éléments communs dans les instruments réglementaires "qui peuvent servir d'éléments de base pour rapprocher les différentes approches" (p.3). Cet exercice a constitué une première étape importante, mais la situation exige une recherche approfondie sur les valeurs et les principes qui sont en jeu pour chaque pays. Cela pourrait faciliter la voie vers une plus grande interopérabilité et une réduction de la fragmentation réglementaire.

1.2.2. Comment les pays réglementent-ils les flux de données transfrontaliers ?

En fonction de leurs objectifs politiques, de leurs préférences et du type de données en question, les pays ont développé différentes approches réglementaires des flux transfrontaliers, qui peuvent être classées en quatre catégories.

D'un côté, certains pays n'ont aucune réglementation sur les transferts de données et, par conséquent, les données peuvent être envoyées à l'étranger sans aucune restriction. D'autres imposent des mesures de responsabilité ex post pour l'exportateur de données "si les données envoyées à l'étranger sont mal utilisées" (Casalini et al., 2021, p.9), mais aucune exigence ex ante n'est établie. Une approche plus stricte implique des flux conditionnels à des garanties, qui comprennent "une série de conditions préautorisées et transparentes pour le transfert de données" (Casalini et al., p.9). Les conditions varient, mais se réfèrent généralement à l'adéquation ou à l'équivalence du pays où les données sont transférées. Dans les cas où "la détermination du caractère adéquat n'a pas encore été faite, les entreprises peuvent transférer des données dans le cadre d'options telles que des règles d'entreprise contraignantes ou des clauses contractuelles types ou approuvées" (p.9). Enfin, les pays les plus restrictifs ne permettent qu'une évaluation au cas par cas et des autorisations ad hoc.

Outre ces quatre grandes catégories, les exigences en matière de localisation des données peuvent également avoir une incidence sur les flux transfrontaliers de données, car l'interdiction du transfert de données implique que les données soient traitées et stockées localement. La figure 2 donne des exemples de chaque cas.

contentés de noter "la discussion entamée par la présidence indonésienne du G20 sur la légalité, l'équité et la transparence dans le contexte de ses "principes" proposés pour la libre circulation des données en toute confiance et les flux de données transfrontaliers" (G20 Indonésie, 2022).

Figure 2: Approaches to data flows regulation. Source: prepared by the authors based on Casalini et al. (2021)

Sur la base de ces cadres généraux, une prolifération d'instruments peut être identifiée (voir tableau 1), en particulier : i) les mécanismes unilatéraux, ii) les arrangements plurilatéraux, iii) les accords commerciaux et les partenariats, et iv) les initiatives axées sur les normes et les technologies.

INSTRUMENT	DESCRIPTION	TOOLS & EXAMPLES
Unilateral mechanisms	Domestic tools that enable data transfers abroad if certain conditions are met	- Open safeguards: *ex post* accountability principles, contracts or private sector-led adequacy decisions - Pre-authorized safeguards: public adequacy decisions and public sector-led *ex ante* safeguards - Standard Contractual Clauses - Binding Corporate Rules
Plurilateral arrangements	International instruments that create rules around cross-border transfers of specific types of data, often on the basis of alignment on underlying principles	- Convention 108 of the Council of Europe - African Union Convention on Cyber Security and Personal Data Protection → usually occur in the context of personal data protection and privacy → enforcement depends on whether they are binding
Trade agreements	Contractual arrangement between countries concerning their trade relationships. They can incorporate provisions on data transfers.	- United States - Mexico - Canada Agreement - Framework Agreement on China-ASEAN Comprehensive Economic Cooperation - EU- MERCOSUR
Standards and technology-driven initiatives	Initiatives from private or non-governmental organizations	- ISO standards

Table 1: instruments that regulate cross-border data flows. Source: authors' production based on Casalini et al. (2021)

Bien que le paysage soit complexe et varié, certains chercheurs envisagent une "tendance mondiale claire vers une convergence croissante" (Şimşek, 2021). En ce sens, l'identification des valeurs et des principes auxquels chaque pays accorde la priorité pourrait être la prochaine étape pour transcender la cartographie des instruments communs et identifier les éventuelles convergences fondées sur des principes.

2. Quels sont les enjeux pour chaque polarité ?

Cette section présente des éléments de réglementation, des stratégies politiques et des actes qui donnent un aperçu des intérêts que chaque acteur cherche à promouvoir et à sauvegarder dans le contexte des transferts transfrontaliers de données, tels que la sécurité nationale, le libre-échange et la protection de la vie privée.

2.1. La Chine

"Il n'y a pas de sécurité nationale sans cybersécurité" (没有网络安全没有国家安全) a déclaré Xi Jinping, secrétaire général du Parti communiste chinois (PCC) et président de la RPC, lors de la Semaine nationale de sensibilisation à la cybersécurité 2022 (People's Daily, 2022). Cela résume les deux logiques de la Chine en tant que régulateur : au niveau national, maintenir le contrôle et la surveillance de tous les types de données - qu'elles soient industrielles, financières, personnelles, etc. - et sur le plan international, pour mettre en place un cadre de gouvernance de la sécurité qui permette, avant tout, de préserver la sécurité nationale. L'État chinois estime que les moyens fondés sur les données, tels que les flux transfrontaliers de données, pourraient nuire gravement à ses intérêts nationaux et adopte donc des réglementations en conséquence. En limitant les flux transfrontaliers de certains types de données, la Chine adopte une approche réglementaire de plus en plus restrictive et au cas par cas. Pourtant, sous prétexte de soutenir le commerce pour la croissance économique, elle expérimente simultanément des zones pilotes de libre transfert transfrontalier et des dispositions facilitant le transfert dans les accords de libre-échange (ALE).

2.2.1 Le cadre de gouvernance des données en Chine

Depuis 2016, la gouvernance des données revêt une importance capitale. Cette année-là, la première législation du cadre évolutif de la cybersécurité en Chine a été promulguée, le "中华人民共和国网络安全法" (loi sur la cybersécurité, CSL). Cette législation est supervisée par le Central Leading Group for Internet Security and Informatization (CLGISI), un organe chargé de la formulation des politiques qui rend compte aux organes les plus élevés du PCC et/ou de l'appareil d'État, notamment le Comité permanent du Politburo et le Conseil d'État (Chan, 2018). Ce double rattachement au Parti et à l'État reflète le parallélisme du système de gouvernance de la RPC et montre en outre l'importance accordée à la gouvernance du numérique et des données. Le principal régulateur chinois du cyberespace est la Cyberspace Administration of China (CAC) qui opère sous l'égide du CLGISI susmentionné. En outre, cette année, l'Assemblée nationale populaire (ANP) a adopté une série de réformes, dont la création d'un Bureau national des données chargé de centraliser la gestion des ressources en données dans tout le pays (People's Daily, 2023).

La LSC peut être résumée comme une législation visant à défendre la sécurité nationale et les droits des citoyens chinois à l'intérieur de la RPC et à l'étranger, comme le montre l'article 1 : "assurer la cybersécurité ; sauvegarder la souveraineté du cyberespace et la sécurité nationale, ainsi que les intérêts sociaux et publics [...]" (NPC, 2016). Pour ce faire, la législation vise à établir une distinction entre les opérateurs

d'infrastructures d'information "critiques" et "non critiques". Les "infrastructures d'information critiques" sont définies comme suit : "si elle est détruite, si elle subit une perte de fonction ou si elle connaît une fuite de données susceptible de mettre gravement en péril la sécurité nationale, le bien-être national, les moyens de subsistance de la population ou l'intérêt public" (article 31). Ainsi, le premier doit "se conformer à la gestion de la sécurité sortante en ce qui concerne le traitement des données importantes" (article 37). La CSL ne précise pas quel type de données est concerné par cette terminologie, laissant à la législation ultérieure le soin de le faire.

Pour clarifier davantage la protection des données, deux nouvelles lois sont entrées en vigueur en 2021 : la loi sur la sécurité des données (中华人民共和国数据安全法) et la loi sur la protection des informations personnelles (PIPL) (中华人民共和国数据安全法), DSL) et la "中华人民共和国个人信息保护法" (loi sur la protection des informations personnelles, PIPL). La DSL définit les données importantes (重要数据) comme "les données liées à la sécurité nationale, aux lignes de vie de l'économie nationale, aux aspects importants des moyens de subsistance des personnes, aux intérêts publics majeurs, etc.", et qu'elles "constituent des données nationales essentielles, pour lesquelles un système de gestion plus strict doit être mis en œuvre" (NPC, 2021a, Art. 21). En outre, les départements régionaux devraient être autonomes dans la définition du champ des données importantes et les répertorier dans un catalogue.

La PIPL (2021) définit les informations personnelles (个人信息) à l'article 4 comme "toutes sortes d'informations, enregistrées par des moyens électroniques ou autres, liées à des personnes physiques identifiées ou identifiables, à l'exclusion des informations après traitement d'anonymisation" (NPC, 2021b), ce qui est analogue à la définition utilisée dans le GDPR. Bien que l'application puisse différer, sur le plan normatif, la PIPL réglemente le traitement par les grandes entreprises technologiques, telles que Tencent ou Alibaba, ainsi que par les organes de l'État, avec certaines spécificités et exceptions pour ces derniers, comme indiqué à la section 3 (Horsley, 2021).

La LIS (2021), quant à elle, tente de prévenir les atteintes à la sécurité nationale et à l'intérêt public causées par des moyens fondés sur les données, y compris les flux de données transfrontaliers. Une telle catégorisation des données importantes, qui peuvent englober des informations personnelles, constitue, selon les principaux spécialistes du domaine, une innovation considérable (Creemers, 2022). La controverse autour du service chinois de covoiturage Didi Chuxing "滴滴出行", coté à New York, qui a été utilisé pour accéder à des sites ministériels sensibles, en est un exemple. Les régulateurs chinois sont intervenus dans les activités commerciales de Didi par crainte que ces données ne soient divulguées aux autorités américaines (Xinhua, 2021). Par conséquent, le gouvernement chinois estime qu'il est absolument nécessaire de réglementer, car le transfert de données importantes à des acteurs étrangers est considéré comme une menace potentielle pour la sécurité nationale.

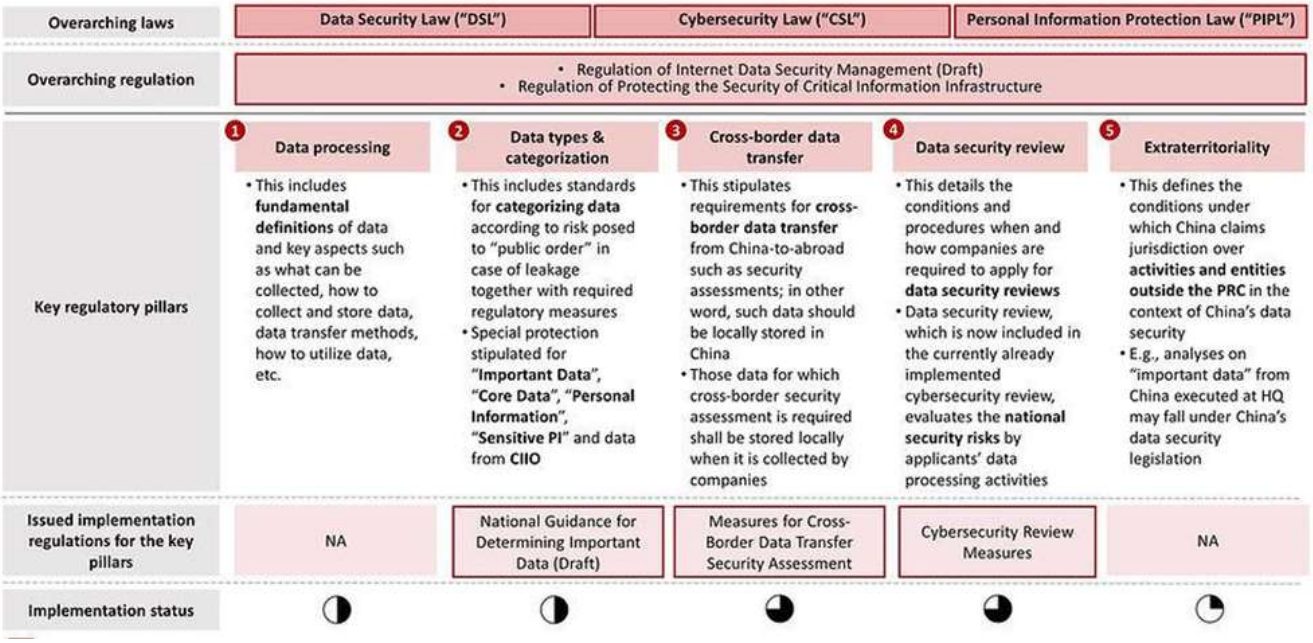


Figure 3 - Illustration du cadre de gouvernance des données de la PRC. Source : China Macro Group (2022) China Macro Group (2022)

2.2.2. Règles spécifiques pour les flux de données transfrontaliers

En ce qui concerne les flux de données, l'article 11 de la LIS souligne que l'État doit promouvoir la sécurité des flux transfrontaliers de données importantes (出境安全管理), ce qui signifie que des mesures de sécurité doivent être appliquées si des données importantes doivent être transférées en dehors de la RPC (article 21). De même, le chapitre 3 de la PIPL contient des dispositions sur la manière dont les informations personnelles doivent être traitées dans le cadre de transferts transfrontaliers. Selon l'article 38, la partie qui effectue le transfert doit : "passer une évaluation de sécurité, obtenir une certification de protection des informations personnelles, conclure un contrat avec le destinataire étranger" ou bénéficier "d'autres conditions", qui ne sont pas précisées.

