Impact Capital for Development

Le rôle des flux de données transfrontaliers dans l'économie numérique

BRIEF

Dans une économie numérique, les flux de données transfrontaliers sont essentiels pour permettre l'amélioration des économies nationales et du niveau de vie dans les pays en développement. Aujourd'hui, la croissance drastique de la circulation des données signifie que ce flux dépasse de loin le transfert de biens ou de services. Si cela signifie que des avancées en matière de politique peuvent être réalisées, il est nécessaire de mettre en place des réglementations qui protègent les industries, les populations et les territoires.

Ce document, rédigé en étroite collaboration avec Macmillan Keck, cherche à identifier les caractéristiques spécifiques des flux de données transfrontaliers qui peuvent aider les décideurs et les régulateurs à construire une économie numérique qui inclut - et sert - tout le monde.

Janvier 2023

Macmillan Keck

Seharish Gillani, Ahmed Dermish, Jeremiah Grossman, and Friederike Rühmann of the UNCDF Policy Accelerator

Résumé

La croissance des flux de données transfrontaliers est plus rapide que celle des flux de biens, de services et de personnes. Cela permet d'améliorer les économies nationales et le niveau de vie des pays en développement grâce à une plus grande intégration dans l'économie mondiale. Lorsque les données traversent les frontières, elles sont exposées à des risques au-delà de ces frontières, et les gouvernements réglementent souvent les mouvements transfrontaliers de données pour protéger leurs industries, leurs populations et leurs territoires