Le cadre chinois de gouvernance de la sécurité des données doit être considéré comme une structure évolutive. Ainsi, les "数据出境安全评估办法" (Mesures pour l'évaluation de la sécurité des transferts transfrontaliers de données, les Mesures), promulguées en juin 2022 (CAC), constituent une autre pièce du puzzle pour préciser la terminologie et la procédure. En effet, les Mesures demandent aux entreprises qui collectent ou produisent par le biais d'opérations des "données importantes" (Art. 19) ou des "informations personnelles" - définies en termes quantitatifs comme (i) des informations personnelles sur plus de 100 000 personnes ou (ii) des informations personnelles sensibles sur plus de 10 000 personnes - une évaluation substantielle de la sécurité si elles veulent fournir ces données à l'étranger.

Le tableau 2 résume les étapes et les descriptions correspondantes de l'évaluation de la sécurité, conformément à l'article 5 des mesures.

Étapes	Description
1. Réalisation d'une évaluation des risques liés au transfert de données sortantes	Les responsables du traitement des données - y compris la collecte, le stockage, l'utilisation, la modification, la transmission, la fourniture, la divulgation, la suppression, etc. (NPC, 2021b) - doivent procéder à une évaluation des risques liés au transfert de données vers l'extérieur, par exemple en ce qui concerne la manière dont ces transferts peuvent porter atteinte à la sécurité nationale et à l'intérêt public.
2. Présentation de la demande d'évaluation de la sécurité	La demande auprès du département national de la cybersécurité et de l'informatisation est soumise par l'intermédiaire du département provincial.
3. Documentation juridique	Les responsables du traitement des données doivent conclure avec le destinataire étranger un document juridique sur la finalité, les limites de portée et de temps ainsi que les mesures correctives (article 9).
4. Réalisation d'une évaluation de la sécurité	Si la demande est acceptée, le département national de la cybersécurité et de l'informatisation confie à un tiers le soin de procéder à l'évaluation de la sécurité (dans un délai de 45 jours ouvrables).
5. Les prochaines étapes	En fonction du résultat, les responsables du traitement des données peuvent présenter une nouvelle demande d'évaluation de la sécurité dans un délai de 15 jours ouvrables. S'ils réussissent, ils bénéficieront de flux de données "gratuits" pendant deux ans.

Tableau 2 : Évaluation de la sécurité par la Chine. Source : production des auteurs sur la base des mesures (CAC, 2022)

Étant donné que les mesures d'évaluation de la sécurité n'ont été adoptées que très récemment, il existe peu de précédents en matière d'application. Toutefois, en janvier 2023, une étude sur le traitement du cancer menée conjointement par des chercheurs

d'Amsterdam et de Pékin a été le premier projet à passer le contrôle de sécurité (Zhou et al., 2023). Néanmoins, la plupart des entreprises européennes adoptent une approche conservatrice, soit en localisant leurs données, soit en restant dans l'expectative, car de nombreux termes des mesures restent imprécis (Arcesati, 2022).

Jusqu'à présent, la RPC a signé 17 ALE, mais seuls six d'entre eux contiennent des dispositions relatives au commerce électronique (MOFCOM, 2023). Il convient de noter que l'ALE signé en 2015 avec la Corée du Sud comporte, dans ses lignes directrices pour les négociations ultérieures, une disposition relative au "transfert d'informations" (annexe 22A). En outre, le Partenariat économique régional global (RCEP) stipule les normes prohibitives sur la localisation des données (art. 12.14 ; 12.15), tout en autorisant des clauses d'exception (RCEP, 2020). Ces deux éléments indiquent une tendance future à inclure les flux de données transfrontaliers dans les négociations et les mises à niveau des ALE. Le cadre réglementaire chinois le permet. Par exemple, l'article 38 de la PIPL (NPC, 2021b) stipule que si les traités et les accords internationaux "[...] contiennent des dispositions pertinentes telles que des conditions sur la fourniture de données à caractère personnel en dehors des frontières de [la RPC], ces dispositions peuvent être mises en œuvre [...]".

En outre, la Chine pilote la libre circulation transfrontalière des données dans certaines zones de libre-échange (FTZ), ce qui constitue un terrain d'essai où différentes politiques et réglementations sont autorisées afin de promouvoir la croissance économique. Par exemple, la zone franche de l'île de Hainan est destinée à devenir une plaque tournante internationale pour les flux de données transfrontaliers sous la supervision du président Xi (gouvernement de Hainan, 2023).

2.2. L'Union européenne

L'UE accorde une grande importance à la protection des données en tant que droit fondamental (article 8 de la Charte des droits fondamentaux). Toutefois, cette importance est contrebalancée par la "libre circulation des biens, des personnes, des services et des capitaux" au niveau interne (article 26 du TFUE) et par la poursuite d'un "commerce libre et équitable" au niveau externe (article 3, paragraphe 5, du TUE). Elle opte donc pour une approche plus stricte des flux de données.

2.2.1. Le cadre de gouvernance des données de l'Union européenne

La création de l'Union européenne a été source d'opportunités et de défis. Elle a permis à ses États membres de constituer un marché intérieur avec une libre circulation des biens, des services, des capitaux et des personnes (Traité sur l'Union européenne, 2007, article 3(3)). En tant que plus grand marché unique, l'UE est devenue un acteur international du commerce et se présente comme "le plus grand bloc commercial du monde" (Commission européenne, n.d.). Jusqu'à présent, l'UE est le premier partenaire commercial de 80 pays et a signé de nombreux accords commerciaux avec des pays tiers dans le monde entier (Commission européenne, n.d.).

Néanmoins, ces projets ont créé des défis pour les droits et libertés fondamentaux, en particulier le droit à la vie privée (Charte des droits fondamentaux de l'Union européenne, 2012, art. 7) et la protection des données personnelles (art. 8).

L'importance du contrôle des informations concernant les personnes n'est pas nouvelle dans l'UE. Elle remonte à 1978, lorsque l'Allemagne a promulgué la première loi fédérale sur la protection des données (Bundesdatenschutzgesetz - BDSG) et a établi les principes de base de la protection des données, tels que l'exigence du consentement de la personne concernée pour le traitement des données à caractère personnel.

Il est donc nécessaire de trouver un équilibre entre les droits et libertés concernant ces biens d'information et la promotion du marché intérieur.

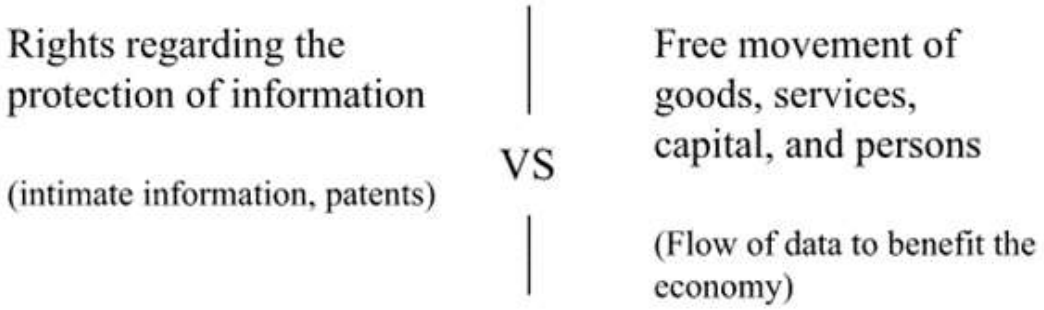


Figure 3 - Équilibre entre les droits et les libertés dans l'UE. Source : préparée par les auteurs

Pour comprendre comment ces droits et libertés souvent contradictoires sont équilibrés, il est important de souligner que l'UE a été construite sur trois principes fondamentaux qui ont apporté certitude et efficacité dans la résolution de problèmes complexes.

Renvoi	"L'Union n'agit que dans les limites des compétences que les États membres lui ont attribuées dans les traités pour atteindre les objectifs de ceux-ci. Les compétences qui ne sont pas attribuées à l'Union dans les traités restent du ressort des États membres"	Article 5, paragraphe 2, du TUE
Proportionnalité	"Le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités.	Article 5, paragraphe 4, du TUE
Subsidiarité	"Dans les domaines qui ne relèvent pas de sa compétence exclusive, l'Union n'intervient que si et dans la mesure où les objectifs de l'action envisagée ne peuvent pas être réalisés de manière suffisante par les États membres.	Article 5, paragraphe 3, du TUE

Tableau 3. Principes fondamentaux de l'UE. Source : préparé par les auteurs sur la base du TUE

Pour traiter les données, l'UE et les États membres ont adopté de nombreux documents juridiques, le dernier en date étant la stratégie européenne pour les données (Commission européenne, 2020a). Son objectif est de définir clairement la voie à suivre pour faire de l'UE un leader dans une société fondée sur les données. La stratégie présente la vision d'un marché unique des données qui permet aux données de circuler librement au sein de l'UE, tout en protégeant les droits relatifs aux données personnelles et aux données non personnelles (Commission européenne, 2020a). En ce qui concerne spécifiquement les flux de données, elle opte pour une approche ouverte et affirmée fondée sur les valeurs européennes (Commission européenne, 2020a). En d'autres termes, elle propose un équilibre clair entre la libre circulation et les droits.

En ce qui concerne les données personnelles, les États membres coopèrent avec les institutions de l'UE pour maintenir un cadre de protection basé sur la Charte des droits fondamentaux. En tenant compte du principe de subsidiarité, l'UE a adopté le règlement général sur la protection des données (RGPD) afin d'assurer l'homogénéité de la protection des données. Avant le GDPR, la directive 95/46/CE ne fournissait que des orientations sur la manière de réglementer le sujet en interne ; en conséquence, chaque État membre a adopté des lois avec des mécanismes de protection et de conformité différents. En outre, le GDPR comporte de nombreuses exceptions et dispositions spéciales visant à faciliter les flux internationaux de données en dehors de l'UE sans porter atteinte au droit à la protection des données.

En ce qui concerne les données non personnelles, telles que la propriété intellectuelle, les États membres partagent également la compétence réglementaire avec l'UE. Toutefois, comme indiqué dans les sections suivantes, les lois nationales jouent un rôle important lorsqu'il s'agit de fixer des limites aux règles de l'UE. Au sein de l'UE, la loi sur la gouvernance des données (Commission européenne, 2020b) et le règlement relatif à un cadre pour la libre circulation des données non personnelles (règlement (UE) 2018/1807) couvrent principalement la manière dont les données doivent être partagées entre les États membres et les secteurs privés. Une prochaine loi sur les données (Commission européenne, 2022a) fournira des règles sur l'utilisation des données dans tous les secteurs, y compris des dispositions sur les flux internationaux de données en dehors de l'UE, et précisera qui peut créer de la valeur à partir des données et dans quelles conditions.

2.2.2. Les règles spécifiques pour les flux de données transfrontaliers

Comme indiqué ci-dessus, le GDPR (articles 45, 46 et 49) et le projet de loi sur les données (article 27) contiennent des dispositions permettant les flux internationaux de données de l'UE vers des pays tiers. Pour les flux de données des pays tiers vers l'UE, la règle générale est qu'une fois que les données sont traitées dans l'UE, toutes les règles internes s'appliquent, y compris les accords commerciaux de l'Organisation mondiale du commerce et d'autres accords bilatéraux. Même les cas spécifiques de sécurité nationale et de coopération judiciaire sont régis par des règles et des exceptions internes, ainsi que par des traités sur mesure.

2.2.2.1. Données personnelles - GDPR

Il convient de mentionner que le "flux de données" international est interprété non seulement comme le mouvement des données de l'UE vers un pays tiers, mais aussi comme leur traitement dans un pays tiers (Ustaran, 2019, p. 296). Par exemple, l'acheminement de paquets de données ne relève pas du champ d'application du GDPR. En outre, les responsables du traitement des données qui doivent se conformer au GDPR sont ceux qui sont établis dans l'UE, ainsi que ceux qui offrent des biens ou des services ou surveillent le comportement des personnes dans l'UE.

Le GDPR mentionne le cas spécifique de la sécurité nationale et publique en précisant qu'ils sont hors du champ d'application du règlement. Toutefois, ces deux sujets pourraient renforcer les règles existantes ou être utilisés pour créer des règles spécifiques, appliquées dans le contexte des transferts transfrontaliers de données. Ainsi, l'article 23 du GDPR prévoit que les États membres et l'UE peuvent adopter des règles spécifiques dans les cas où la sécurité de l'État, la défense et la sécurité publique sont en jeu. En outre, l'article 48 mentionne que les transferts demandés par une institution judiciaire d'un pays tiers sont généralement couverts par des accords internationaux tels que le traité d'entraide judiciaire. Ce sujet est développé par la directive (UE) 2016/680.

Le GDPR s'articule autour de six principes[3] et fixe des obligations aux responsables du traitement des données et aux États membres. En outre, le cadre juridique est supervisé par des autorités indépendantes dans les États membres et par des organes spécifiques au niveau de l'UE. Les dispositions relatives aux flux transfrontaliers de données figurent au chapitre 5. Son application suit une logique subsidiaire, ce qui signifie que si la première option ne s'applique pas à l'affaire, la deuxième option devient disponible. Suivant l'esquisse de Casalini et al. (2021), l'UE a globalement opté pour une approche plus stricte fixant des conditions ex ante pour les flux de données.

En premier lieu, le responsable du traitement doit vérifier si le pays tiers a obtenu une décision d'adéquation (article 45). Seuls 14 pays[4] ont obtenu cette décision à ce jour, tandis que la Chine et les États-Unis ne bénéficient pas de ce statut. Pour figurer sur la liste d'adéquation, la Commission évalue si l'autorité de protection des données est indépendante et si le pays tiers participe à des systèmes régionaux de protection des droits de l'homme.

Cas : Transfert transatlantique de données entre les États-Unis et l'Union européenne

Entre 1998 et 2000, la Commission européenne et le ministère américain du commerce ont élaboré les principes de la sphère de sécurité, un instrument ad hoc. En 2000, la Commission européenne a adopté la décision 2000/520/CE déclarant que ces principes offraient une protection adéquate pour permettre les transferts de données à

[3] (1) la légalité, l'équité et la transparence, (2) la limitation des finalités, (3) la minimisation des données, (4) l'exactitude, (5) la limitation du stockage, (6) l'intégrité et la confidentialité.

[4] Ces pays sont Andorre, l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernesey, Israël, l'île de Man, le Japon, Jersey, la Nouvelle-Zélande, la République de Corée, la Suisse, le Royaume-Uni et l'Uruguay.

caractère personnel vers les États-Unis. Toutefois, en 2015, la CJUE a déclaré la sphère de sécurité invalide (affaire Schrems I, Maximillian Schrems contre le commissaire à la protection des données). Parallèlement, il existait un bouclier de protection de la vie privée UE-États-Unis (décision (UE) 2016/1250), que la CJUE a déclaré invalide en 2020 (affaire Schrems II, Maximillian Schrems/Commissaire à la protection des données). Cette décision a été prise en raison des préoccupations concernant les activités de surveillance des États-Unis par les entreprises et le gouvernement, et des moyens inadéquats pour les citoyens de l'UE de faire respecter leurs droits garantis par le GDPR. Depuis lors, le dernier effort en date a été l'initiative d'un cadre transatlantique de protection des données personnelles. En mars 2022, l'UE et les États-Unis se sont mis d'accord sur le principe et travaillent actuellement sur des projets visant à transformer l'initiative en texte juridique (Commission européenne 2022b). Le futur cadre devrait permettre la libre circulation des données, fixer des règles et des garanties pour contrôler l'accès aux données par les agences de renseignement américaines, établir un système de recours pour les Européens, des obligations pour les entreprises de traitement des données qui reçoivent des données de l'UE, et des mécanismes de contrôle.

Si la première option n'est pas disponible, le responsable du traitement peut transférer des données à caractère personnel s'il offre l'une des garanties appropriées suivantes (article 46) :

Clauses types de protection des données approuvées par la Commission (art. 93)	Les clauses incorporées dans les contrats contiennent des dispositions visant à assurer une protection adéquate des données à caractère personnel. Son application pratique est supervisée par la Commission européenne. En 2021, la Commission a publié la décision (UE) 2021/9 qui fixe les clauses contractuelles.
Un mécanisme de certification approuvé (art. 42)	Le responsable du traitement dans un pays tiers peut obtenir une certification par un organisme de certification agréé. La certification prouve que le responsable du traitement des données se conforme au GDPR et dure 3 ans. La certification ne supprime pas les autres obligations prévues par le GDPR (European Data Protection Board, 2019).
Règles d'entreprise contraignantes (BCR) (article 47)	Il s'agit de règles internes de protection de la vie privée approuvées par l'autorité de protection des données. Ces règles permettent à une entreprise de transférer des données entre différentes juridictions, mais créent en même temps une obligation de conformité.

Un code de conduite approuvé (art. 40)	Il s'agit d'un document qu'un responsable du traitement des données dans un pays tiers peut adopter. Le code doit contenir des principes, des droits, des obligations basées sur le GDPR et des mesures spéciales en fonction du contexte du pays. En outre, le responsable du traitement des données doit signer des engagements exécutoires. (Comité européen de la protection des données, 2022)
Un instrument juridiquement contraignant et exécutoire entre des autorités ou des organismes publics	Les accords bilatéraux/multilatéraux qui garantissent que les données transférées vers un pays tiers bénéficieront d'une protection similaire à celle de l'UE. Les thèmes de ces accords entrent dans le champ d'application du GDPR, par exemple la sécurité nationale est exclue. (Comité européen de la protection des données, 2020)

Tableau 4. Garanties appropriées pour les transferts

Enfin, si le sous-traitant ne peut satisfaire à aucune de ces garanties, la dernière option consiste à examiner les exceptions spécifiques énumérées à l'article 49[5] .

2.2.2.2. Données non personnelles - Proposition de loi sur les données

Globalement, la proposition vise à permettre aux différents acteurs d'extraire la valeur des données non personnelles et à les inciter à le faire, en créant des règles harmonisées sur l'accès et l'utilisation équitables des données (article 1). Elle vise donc à répondre aux préoccupations concernant le transfert de données vers des pays tiers. En outre, la proposition indique clairement qu'elle n'affecte pas les règles spéciales applicables aux transferts internationaux de données liés à la sécurité publique, à la défense et à la sécurité nationale (article 1.4).

Comme le GDPR, il propose un modèle de fixation de conditions ex ante pour les flux de données transfrontaliers, tout en respectant l'existence d'accords internationaux. Les dispositions pertinentes sur le transfert de données non personnelles en dehors de l'UE figurent au chapitre VII, article 27. La loi sur les données est encore à l'état de projet et il reste donc un long processus à suivre pour mener à bien cette proposition.

L'article 27 intègre une approche fondée sur les risques. La Commission européenne comprend que les flux internationaux de données non personnelles pourraient potentiellement mettre en péril des questions importantes telles que les droits fondamentaux, les voies de recours, la sécurité nationale, les données commercialement sensibles et les droits de propriété intellectuelle (considérant 77). Ces questions sont normalement réglementées et protégées au niveau national et au

[5] Le responsable du traitement ne peut soutenir le flux de données qu'avec le consentement (spécifique, éclairé et explicite), des contrats, un intérêt public important, des revendications légales, un intérêt vital, si les données à caractère personnel figurent dans un registre public, ou si le transfert n'est pas répétitif.

niveau de l'UE par différents instruments juridiques tels que les engagements commerciaux de l'Organisation mondiale du commerce, l'Accord général sur le commerce des services et d'autres accords commerciaux (exposé des motifs). Par conséquent, la loi invite les fournisseurs de services de traitement de données à prendre des mesures raisonnables pour empêcher les flux internationaux de données à caractère non personnel affectant le droit de l'Union ou le droit national.

En outre, l'article 27, chiffres 2 et 3, traite des demandes d'accès aux données à caractère non personnel par les autorités judiciaires ou administratives d'un pays tiers. Selon la proposition, cela ne pourrait être possible que par le biais d'un accord international, tel que les traités d'entraide judiciaire. En l'absence d'un tel accord, la proposition mentionne une série de possibilités. Par exemple, le système des pays tiers exige que les motifs et la proportionnalité de la demande de transfert soient spécifiques. Dans les cas où le transfert et l'accès sont demandés par une autorité d'un pays tiers, les données transférées doivent être le minimum possible et le détenteur des données doit être notifié lorsque cela est possible.

2.3. États-Unis

Anu Bradford (2021) explique que le modèle américain de gouvernance numérique " [...] est centré sur l'idée de protéger la liberté d'expression, l'internet libre et les incitations à l'innovation [et] fait partie de l'idéologie plus large [...] qui embrasse les marchés et fait moins confiance à la capacité d'intervention du gouvernement ". Pour ces raisons, les États-Unis ont fortement plaidé en faveur de la libéralisation des flux de données transfrontaliers en qualifiant leur restriction d'obstacle au commerce (USITC, 2013, chapitre 5). Inversement, ils reconnaissent que cette libre circulation implique des compromis en matière de protection de la vie privée et de sécurité nationale.

2.3.1. Cadre de gouvernance des données aux États-Unis

Tout d'abord, le libre-échange numérique sous-tend la logique américaine en matière de flux de données transfrontaliers. Ce dernier est constitué de l'ensemble du "commerce effectué par des moyens électroniques et comprend le commerce de biens et de services" (Trachtenberg, 2023). La libéralisation du commerce numérique international soutient les arguments américains en faveur de la libre circulation transfrontalière des données (Selby, 2017). Dans cette logique, la principale motivation du pays est son gain économique dans l'économie numérique. En 2019, celle-ci représentait 9,6 % de son PIB (Akhtar & Sutherland, 2021, p.1) et, en 2012, elle représentait un excédent de 117 milliards USD dans le commerce numérique (Selby, 2017). En effet, dans le cadre de la Trade Promotion Authority (Public Law 114-26, 2015), le Congrès a attribué au président les pouvoirs de négocier des accords commerciaux. L'un de ses principaux objectifs était de "veiller à ce que les gouvernements s'abstiennent de mettre en œuvre des mesures liées au commerce qui entravent le commerce numérique de biens et de services, restreignent les flux de données transfrontaliers ou exigent un stockage ou un traitement local des données".

Ces dernières années, les États-Unis ont suivi une politique cohérente de libéralisation du commerce numérique. Par exemple, l'article 15.8 de l'accord de libre-échange entre

les États-Unis et la Corée du Sud interdit les obstacles inutiles à la circulation transfrontalière des données, tout en reconnaissant "l'importance de la protection des informations personnelles" (Chin & Zhao, 2022, p.4). De même, l'accord sur le commerce numérique entre les États-Unis et le Japon et l'accord de libre-échange entre les États-Unis, le Mexique et le Canada (USMCA) (i) interdisent les restrictions à la circulation et à la localisation des données ; (ii) limitent la responsabilité des intermédiaires pour les contenus générés par les utilisateurs ; et (iii) prévoient des mesures de protection des consommateurs (Trachtenberg, 2023, p.2).

Deuxièmement, la liberté d'expression influence également la gouvernance des données. Aux États-Unis, ce droit découle du premier amendement : "Le Congrès ne fera aucune loi (...) qui restreigne la liberté d'expression" (US Const., 1791). En conséquence, la "Déclaration sur l'avenir de l'internet" (DFI) de Joe Biden (2022) présente un internet mondial où les données circulent librement comme nécessaire pour favoriser des sociétés dans lesquelles "la technologie est utilisée pour promouvoir le pluralisme et la liberté d'expression".

Troisièmement, la Cour suprême a reconnu à plusieurs reprises que la vie privée est un droit constitutionnel qui découle systématiquement des premier, troisième, quatrième et neuvième amendements (Griswold v. Connecticut, 1965 ; voir également : Riley v. California, 2014 ; Carpenter v. United States, 2018). Son cadre juridique est néanmoins fragmenté entre la législation fédérale et celle des États.

Au niveau fédéral, la protection est segmentée. D'une part, la Children's Online Privacy Protection Rule (COPPR, 2013) exige des opérateurs en ligne qu'ils respectent un ensemble d'obligations pour protéger les informations personnelles des enfants de moins de treize ans. Deuxièmement, la loi HIPAA (Health Insurance Portability and Accountability Act) exige que les entités de soins de santé et les entreprises associées "protègent les informations sensibles relatives à la santé des patients contre toute divulgation à l'insu du patient ou sans son consentement" (CDC, 2022 ; HHS, 2022a). Troisièmement, l'article 5 de la loi sur la Commission fédérale du commerce (Federal Trade Commission Act, FTC Act) confère à la FTC des pouvoirs étendus pour interdire les pratiques "déloyales ou trompeuses" dans ou affectant le commerce, y compris les déclarations trompeuses et les préjudices concernant la sécurité des données, les consommateurs et la protection de la vie privée (FTC Act, 1914 ; FTC, n.d. ; FTC v. Wyndham Worldwide Corp., 2015).

Au niveau des États, le Connecticut, le Colorado, l'Utah, la Virginie et la Californie ont adopté des lois complètes sur la protection de la vie privée (IAPP, 2023), cette dernière étant la plus influente. En effet, le California Consumer Privacy Act (CCPA, 2020) s'applique à toute entreprise traitant des données de résidents californiens, quel que soit leur lieu de résidence, et ses normes réglementaires ont un effet de facto et de jure au-delà des frontières de l'État (Chander et al., 2021). En bref, la CCPA attribue des droits et des devoirs dans le but de "donner aux consommateurs le contrôle des informations personnelles que les entreprises collectent à leur sujet". En conséquence, la politique de l'exécutif américain a toujours reconnu que la circulation des données et la protection de la vie privée devaient être mises en balance. L'administration Obama a fait de la protection de la vie privée des consommateurs une valeur fondamentale de la stratégie "Digital 2 Dozen" pour le commerce numérique (USTR, 2016). De même,

le DFI de Biden (2022) met en avant la "[protection de] la vie privée des individus [tout en résistant] aux efforts visant à diviser l'Internet mondial et [en promouvant] une économie mondiale libre et compétitive".

Quatrièmement, la sécurité nationale et l'application de la loi sont des raisons qui justifient à la fois la promotion et la restriction des flux de données transfrontaliers. D'une part, les flux permettent aux services de renseignement américains d'agir. Selby (2017) explique que les États-Unis détiennent un avantage comparatif en matière d'hébergement de données. Ceci, à son tour, contribue à l'"avantage comparatif du gouvernement américain pour ses agences de renseignement d'origine électromagnétique (SIGINT) dans leurs économies de surveillance des données en ligne par rapport à [celles des] agences SIGINT étrangères" (p.215-216). En effet, la section 702 du Foreign Intelligence Surveillance Act (FISA) autorise les agences américaines à mener une "surveillance ciblée de personnes étrangères situées en dehors des États-Unis" (ODNI, n.d.). De même, l'Executive Order 12333 (EO, 1981) couvre "la collecte par les autorités de surveillance américaines de données stockées ou transitant en dehors des frontières géographiques des États-Unis" (Hoffman, 2021, p.590). Enfin, l'application de la loi joue également un rôle. Le Clarifying Lawful Overseas Use of Data Act (CLOUD Act) impose aux services électroniques de "divulguer toutes les données en leur possession, sous leur garde ou sous leur contrôle, [...], quel que soit l'endroit où elles se trouvent" lorsque la loi l'exige (Daskal, 2018-19, p.11).

D'autre part, les flux peuvent être limités pour empêcher les adversaires d'obtenir des renseignements sur les États-Unis. Par exemple, en vertu du Foreign Investment Risk Review Modernization Act (2018), le Committee on Foreign Investment in the US (CFIUS) peut examiner les investissements étrangers pour déterminer s'ils constituent une menace pour la sécurité nationale. Il s'agit notamment de déterminer si les transactions peuvent créer des vulnérabilités en matière de cybersécurité ou exposer les informations personnelles des citoyens. Une conclusion en ce sens autorise une action présidentielle pour bloquer ou atténuer les risques (CSIS, 2020). En outre, l'administration Trump a promulgué le décret 13873 (EO, 2019), interdisant ainsi l'acquisition de technologies ou de services d'information et de communication auprès d'adversaires étrangers, si cela présente un risque excessif pour les objets de l'acquisition eux-mêmes, les infrastructures critiques, l'économie numérique ou la "sécurité et la sûreté des personnes [américaines]". Enfin, la stratégie nationale de cybersécurité de l'administration Biden (Maison Blanche, 2023) souligne la nécessité d'une "harmonisation réglementaire transfrontalière pour éviter que les exigences en matière de cybersécurité n'entravent les flux commerciaux numériques" (p. 9).

2.3.2. Règles spécifiques pour les flux de données transfrontaliers

Les lois sur la protection de la vie privée ne font pas expressément référence aux flux de données transfrontaliers, mais imposent des obligations vis-à-vis des transferts de données à des tiers. En vertu de la COPPR et de l'HIPAA, les opérateurs doivent s'assurer que les tiers garantissent la confidentialité, la sécurité et l'intégrité des données (Sec. 312.8, COPPR) et conclure des contrats qui protègent la confidentialité et la sécurité des données de santé (HHS, 2019). En vertu de la loi sur la FTC, les entreprises américaines doivent se conformer à la loi, même si les données circulent

au-delà des frontières. Par exemple, dans l'affaire GMR Transcription Services (FTC, 2014a), la FTC a estimé qu'une société de transcription médicale et juridique avait enfreint la loi sur la FTC en exportant des données vers des transcripteurs en Inde, ne garantissant ainsi pas la sécurité des données, la protection de la vie privée des consommateurs et la protection de la santé (FTC, 2014b). En vertu de l'article 1798.100(d) de la loi californienne sur la protection des données, les entreprises qui partagent des informations personnelles avec des tiers sont tenues de conclure un contrat qui établit (i) une limitation de la finalité du traitement des données, (ii) un niveau égal de protection de la vie privée et (iii) des droits permettant de s'assurer que le tiers traite les données de manière appropriée et de remédier à la situation si ce n'est pas le cas (Kutner et al., 2022).

La sécurité nationale est le seul autre motif politique analysé dans le présent document susceptible de restreindre les flux transfrontaliers. Les États-Unis ne disposent pas d'un cadre concret pour les transferts transfrontaliers qui garantisse leur sécurité nationale tout en offrant une sécurité juridique aux responsables du traitement des données. Le débat en cours sur TikTok et WeChat en est l'illustration. La Maison Blanche de Trump (2020) a tenté d'interdire WeChat, une application de messagerie chinoise, en invoquant la sécurité nationale, mais cette mesure a été limitée par la liberté d'expression. Un tribunal a bloqué l'interdiction parce qu'elle "entravait considérablement plus d'expression que nécessaire [pour sauvegarder la sécurité nationale]" (WeChat Users Alliance v. Trump, 2020, p.18). De même, dans l'affaire Packingham v. North Carolina (2016, pp.9-10), la Cour suprême a estimé que la loi ne pouvait pas interdire complètement "l'exercice des droits du premier amendement sur des sites web qui font partie intégrante du tissu de notre société et de notre culture modernes" (Jaffer, 2023 ; ACLU, 2023a).

3. Où ces règlements se chevauchent-ils ?

L'aperçu ci-dessus de chaque cadre de gouvernance des données montre que le commerce international est l'intérêt convergent des trois politiques pour la promotion des flux de données transfrontaliers. Néanmoins, cela s'accompagne principalement de deux mises en garde : (i) la protection des données et de la vie privée, et (ii) la sécurité nationale.

Figure 4: convergence and divergence of regulations. Source: prepared by authors.

En conséquence, chaque pays a prescrit des instruments visant à évaluer, instruire et mettre en conformité les responsables du traitement des données impliqués dans des flux transfrontaliers. En conséquence, la présente section comporte quatre volets. Tout d'abord (3.1.), elle présente des éléments sur les intérêts convergents dans le commerce international. Viennent ensuite les convergences et les divergences concernant (3.2.) la protection des données et de la vie privée, et (3.3.) la sécurité nationale. Enfin, (3.4.) il présente les instruments prescrits par chaque politique pour permettre les flux transfrontaliers de données dans les deux domaines politiques susmentionnés.

3.1. Comment le libre-échange numérique influence-t-il les flux de données transfrontaliers ?

En bref, le libre-échange international des biens et services numériques est l'endroit où les intérêts de la Chine, de l'UE et des États-Unis convergent, en principe. Par exemple, dans le cas de la Chine, le traité RCEP (2020) établit que chaque partie "n'empêchera pas le transfert transfrontalier d'informations par des moyens électroniques [à des fins commerciales]" (art. 12.15(2)). Il ajoute que les parties doivent (i) adopter un cadre juridique qui garantit la "protection des informations personnelles" (Art. 12.8) et (ii) renforcer les capacités en matière de cybersécurité. En outre, il précise qu'aucune partie ne peut exiger la localisation des données comme condition à l'exercice d'une activité commerciale sur son territoire (article 12.14(2)). Toutefois, cette disposition peut faire l'objet d'une exception lorsqu'une partie la juge "nécessaire pour atteindre un objectif légitime de politique publique" ou pour protéger "ses intérêts essentiels de sécurité", et cette dernière ne peut être contestée par d'autres parties (article 12.14(3) (a) et (b)).

En outre, les positions des États-Unis et de l'UE sont illustrées par les négociations menées dans le cadre de l'Initiative conjointe de l'OMC sur le commerce électronique (2019). Les États-Unis soutiennent "la limitation des exceptions aux flux transfrontaliers de données à des "objectifs légitimes de politique publique"", tandis que l'UE diverge partiellement en incluant explicitement "une exception relative à la protection de la vie privée et des données personnelles" (Ismail, 2023, p.16). En conclusion, le commerce peut servir de base commune à la gouvernance des flux de données transfrontaliers entre les trois pays. Cependant, pour résoudre les problèmes, les parties doivent aligner leurs politiques nationales en matière de protection des données et de sécurité nationale sur leurs engagements commerciaux en matière de flux transfrontaliers, et vice-versa.

3.2. Comment la protection des données et de la vie privée influence-t-elle les flux de données transfrontaliers ?

Comme indiqué, la convergence en matière de protection des données et de la vie privée est essentielle pour les flux de données transfrontaliers, car les pays attendent des autres qu'ils maintiennent des niveaux de protection égaux une fois que les données de leurs citoyens circulent à l'étranger. Comme on le voit ci-dessous, ce dernier point se recoupe partiellement entre les trois pays.

PROTECTION DES DONNÉES ET VIE PRIVÉE	L'UE	US-CA[1]	RPC
	GDPR (2016)	CCPA (2018)	PIPL (2021), DSL (2021)
Notification de la collecte de données	Arts. 13(f) ; 14(f), GDPR	1798.100(a)(c), CCPA	Art. 17, PIPL
Mécanisme de consentement	Arts. 6, 7, 49, GDPR	NA	Art. 13, PIPL
Spécification de l'objet	Art. 5(b), GDPR	1798.100(a)(1)(2), (c), CCPA	Art. 6, PIPL
Limitation de la collecte / proportionnalité	Art. 5(c), GDPR	1798.100(a)(1)(2), (c), CCPA	Arts. 5, 6, PIPL
Limitation de la conservation des données	Art.5(e), GDPR	1798.100(a)(3),(c), CCPA	Art. 19, PIPL
Sécurité et confidentialité	Arts. 5(f), 32 GDPR	1798.100(e), CCPA	Art. 10, PIPL
Précision des données	Arts. 5(d), 32, GDPR	NA	Art. 46, PIPL
Mesures supplémentaires pour les données sensibles	Art. 9, GDPR	1798.121, CCPA 1798.100(a)(2), CCPA	Art. 21, LIS

Contrôle indépendant au sein de l'organisation (c'est-à-dire le DPD)	Arts. 37, 38, 39, GDPR	NA	Art. 58, PIPL
Notification de violation	Arts. 33, 34, GDPR	1798.82(a), Code civil	Art. 57, PIPL
Droit au réexamen de la décision automatisée	Arts. 22, GDPR	NA	Art. 24, PIPL
Droits de l'utilisateur (accès, opposition, suppression, rectification, portabilité des données)	Arts. 15, 16, 17, 20, 21, GDPR	1798.105, CCPA	Art. 43, CSL Art. 15, PIPL
Médiateur (Autorité publique)	Chapitre VI, GDPR	1798.199.10, CCPA	Art. 11, PIPL

Tableau 5 : Base juridique aux États-Unis, dans l'UE et en RPC. Source : production des auteurs (adaptée de Casalini et al., 2021).

[1] Le cadre compare les règles de protection de la vie privée et des données en RPC, dans l'UE et aux États-Unis. Pour ces derniers, il se concentre exclusivement sur le cadre juridique californien, car c'est le seul qui énonce des règles de fond avec une certitude juridique suffisante pour permettre la comparaison. Notamment, la loi sur la FTC, associée aux mesures d'application de la FTC, peut légitimer l'existence de certaines des dispositions comparées ci-dessus au niveau fédéral. Toutefois, ces dispositions manquent à la fois **(i) de** sécurité juridique et **(ii) d'**effets à l'égard de tous (*erga omnes*) parce que **(i)** la loi sur la FTC est trop vague et **(ii) les** mesures d'application ne sont contraignantes que pour les parties à l'affaire.

3.3. Comment la sécurité nationale influence-t-elle les flux de données transfrontaliers ?

Notamment, les points communs ici ne soutiennent pas la convergence sur la base de la substance en raison du caractère contradictoire des préoccupations en matière de sécurité nationale. En d'autres termes, chaque pays peut s'accorder sur sa politique de sécurité nationale, mais ces politiques sont poursuivies l'une contre l'autre et ne constituent pas une base normative commune pour favoriser les flux de données transfrontaliers. Toutefois, l'existence de préoccupations en matière de sécurité nationale peut favoriser la convergence des procédures relatives aux transferts internationaux de données.

Dans l'UE et aux États-Unis, il n'existe actuellement aucune règle de procédure pour les transferts transfrontaliers de données qui attribue ce niveau de sécurité juridique pour des raisons de sécurité nationale. En effet, le premier n'est pas pleinement compétent pour les questions de sécurité nationale (TFUE, art. 72, et TUE, art. 4(2)). Le second illustre, par exemple avec l'affaire TikTok, l'attention croissante portée au risque que les données peuvent représenter pour la sécurité nationale, mais ne dispose pas d'une base juridique claire. La Chine, quant à elle, met en œuvre son "数据分类分级保护制度" (système de protection catégorisée et graduée des données) (DSL, art. 21). Dans cette classification, le terme "catégorisé" fait référence au type de données et le terme "gradué" au niveau de sensibilité pour la sécurité nationale, l'économie, les moyens de subsistance des personnes ou les intérêts publics majeurs.

Ainsi, la Chine dispose de moyens juridiques pour restreindre les flux transfrontaliers de données à la fois pour des raisons de protection des informations personnelles et de sécurité nationale. Il devrait être dans l'intérêt de tous les pays de prescrire des instruments qui garantissent que leur sécurité nationale n'est pas compromise tout en offrant une sécurité juridique aux acteurs impliqués dans les flux transfrontaliers de données, comme c'est le cas dans le domaine de la protection des données.

3.4. Instruments d'évaluation de la conformité et du respect des règles pour les flux de données transfrontaliers

Chaque cadre juridique dispose de moyens différents pour permettre les flux de données transfrontaliers. Toutefois, alors que les États-Unis se limitent principalement aux CSC, le GDPR de l'UE et la PIPL de la Chine autorisent d'autres instruments tels que les mécanismes de certification et les règles d'entreprise contraignantes. L'UE est le seul acteur à utiliser l'instrument comparatif d'une décision d'adéquation et la Chine, comme nous l'avons vu au chapitre 3.3, applique de manière unique un instrument d'évaluation pour mesurer le risque en matière de sécurité nationale.

Instruments permettant les flux de données	GDPR (2016)	CCPA (2018)	PIPL (2021), DSL (2021)
Décision d'adéquation	Art 45 GDPR	NA	Na
Clauses contractuelles types (CCN)	Art 46. 2 c) d) , Art 46. 3 a), Art 93.2 GDPR	Art. 1789.100(d)	Art. 38 (3), PIPL
Mécanisme de certification	Art 46. 2 f), Art 42, Art 43 GDPR	NA	Art. 38 (2), PIPL

Règles d'entreprise contraignantes	Art 46.2 b), Art 47 GDPR	NA	NA
Code de conduite	Art 46. 2 e), Art 40, Art 42 GDPR	NA	NA
Mesures d'évaluation de la sécurité[1]	NA	NA	Art. 31, DSL ; art. 40, PIPL

Tableau 6 : Instruments visant à permettre les flux transfrontaliers (y compris la protection de la vie privée, la sécurité nationale et les raisons commerciales)

[1] Seul instrument couvrant également les questions de sécurité nationale.

Notamment, ces processus comportent deux dimensions en ce qui concerne la restriction ou la promotion du flux transfrontalier de données. Premièrement, leur rigueur réglementaire et économique à l'égard des responsables du traitement des données. En d'autres termes, plus la réglementation est stricte, plus il est coûteux de s'y conformer, plus les flux transfrontaliers sont restreints. Par exemple, une décision d'adéquation ou des BCR sont plus strictes que des CSC. Deuxièmement, le niveau d'harmonisation relative des processus utilisés par chaque pays pour permettre le flux transfrontalier de données. En effet, si les pays utilisent les mêmes procédures réglementaires, les sous-traitants peuvent se conformer simultanément et donc plus efficacement au cadre juridique de plus d'un pays. Par conséquent, un processus donné peut être très strict au regard de la première dimension, mais s'il est harmonisé avec les processus adoptés par d'autres pays, les gains d'efficacité découlant de la deuxième dimension peuvent compenser les inefficacités découlant de la première.

cet égard, la localisation des données est une mesure qui permet l'accès aux marchés numériques, comme tous les processus susmentionnés ; cependant, contrairement à ces derniers, elle ne favorise pas la circulation transfrontalière des données. La localisation des données en tant que telle n'est obligatoire en Chine que lorsque le responsable du traitement des données traite des données importantes et des informations personnelles (CSL, article 37 ; PIPL, article 40). Cette idée, bien que restrictive, peut être explorée en tant que solution expérimentale au dilemme entre les transferts transfrontaliers de données et la sécurité nationale, car elle offre une forme de sécurité juridique. Toutefois, en tant que moyen unilatéral d'entraver les flux de données, cet instrument est contesté (Chander, 2020).

4. Recommandations politiques

Cette section propose des recommandations concrètes aux ministres de l'économie numérique du G20, en particulier aux autorités de la Chine, des États-Unis et de l'UE, afin de faciliter les flux de données transfrontaliers. Ces recommandations sont

divisées en (4.1.) mesures de stabilisation, c'est-à-dire modifications ou extensions des pratiques existantes, et (4.2.) mesures de transformation.

4.1. Mesures de stabilisation : amélioration des pratiques existantes

4.1.1. Créer un répertoire des cadres de gouvernance existants

La première étape pour favoriser les transferts de données consiste à comprendre les cadres juridiques existants et à identifier les raisons qui peuvent entraver la libre circulation des données. Il est donc recommandé aux organisations internationales de s'appuyer sur ce rapport pour créer un référentiel des cadres de gouvernance existants. Elles devraient y intégrer une étude approfondie des principes et valeurs susmentionnés pour chaque pays, et continuer à explorer les domaines de convergence potentielle.

4.1.2. Améliorer l'interopérabilité technique et basée sur les données : normes de données, granularité, API

L'interopérabilité peut être envisagée en quatre niveaux (Palfrey et Gasser 2012, pp. 6-7). La première est technique et fait référence à la connexion des systèmes et à l'échange de signaux par l'intermédiaire d'une interface. La deuxième concerne les données. Ici, l'interopérabilité est réalisée lorsque les acteurs qui interagissent peuvent lire, traiter et manipuler les informations transmises. Ces premiers niveaux peuvent être atteints grâce à l'élaboration de normes de données qui définissent, structurent et clarifient l'utilisation et la gestion des données. En outre, la granularité et la classification des données peuvent aider les entreprises à se conformer aux différentes réglementations. En outre, les interfaces de programmation d'applications (API) peuvent permettre l'authentification et la sécurisation des échanges de données.

4.1.3. Renforcer l'interopérabilité fondée sur l'être humain : ALE et cadre multilatéral

La troisième couche de l'interopérabilité est une couche humaine, à savoir "si [les acteurs] sont prêts à faire des efforts pour travailler ensemble", par exemple en créant un langage commun (p. 7). Comme nous l'avons vu dans la section précédente, il convient de tirer parti des domaines politiques dans lesquels les points de convergence sont les plus élevés. Le point de départ pour y parvenir pourrait être les accords commerciaux, dans lesquels les trois politiques ont des points communs existants et dans lesquels les intérêts économiques peuvent converger. Les accords commerciaux bilatéraux et multilatéraux pourraient comporter des dispositions prévoyant des obligations de normaliser les cadres de protection des données au niveau national et de rendre le traitement des données plus transparent. D'autres considérations pourraient inclure des clés de cryptage pour renforcer la confiance entre les parties.

Pour s'attaquer à la quatrième couche d'interopérabilité, un cadre de gouvernance multipartite, multilatéral et multidisciplinaire devrait être institutionnalisé afin de libérer la valeur des flux de données transfrontaliers tout en sauvegardant les intérêts de chaque pays et en renforçant la sécurité juridique.

4.1.4. Tirer parti des clauses contractuelles types

Il est également suggéré que les pays continuent d'harmoniser et de s'appuyer sur des clauses contractuelles types pour faciliter les transferts de données. Les CSC peuvent être utilisées par des parties privées dans leurs accords contractuels et présentent l'avantage d'être prévisibles, préapprouvées, normalisées et faciles à mettre en œuvre. Il est important de noter qu'elles attribuent une responsabilité juridique aux sous-traitants transfrontaliers, quel que soit leur lieu d'implantation, en transposant le droit national dans les clauses contractuelles. Par conséquent, ces dernières deviennent opposables à ces responsables du traitement des données par le biais du système judiciaire de leur propre pays sur la base de la responsabilité contractuelle. Comme le montre le tableau 6, les trois polities utilisent actuellement les CSC et cet instrument pourrait donc être davantage adopté.

4.2. Mesures de transformation : explorer de nouvelles voies pour la circulation transfrontalière des données

4.2.1. Envisager des technologies renforçant la protection de la vie privée

D'autres approches n'ont pas encore été pleinement explorées, notamment l'adoption de technologies d'amélioration de la protection de la vie privée (PET). Il s'agit d'un "ensemble de technologies, d'approches et d'outils numériques qui permettent le traitement et l'analyse des données tout en protégeant la confidentialité et, dans certains cas, l'intégrité et la disponibilité des données et, par conséquent, la vie privée des personnes concernées et les intérêts commerciaux des responsables du traitement des données" (OCDE, 2023, p. 13). Certaines techniques qui pourraient être expérimentées sont la confidentialité différentielle, la pseudo-anonymisation, le cryptage homomorphique ou l'analyse fédérée, entre autres[6] .

4.2.2. Établir des centres de données juridiquement adéquats dans les zones franches d'exportation (FTZ) situées dans des tiers de confiance

Outre les outils techniques, des mécanismes expérimentaux peuvent être examinés. Les accords de dépôt fiduciaire peuvent servir d'inspiration. Il s'agit d'accords contractuels par lesquels les parties désignent un tiers ("agent de séquestre") qui garantit la responsabilité, la supervision, le contrôle et le respect d'une transaction. L'agent "conserve sous séquestre certains actifs, documents et/ou argent déposés par ces parties jusqu'à ce qu'une condition contractuelle soit remplie" (Cornell Law School, 2021). Ce raisonnement peut être associé au concept de zones de libre-échange (ZLE) pour la libre circulation des données. Par exemple, le centre international de données susmentionné dans la zone franche de Hainan en Chine tient compte des conditions transversales techniques, commerciales, sécuritaires et réglementaires pour devenir

[6] **Les techniques de confidentialité différentielle** "apportent de petites modifications (ajout de bruit) aux données brutes pour masquer les détails des entrées individuelles, tout en conservant le pouvoir explicatif des données". La **pseudo-anonymisation** est une forme de dépersonnalisation (OCDE, 2023, p.16-17). Le **chiffrement homomorphe** implique que "les données sont chiffrées avant d'être partagées afin qu'elles puissent être analysées, mais pas décodées en informations d'origine". L'**analyse fédérée** signifie que les parties partagent les "connaissances issues de l'analyse de leurs données sans partager les données elles-mêmes." (WEF, 2023, p.8).

un havre de sécurité pour le transfert transfrontalier de données en provenance et à destination de la Chine (Plattform Industrie 4.0, 2020).

Les régimes politiques peuvent engager des négociations multilatérales entre elles et avec des pays tiers (dépôts fiduciaires / escrows) afin d'attribuer une FTZ pour les flux de données transfrontaliers sur leur territoire. Cette zone comprendrait des cadres institutionnels et techniques convenus en matière de sécurité et de protection des données qui satisfont chaque pays vis-à-vis de son droit national et de ses préoccupations géopolitiques. En conséquence, ces zones franches seraient automatiquement jugées adéquates par chaque pays sur la base de la protection des données et de la sécurité nationale. Les aspects techniques et institutionnels seraient gérés par le séquestre, mais entièrement supervisés et contestables par les régimes politiques. Enfin, les négociations pourraient être menées de manière progressive, en commençant par les flux de données dans les secteurs les moins sensibles à la protection des données et à la sécurité nationale et en allant vers des secteurs plus sensibles. Ainsi, chaque étape de la négociation peut être mise à profit pour réussir la suivante.

De nombreux arguments plaident en faveur de cet arrangement. Tout d'abord, il s'agit d'un système d'équilibre des pouvoirs (Lessig, 1999, 2006), car chaque pays est incité à informer sur les vulnérabilités techniques. Dans le cas contraire, ils risquent de voir d'autres personnes exploiter ces failles non signalées. Deuxièmement, il confère une certitude juridique aux responsables du traitement transfrontalier des données pour qu'ils puissent s'engager dans le commerce numérique et avoir accès aux trois marchés les plus riches du monde. Troisièmement, plutôt que d'exiger la localisation des données, elle encourage économiquement une version adaptée de celles-ci, qui bénéficie de sa sécurité tout en permettant les flux transfrontaliers. Quatrièmement, même si ce processus peut être plus strict que d'autres et, par conséquent, inefficace vis-à-vis de la promotion du flux de données, l'harmonisation entre les trois pays peut le compenser.

4.2.3. Mettre en place une cour à compétence transnationale au sein du pouvoir judiciaire

Comme expliqué à la section 3.2 (p. 21), la Chine et les États-Unis se heurtent à des obstacles pour transférer des données depuis l'UE en raison du cadre juridique de cette dernière, en particulier le GDPR et les arrêts Schrems I et II de la CJUE. Bien que l'"accord de principe" en cours entre les États-Unis et l'UE sur le transfert transatlantique de données comprenne une "Cour d'examen de la protection des données" (WH, 2022 ; EC, 2022c), d'importantes parties prenantes ont fait valoir qu'elle n'offrait pas un niveau de protection adéquat car, entre autres, elle n'était pas suffisamment indépendante du pouvoir exécutif (NOYB, 2023 ; Bertuzzi, 2023 ; EDPB, 2023, par. 216, 222-228).

Les pays pourraient donc envisager de mettre en place des tribunaux à compétence transnationale au sein de leur système judiciaire. Comme l'explique Jessup (1956), le droit transnational désigne "tout le droit qui régit des actions ou des événements qui transcendent les frontières nationales". En effet, la compétence des tribunaux et des lois transcende depuis longtemps les frontières nationales dans des domaines

spécifiques, tels que le droit de la famille (Romano, 2020) et le droit antitrust américain (Kraus, 2014). La présente proposition diffère en ce sens qu'elle avance l'institution de tribunaux nationaux pour sauvegarder les droits attribués par le droit étranger à des personnes situées à l'étranger. La légitimité de porter une affaire devant un tel tribunal découlerait des termes du champ d'application juridictionnel du GDPR (article 3). C'est-à-dire pour les sous-traitants qui ne sont pas établis dans l'UE, s'ils (1) offrent des biens ou des services ou (2) surveillent le comportement de personnes situées sur le territoire de l'UE.

Ainsi, la prise de décision sur les compromis entre la protection des données et la sécurité nationale reste entièrement du ressort de la juridiction nationale d'un pays (les États-Unis), tout en permettant l'application interne d'une loi promulguée par la juridiction prescriptive d'un acteur étranger (l'Union européenne). Même si cela affecte la sécurité nationale, cette dernière a été relativement préservée tout en étant mise en balance avec d'autres droits par le passé. Par exemple, la Cour suprême des États-Unis n'a jamais "confirmé une injonction contre la liberté d'expression pour des raisons de sécurité nationale" (ACLU, 2023b) ; et pourtant, le pays reste sûr. L'une des limites de la Chine est que son "système judiciaire est régulièrement critiqué pour son manque d'indépendance (réelle)", en particulier en Occident (Peerenboom, 2012, p.69). Ainsi, même cette proposition ne satisferait probablement pas aux normes de l'UE en matière de flux transfrontaliers de données.

Enfin, cette expérience aurait des implications politiques plus larges pour la gouvernance numérique. En effet, le caractère transfrontalier de cette dernière a bouleversé tous les concepts juridiques historiquement développés en association avec un territoire physique, tels que la juridiction et la souveraineté. En cas de succès, cette expérience pourrait donner naissance à un système judiciaire transnational et contribuer à la résolution des litiges dans d'autres domaines de la politique numérique qui sont de plus en plus controversés au-delà des frontières, tels que l'emploi à distance.

4.3. Considérations particulières

Il existe d'autres domaines d'un débat politique plus large qui affectent également les flux de données transfrontaliers et qui ne sont pas couverts par les recommandations ci-dessus, tels que (1) la collecte et la production de preuves électroniques à l'étranger à des fins judiciaires et (2) les différentes normes de liberté d'expression d'un pays à l'autre, en particulier en ce qui concerne la modération du contenu.

5. Conclusion

En conclusion, permettre les flux de données transfrontaliers pour le commerce et la croissance de l'économie numérique, mais sans compromettre la protection de la vie privée et des données et la sécurité nationale, est une priorité pour la RPC, l'UE et les États-Unis. Afin de trouver une convergence entre ces pays, cette note compare leurs valeurs et principes ainsi que les cadres réglementaires et les instruments permettant le transfert. Toutefois, pour certaines réglementations, comme la LIS et la LPRP, il n'existe pratiquement aucun précédent dans la manière dont les règles et les lignes

directrices sont mises en œuvre, et la loi sur les données de l'UE en est encore au stade de la proposition.

Néanmoins, la comparaison permet d'identifier une convergence dans le libre-échange international des biens et services numériques et une divergence dans la protection des données entre les États-Unis et l'UE, ainsi que dans la sécurité nationale de ces deux pays vis-à-vis de la Chine. En outre, les instruments indiquent des chevauchements qui pourraient être davantage encouragés pour permettre les flux de données transfrontaliers. À cet égard, les obstacles potentiels découlant d'un renforcement de la rigueur pour les responsables du traitement des données devraient être atténués par l'harmonisation des procédures.

Dans l'ensemble, les ministres de l'économie numérique du G20 devraient mettre en œuvre les mesures de stabilisation et explorer la possibilité de mesures de transformation afin d'améliorer la convergence dans la réglementation des flux de données transfrontaliers dans l'intérêt d'une économie numérique prospère tout en sauvegardant les logiques de sécurité et de protection de la vie privée de leur nation.

Bibliographie

Akhtar S. et Sutherland, M. (2021). Le commerce numérique et la politique commerciale des États-Unis. Congressional Research Service. Consulté le 20 mars sur https://crsreports.congress.gov/product/pdf/R/R44565

Union américaine pour les libertés civiles. (ACLU). (2023a). L'ACLU condamne le vote de la commission des affaires étrangères de la Chambre des représentants sur le projet de loi d'interdiction de TikTok. Consulté le 20 mars 2023 sur https://www.aclu.org/press-releases/aclu-condemns-house-foreign-affairs-committee-vote-on-tiktok-ban-bill

Union américaine pour les libertés civiles. (ACLU). (2023b). Freedom of Expression. Consulté le 18 avril 2023 sur https://www.aclu.org/other/freedom-expression

Arcesati, R. (2023, 23 février). Fragmenter la gouvernance des données - L'Europe a besoin d'une stratégie pour vivre avec la Chine. Merics. Consulté le 28 mars 2023 sur https://merics.org/en/short-analysis/fragmenting-data-governance-europe-needs-strategy-live-china

Bertuzzi L. (2023) Les eurodéputés vont demander une renégociation du cadre de transfert de données entre l'UE et les Etats-Unis. EURACTIV. Consulté le 18 avril 2023 sur https://www.euractiv.com/section/data-privacy/news/meps-to-call-for-renegotiation-of-eu-us-data-transfer-framework/

Maison Blanche de Biden (2022). Déclaration pour l'avenir de l'internet. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Bradford, A. (2020, 17 juin). Comment l'Europe régit l'économie numérique. Project Syndicate. Consulté le 28 mars 2023 sur https://www.project-syndicate.org/magazine/brussels-effect-digital-economy-by-anu-bradford-2020-04

Bradford, A. [Université de Tilburg]. (2021). L'avenir de la démocratie libérale à l'ère du capitalisme de surveillance et de l'autoritarisme numérique [Vidéo]. Conférence prononcée dans le cadre du programme de maîtrise en droit de la concurrence et de la réglementation des marchés. https://www.youtube.com/watch?v=p_xyagWJy3U

Brishan, M., Devesa, T., Samandari, H., Smit, S., Seong, J., White, O., & Woetzel, J. (2022, 15 novembre). Global flows : Les liens qui unissent dans un monde interconnecté. Discussion Paper. McKinsey Global Institute. Consulté le 19 mars 2023 sur https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world#/

Loi californienne sur la protection de la vie privée des consommateurs (CCPA). (2020 & rev. 2023). État de Californie, ministère de la justice, bureau du procureur général. https://oag.ca.gov/privacy/ccpa

Casalini, F., González, J. C. et Nemoto, T. (2021). Cartographie des points communs dans les approches réglementaires des transferts transfrontaliers de données. Documents de travail de l'OCDE sur la politique commerciale, n°248 https://doi.org/10.1787/ca9f974e-en

Carpenter c. États-Unis. (2017). Oyez. Consulté le 1er avril 2023 à l'adresse suivante : https://www.oyez.org/cases/2017/16-402

Centre de contrôle et de prévention des maladies (CDC). (2022). Loi de 1996 sur la portabilité et la responsabilité de l'assurance maladie (HIPAA). Consulté le 6 avril 2023 sur https://www.cdc.gov/phlp/publications/topic/hipaa.html#security-rule

Centre d'études stratégiques et internationales. (CSIS). (2020). TikTok Is Running out of Time : Understanding the CFIUS Decision and Its Implications. Consulté le 23 mars 2023 sur https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications

Chan, S. (2018). La cybersécurité sous Xi Jinping. Centre pour l'avenir numérique. https://www.digitalcenter.org/wp-content/uploads/2018/01/Cybersecurity-under-Xi-Jinping-analysis.pdf

Chander, A. (2020). La localisation des données est-elle une solution pour Schrems II ? In : Journal of Economic Law 23(3). https://doi.org/10.1093/jiel/jgaa024

Chander, A., Kaminski, M. et McGeveran, W. (2021). Catalyzing Privacy Law. Minnesota Law Review. 3305. Consulté le 1er avril 2023 sur https://scholarship.law.umn.edu/mlr/3305

Charte des droits fondamentaux de l'Union européenne. (2012). Journal officiel de l'Union européenne. 2012/C 326/02. http://data.europa.eu/eli/treaty/char_2012/oj

Règle de protection de la vie privée des enfants en ligne. 78 FR 4008. (2013). https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Chin, Y., & Zhao, J. (2022), Governing Cross-Border Data Flows : International Trade Agreements and Their Limits. Laws 11(63). Consulté le 29 mars 2023 sur https://doi.org/10.3390/laws11040063

Groupe Macro Chine. (2022). La Chine clarifie sa réglementation en matière de sécurité des données pour régir les flux de données transfrontaliers. Consulté le 19

mars 2023 sur https://www.chinamacro.ch/post/china-clarifies-its-data-security-regulation-to-govern-cross-border-data-flows

Cornell Law School (2021). Escrow agreement. Consulté le 18 avril 2023 à l'adresse https://www.law.cornell.edu/wex/escrow_agreement#:~:text=The%20escrow%20agreement%20is%20a,a%20contractual%20condition%20is%20fulfilled.

Creemers, R. (2022). China's emerging data protection framework. In : Journal of Cybersecurity, Volume 8, Issue 1, 2022. Consulté le 29 mars 2023 sur : https://academic.oup.com/cybersecurity/Article/8/1/tyac011/6674794

Agence pour la cybersécurité et la sécurité des infrastructures (CISA). (2021, 1er février). Qu'est-ce que la cybersécurité ? Consulté le 2 avril 2023 sur https://www.cisa.gov/news-events/news/what-cybersecurity#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information

Administration du cyberespace de la Chine (CAC). (2022, 9 juin). Shùjù chūjìng ānquán pínggū bànfǎ 数据出境安全评估办法 [Mesures d'évaluation de la sécurité des transferts de données sortants]. Consulté le 23 mars 2023 sur http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review.

Criddle, C., McMorrow, R. et Murphy, H. (2023, 22 mars). TikTok pris dans une bataille entre les États-Unis et la Chine à propos de son puissant algorithme. Financial Times. Consulté le 26 mars 2023 sur https://www.ft.com/content/b9f3b5a8-19ae-407f-be4b-e2536617b0f8

Daskal J. (2019). Microsoft Irlande, le CLOUD Act et la législation internationale 2.0. Consulté le 23 mars 2023 sur : https://heinonline.org/HOL/P?h=hein.journals/slro71&i=9

Décision 2000/520/CE. Sur l'adéquation de la protection fournie par les principes de la sphère de sécurité en matière de protection de la vie privée et les questions fréquemment posées y afférentes, publiés par le ministère américain du commerce. http://data.europa.eu/eli/dec/2000/520/oj

Décision (UE) 2016/1250. Sur le caractère adéquat de la protection offerte par le bouclier de protection de la vie privée UE-États-Unis. http://data.europa.eu/eli/dec_impl/2016/1250/oj

Décision (UE) 2021/9. relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en application du règlement (UE) 2016/679 du Parlement européen et du Conseil. http://data.europa.eu/eli/dec_impl/2021/914/oj

DigiChina. (2018, 29 juin). Traduction : Loi sur la cybersécurité de la République populaire de Chine Consulté le 23 mars 2023 sur https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

DigiChina. (2021, 29 juin). Traduction : Loi sur la sécurité des données de la République populaire de Chine. Consulté le 23 mars 2023 sur https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

DigiChina. (2021, 7 septembre). Traduction : Loi sur la protection des informations personnelles de la République populaire de Chine. Consulté le 23 mars 2023 sur https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

DigiChina. (2022, 8 juillet). Traduction : Outbound Data Transfer Security Assessment Measures (Mesures d'évaluation de la sécurité du transfert de données vers l'extérieur). Consulté le 23 mars 2023 sur https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

Directive 95/46/CE. 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. http://data.europa.eu/eli/dir/1995/46/oj

Directive (UE) 2016/680. 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. http://data.europa.eu/eli/dir/2016/680/oj

Desai, A. (2023). US State Comprehensive Privacy Laws Report - Overview. Association internationale des professionnels de la protection de la vie privée. Consulté le 29 mars 2023 sur https://iapp.org/resources/Article/us-state-privacy-laws-overview/

Commission européenne.(2020a). Une stratégie européenne pour les données. COM/2020/66 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066&from=EN

Commission européenne. (2020b). Proposition de règlement du Parlement européen et du Conseil relatif à la gouvernance européenne des données (loi sur la gouvernance des données). COM/2020/767 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767

Commission européenne. (2022a). Proposition de règlement du Parlement européen et du Conseil concernant des règles harmonisées relatives à l'accès équitable aux données et à leur utilisation (loi sur les données). COM/2022/68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068

Commission européenne. (2022b). Déclaration commune de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles. Consulté le 1er avril 2023 sur https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

Commission européenne. (CE). (2022c). Déclaration commune de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

Commission européenne. (n.d). Position de l'UE dans le commerce mondial. Consulté le 23 mars 2023 sur https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/eu-position-world-trade_en

Comité européen de protection des données. (2019). Lignes directrices 4/2018 relatives à l'accréditation des organismes de certification en vertu de l'article 43 du règlement général sur la protection des données (2016/679). Version 3.0. Consulté le 23 mars 2023 à l'adresse suivante : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

Comité européen de protection des données. (2020). Lignes directrices 2/2020 relatives aux articles 46 (2) (a) et 46 (3) (b) du règlement 2016/679 pour les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et de pays tiers. Version 2.0. Consulté le 23 mars 2023 à l'adresse suivante : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

Comité européen de protection des données. (2022). Lignes directrices 04/2021 sur les codes de conduite en tant qu'outils pour les transferts Version 2.0. Consulté le 23 mars 2023 sur https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf

Conseil européen de la protection des données. (EDPB). (2023). Avis 5/2023 sur le projet de décision d'exécution de la Commission européenne concernant le niveau de protection adéquat des données à caractère personnel au titre du cadre UE-États-Unis de protection des données à caractère personnel. Consulté le 18 avril 2023 sur https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf

Contrôleur européen de la protection des données. (CEPD). (2019). L'accès des gouvernements aux données dans les pays tiers : Rapport final. Consulté le 23 mars 2023 à l'adresse suivante : https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

Décret exécutif. (EO, 1981). 12333. Activités de renseignement des États-Unis. 6 FR 59941, 3 CFR

Décret exécutif. (EO) (2019). 13873. Sécurisation de la chaîne d'approvisionnement des technologies et services de l'information et de la communication. 84 FR 22689.

Loi fédérale sur la protection des données (Bundesdatenschutzgesetz - BDSG). (1978). NCJ 53219.

Loi sur la Commission fédérale du commerce. (1914). 15 USC Chapter 2, Subchapter I. http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim

Commission fédérale du commerce. (FTC). (n.d.). Privacy and Security Enforcement. Consulté le 21 mars 2023 sur https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacysecurity-enforcement

Commission fédérale du commerce. (FTC). (2014a). In the Matter of GMR Transcription Service, Inc. - Decision and Order.Retrieved March 28, 2023 fromhttps://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf

Commission fédérale du commerce. (FTC). (2014b). FTC Approves Final Order in Case Against GMR Transcription Services (La FTC approuve l'ordonnance finale dans l'affaire contre GMR Transcription Services). Consulté le 28 mars 2023 sur https://www.ftc.gov/news-events/news/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services

Federal Trade Commission (FTC) c. Wyndham Worldwide Corp. (2015). Cour d'appel des États-Unis pour le troisième circuit. No. 14-3514. https://www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf

Fefer, R. (2020, 26 mars). Flux de données, vie privée en ligne et politique commerciale. Congressional Research Service.

Ferracane, M. F., Lee-Makiyama, H., & Van Der Marel, E. (2018). Indice de restriction du commerce numérique. Centre européen d'économie politique internationale (ECIPE). Consulté le 20 mars 2023 sur https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Loi sur la surveillance des renseignements étrangers. (FISA). 92 Stat. 1783.

Loi de modernisation de l'examen des risques liés aux investissements étrangers. (2018). H. R. 5515-538. Consulté le 2 avril 2023, à l'adresse suivante : https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf

G20 Indonésie. (2022). Déclaration des dirigeants du G20 à Bali.

Griswold contre Connecticut. (1965). Oyez. Consulté le 1er avril 2023, à l'adresse suivante : https://www.oyez.org/cases/1964/496

Loi sur la portabilité et la responsabilité en matière d'assurance maladie (Health Insurance Portability and Accountability Act). (HIPAA). Pub. L. No. 104-191, § 264, 110 Stat.1936.

Santé et services sociaux. (HHS). (2019). Business Associates. Consulté le 23 mars 2023 à l'adresse suivante : https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Santé et services sociaux. (HHS). (2022a). The HIPAA Privacy Rule. Consulté le 23 mars 2023 sur https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule&text=The%20Rule%20requires%20appropriate%20safeguards,information%20without%20an%20individual's%20authorization.

Hoffman, D. A. (2021). Schrems II et tiktok : les deux faces d'une même pièce. North Carolina Journal of Law & Technology, 22(4), 573-616. Consulté le 2 avril 2023 sur https://heinonline.org/HOL/P?h=hein.journals/ncjl22&i=605

Horsley, J. (2021, 26 janvier). Comment la loi chinoise sur la protection de la vie privée s'appliquera-t-elle à l'État chinois ? New America. Consulté le 2 avril 2023 sur https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/

IAPP. (2023). Lois globales sur la protection de la vie privée des États américains - Aperçu. Consulté le 26 mars 2023 sur le site https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_overview.pdf

Ismail, Y. (2023). L'évolution du contexte et de la dynamique de l'initiative conjointe de l'OMC sur le commerce électronique : Bilan de la cinquième année et perspectives pour 2023. Genève, Suisse. Institut international du développement durable et CUTS International. Consulté le 1er avril 2023 à l'adresse suivante : https://www.iisd.org/system/files/2023-04/wto-joint-initiative-e-commerce-fifth-year-stocktake-en.pdf

ISO/IEC 20889:2018. Terminologie et classification des techniques de dépersonnalisation des données visant à renforcer la protection de la vie privée. Consulté le 29 mars 2023 à l'adresse suivante : https://www.iso.org/standard/69373.html

Jaffer, J. (2023). L'interdiction de TikTok pose un problème. Il s'agit du premier amendement. The New York Times.Retrieved April 2, 2023 fromhttps://www.nytimes.com/2023/03/24/opinion/tiktok-ban-first-amendment.html

Jessup P. C. (1956) Transnational Law II. Série de conférences Storrs prononcées à l'université de Yale.

Kraus E. F. (2014). Extraterritorialité et antitrust : A Perspective on the U.S. Experience. Commission fédérale du commerce. Consulté le 18 avril 2023 sur https://www.ftc.gov/system/files/attachments/key-speeches-presentations/extraterritoriality.pdf

Kutner et al. (2022). Transferts de données transfrontaliers : PIPL vs. GDPR vs. CCPA. Cooley. Consulté le 21 mars 2023 à l'adresse suivante : https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/#_ftn5

Ladley, J. (2012). Data Governance How to Design, Deploy, and Sustain an Effective Data Governance Program. 1ère édition. Waltham, Mass : Morgan Kaufmann.

Le Monde. (2023, 24 mars). La France interdit TikTok sur les téléphones professionnels des fonctionnaires. Consulté le 28 mars 2023 sur https://www.lemonde.fr/en/politics/article/2023/03/24/france-bans-tiktok-from-public-employee-work-phones_6020523_5.html

Lessig, L. (1999). The Law of the Horse : What Cyberlaw Might Teach. Harvard Law Review, 113(2), pp. 501-549. Consulté le 18 avril 2023 sur https://doi.org/10.2307/1342331

Lessig, L. (2006). Code : Et autres lois du cyberespace, version 2.0. Tiger Prints. Consulté le 16 avril 2023 sur https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1183&context=cheer

Maximillian Schrems contre Commissaire à la protection des données. (2015).ECLI:EU:C:2015:650. Arrêt de la Cour (grande chambre). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

Maximillian Schrems / Commissaire à la protection des données. (2020). ECLI:EU:C:2020:559. Arrêt de la Cour (Grande Chambre). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

Ministère du commerce de la République populaire de Chine (MOFCOM). (2018). La Chine et Singapour concluent les négociations sur l'amélioration de l'accord de libre-échange. Consulté le 21 mars 2023 sur http://fta.mofcom.gov.cn/enarticle/ensingapore/ensingaporenews/201811/39321_1.html

Congrès national du peuple (CNP) (2016, 11 novembre). Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ 中华人民共和国网络安全法 [Loi sur la cybersécurité de la République populaire de Chine]. Consulté le 23 mars 2023 sur http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

Congrès national du peuple (CNP) (2018, 12 juin). Zhōnghuá rénmín gònghéguó guójiā qíngbào fǎ 中华人民共和国国家情报法 [Loi sur le renseignement national de la République populaire de Chine]. Consulté le 23 mars 2023 sur http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

Congrès national du peuple (CNP), (2021a, 6 octobre). Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ 中华人民共和国数据安全法 [Loi sur la sécurité des données de la République populaire de Chine]. Consulté le 23 mars 2023 sur http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

Congrès national du peuple (CNP) (2021b, 20 août). Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ 中华人民共和国个人信息保护法 [Loi sur la protection des informations personnelles de la République populaire de Chine]. Consulté le 23 mars 2023 sur http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Aucune de vos affaires. (NOYB). (2022). Six mois après l'"accord de principe", l'accord EU-USE n'a toujours pas été conclu. Consulté le 18 avril 2023 sur https://noyb.eu/en/6-months-agreement-principle-eu-us-agreement-fact-still-missing

Palfrey, J. et Gasser, U. (2012). Interop : The Promise and Perils of Highly Interconnected Systems (La promesse et les dangers des systèmes hautement interconnectés). Centre Berkman Klein pour l'Internet et la société à l'université de Harvard.

Peerenboom R. (2012). L'indépendance judiciaire en Chine : Lessons for Global Rule of Law Promotion. Cambridge University Press. Consulté le 18 avril 2023 sur https://doi-org.acces-distant.sciencespo.fr/10.1017/CBO9780511809484

Le Quotidien du Peuple. (2022, 6 septembre). Xíjìnpíng : Méiyǒu wǎngluò ānquán jiù méiyǒu guójiā ānquán习近平：没有网络安全就没有国家安全 [Xi Jinping : Il n'y a pas de sécurité nationale sans cybersécurité]. Consulté le 23 mars 2023 sur http://politics.people.com.cn/n1/2022/0906/c1001-32520806.html

Le Quotidien du Peuple. (2023, 11 mars). Guówùyuàn jīgòu gǎigé fāng'àn 国务院机构改革方案 [Programme de réforme institutionnelle du Conseil d'État]. Consulté le 23 mars 2023 sur http://lianghui.people.com.cn/2023/n1/2023/0311/c452482-32641702.html

Plateforme Industrie 4.0 (2020). Pilotage du transfert transfrontalier de données - Port de libre-échange de Hainan. Consulté le 21 avril 2023 sur https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/China/Policy-Briefing-Cross-BorderDataTransfer.pdf?__blob=publicationFile&v=2

Loi publique 114-26. (2015). Defending Public Safety Employees' Retirement Act (loi sur la défense de la retraite des employés de la sécurité publique). https://www.congress.gov/114/plaws/publ26/PLAW-114publ26.pdf

Romano G. P. (2020) Hacia la creación de tribunales transnacionales para las familias transnacionales : el ejemplo de la responsabilidad parental. La Ley : Mediación y Arbitraje, Iss. 3. Consulté le 18 avril 2023 sur https://archive-ouverte.unige.ch/unige:143199

The Economist. (2017, 11 mai). La ressource la plus précieuse du monde n'est plus le pétrole, mais les données. Consulté le 28 mars 2023 sur https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

La loi "Clarifying Lawful Overseas Use of Data Act" (loi clarifiant l'utilisation licite des données à l'étranger). (CLOUD Act). S.2383 - 115e Congrès (2017-2018).

Le gouvernement populaire de la province de Hainan (gouvernement de Hainan). (2023, 7 mars). Zhīchí hǎinán tànsuǒ guójì shùjù zhōngxīn shìdiǎn 支持海南探索国际

数据中心试点 [Hainan explorera la possibilité d'un centre de données international]. Consulté le 3 avril 2023 sur https://www.hainan.gov.cn/hainan/szfldhd/202303/d55d9f928ee045a2ad7ba13dfae21114.shtml

Trachtenberg, D.(2023). Commerce numérique et politique des données : Select Key Issues. Congressional Research Service. Consulté le 20 mars 2023 sur https://crsreports.congress.gov/product/pdf/IF/IF12347

Traité sur l'Union européenne. (2007). Journal officiel des Communautés européennes. C326/13. http://data.europa.eu/eli/treaty/teu_2012/oj

Maison Blanche de Trump (2020). Décret sur la lutte contre la menace posée par WeChat. Consulté le 28 mars 2023 sur https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

Torreblanca, J. I. (2021). La technologie. In : Conseil européen des relations étrangères, Stiftung Mercator, The Power Atlas (pp. 38-61). Consulté le 28 mars 2023 sur https://ecfr.eu/wp-content/uploads/power-atlas.pdf

OCDE. (2014). Recommandation de l'OCDE sur les stratégies d'administration numérique. Consulté le 28 mars 2023 à l'adresse suivante : https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm

OCDE. (2017). Perspectives de l'économie numérique de l'OCDE 2017. Consulté le 28 mars 2023 à l'adresse suivante : https://doi.org/10.1787/9789264276284-en

OCDE. (2019). Le chemin pour devenir un secteur public piloté par les données, Études de l'OCDE sur l'administration numérique, Éditions de l'OCDE, Paris, https://doi.org/10.1787/059814a7-en.

OCDE. (2020). Cartographie des approches en matière de données et de flux de données. Rapport pour le groupe de travail sur l'économie numérique du G20. Consulté le 6 avril 2023 sur https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf

OCDE. (2023). Technologies émergentes renforçant la protection de la vie privée. Approches réglementaires et politiques actuelles. Documents de l'OCDE sur l'économie numérique, n° 351. https://doi.org/10.1787/20716826

Bureau du directeur du renseignement national. (ODNI). (n.d.). Section 702 - Overview. https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf

Bureau du représentant américain au commerce (USTR), (2016). The Digital 2 Dozen. Consulté le 27 mars 2023 sur https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf

Packingham c. Caroline du Nord. (2016). Cour suprême des États-Unis. Consulté le 27 mars 2023 sur https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf

Accord de partenariat économique régional global (RCEP). (2020). Chapitre 12, Commerce électronique. Consulté le 29 mars 2023 sur https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf

Règlement (UE) 2016/679. relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). http://data.europa.eu/eli/reg/2016/679/oj

Règlement (UE) 2018/1807. relatif à un cadre pour la libre circulation des données à caractère non personnel dans l'Union européenne. http://data.europa.eu/eli/reg/2018/1807/oj

Règlement (UE) 2019/881. relatif à la certification en matière de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (loi sur la cybersécurité). http://data.europa.eu/eli/reg/2019/881/oj

Riley c. Californie. (2014). Oyez. Consulté le 1er avril 2023 à l'adresse suivante : https://www.oyez.org/cases/2013/13-132

Schmitt M. N. (2017). Manuel de Tallinn 2.0 sur le droit international applicable aux opérations cybernétiques. Cambridge University Press. Consulté le 18 avril 2023 à l'adresse suivante : https://doi-org.acces-distant.sciencespo.fr/10.1017/9781316822524

Selby, J. (2017). Les lois sur la localisation des données : barrières commerciales ou réponses légitimes aux risques de cybersécurité, ou les deux ? International Journal of Law and Information Technology, 25(3), 213-232. https://doi.org/10.1093/ijlit/eax010

Şimşek, C. (2021, 21 août). [Interview] Les tendances internationales en matière de réglementation de la protection des données et de la vie privée : 3 questions à Fabian Delcros.Sciences Po. Chaire numérique, gouvernance et souveraineté. Consulté le 2 avril 2023 sur https://www.sciencespo.fr/public/chaire-numerique/en/2021/08/26/international-trends-in-data-protection-and-privacy-regulations-3-questions-to-fabian-delcros/

Commission du commerce international des États-Unis (USITC) (2013). Le commerce numérique aux États-Unis et dans les économies mondiales, partie 1. Consulté le 3 avril 2023 sur : https://www.usitc.gov/publications/332/pub4415.pdf

Constitution des États-Unis (1791), amendement. I

Ustaran, E. (2018). Droit et pratique de la protection des données en Europe. Deuxième édition. Association internationale des professionnels de la protection de la vie privée.

Alliance des utilisateurs de WeChat c. Trump. (2020). United States District Court Northern District of California. San Francisco Division. Affaire n° 20-cv-05910-LB. Consulté le 9 avril 2023 sur https://www.courtlistener.com/docket/17470217/59/us-wechat-users-alliance-v-trump/

Maison Blanche (WH). (2022). Fiche d'information : Les États-Unis et la Commission européenne annoncent un cadre transatlantique de protection des données personnelles. Consulté le 18 avril 2023 sur https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

Maison Blanche (2023). Stratégie nationale de cybersécurité. Consulté le 9 avril 2023 sur https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

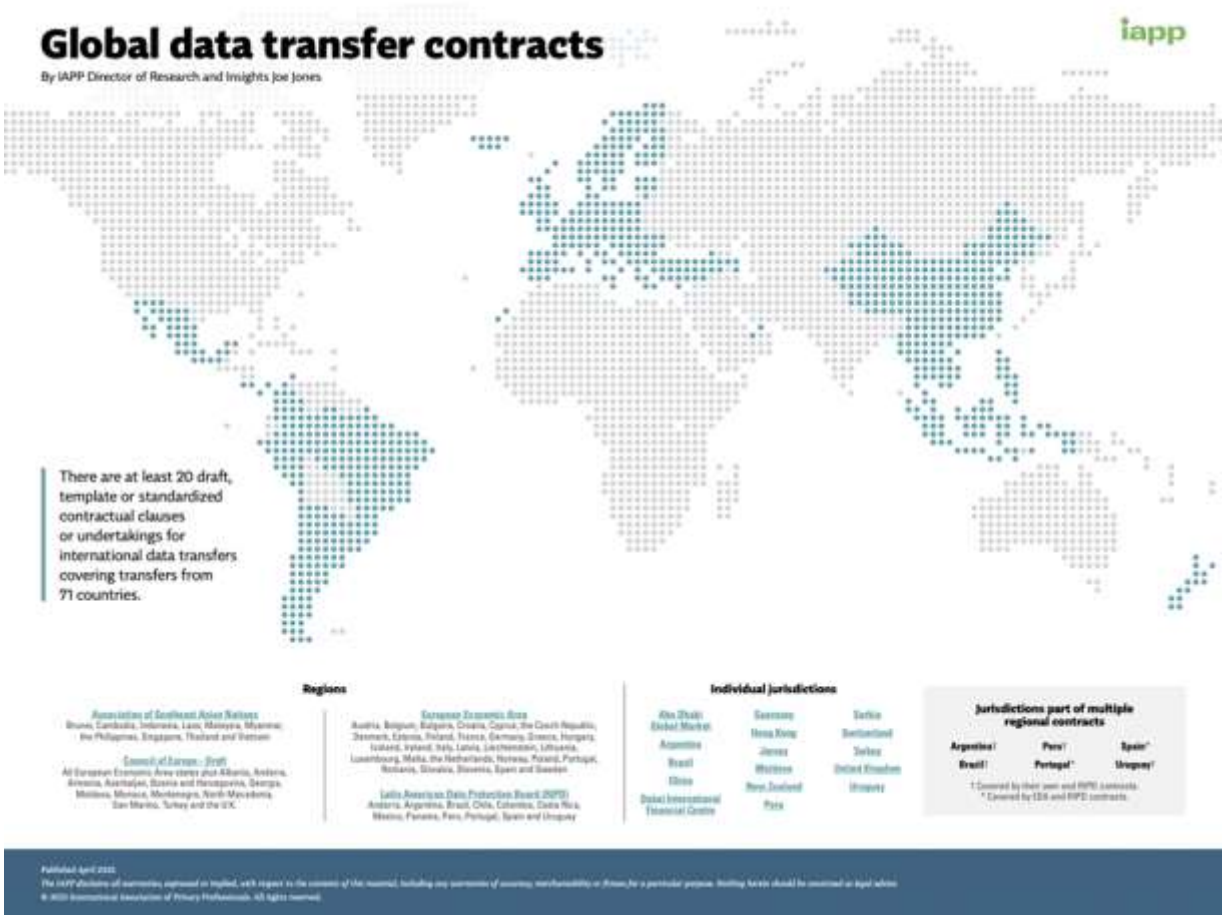
Forum économique mondial (WEF). (2023, 17 janvier). Nous devons protéger les flux de données transfrontaliers - voici pourquoi. Consulté le 3 avril 2023 sur https://www.weforum.org/agenda/2023/01/data-flows-cross-border-wef23/

Organisation mondiale du commerce. (OMC). (2019). Déclaration conjointe sur le commerce électronique. WT/L/1056.

Agence de presse Xinhua (Xinhua). (2021, 4 juillet). Guójiā wǎng xìn bàn : Guānyú xià jià "dī dī chūxíng "App de tōngbào国家网信办：关于下架 "滴滴出行 "App的通报 [Administration du cyberespace de Chine : Notification de retrait de l'application 'Didi Chuxing' de l'app store]. Consulté le 1er avril 2023 sur http://www.xinhuanet.com/legal/2021-07/04/c_1127621838.htm

Zhou, W. et Zhihang, D. (2023, 19 janvier). Cancer Collaboration Becomes First Overseas Data Transfer Approved Under New Regime. Caixin Global. Consulté le 1er avril 2023 sur https://www.caixinglobal.com/2023-01-19/cancer-collaboration-becomes-first-overseas-data-transfer-approved-under-new-regime-101991040.html

Annexe I


Global data transfer contracts
By IAPP Director of Research and Insights Joe Jones
iapp
There are at least 20 draft, template or standardized contractual clauses or undertakings for international data transfers covering transfers from 71 countries.
Regions
Individual jurisdictions
Jurisdictions part of multiple regional contracts

A propos des auteurs :

Karin Hess a une formation en sinologie, en sciences politiques et en gestion d'entreprise. De nationalité suisse, elle a passé deux ans à travailler, entre autres sujets, sur la cyber-réglementation à l'ambassade de Suisse à Pékin, et plaide pour une compétence interculturelle dans le domaine de la gouvernance des données.

Formation : double master en politiques publiques à l'École des affaires publiques de Sciences Po et en administration publique à l'École des politiques publiques de la London School of Economics (LSE). Filière politique : Numérique, nouvelles technologies et politiques publiques.

Nicole Grünbaum est conseillère en coopération internationale et a plus de 4 ans d'expérience dans le domaine du numérique et du gouvernement ouvert. Elle a dirigé la délégation argentine au sein du groupe de travail sur l'économie numérique du G20 et a coordonné l'agenda international du secrétariat de l'innovation publique au sein du bureau du chef de cabinet.

Master en politiques publiques à l'École d'affaires publiques de Sciences Po. Filière politique : Numérique, nouvelles technologies et politiques publiques

Verónica Arroyo est une militante péruvienne des droits numériques et une avocate dotée de plus de quatre ans d'expérience dans les pays en développement du monde entier. Elle est certifiée CIPP/E et s'intéresse à l'élaboration de la politique numérique des nouvelles technologies afin de garantir la protection de la vie privée, la sécurité numérique et le droit à la non-discrimination.

Double diplôme : Master en politiques publiques à l'École d'affaires publiques de Sciences Po et Master en affaires mondiales à l'École Munk d'affaires mondiales et de politiques publiques de l'Université de Toronto. Filière politique : Numérique, nouvelles technologies et politiques publiques.

Gustavo Fonseca Ribeiro est un avocat brésilien qui a de l'expérience en matière de droit et de politique numériques. Il travaille sur l'intelligence artificielle et la transformation numérique à l'UNESCO, à Paris. Auparavant, il a travaillé dans l'équipe technologique de Baker McKenzie, à Rio de Janeiro. Affilié au Laboratoire des politiques publiques et d'internet (LAPIN), il a travaillé sur des questions telles que la protection des données, la désinformation en ligne et les fermetures d'internet.

Master en politiques publiques à l'École d'affaires publiques de Sciences Po. Filière politique : Numérique, nouvelles technologies et politiques publiques.

À propos de la chaire Digital, gouvernance et souveraineté :

La **Chaire Digital, Gouvernance et Souveraineté** de Sciences Po a pour mission de créer un forum unique réunissant des entreprises techniques, des universitaires, des décideurs politiques, des acteurs de la société civile, des incubateurs de politiques publiques ainsi que des experts de la régulation numérique. Hébergée par l'École d'affaires publiques, la Chaire adopte une approche multidisciplinaire et holistique pour rechercher et analyser les 44 transformations économiques, juridiques, sociales et institutionnelles induites par l'innovation numérique. La Chaire Digital, Gouvernance et Souveraineté est dirigée par **Florence G'sell**, professeur de droit à l'Université de Lorraine, professeur à l'École d'Affaires Publiques de Sciences Po et professeur invitée à Stanford en 2023.

Les activités de la Chaire sont soutenues par :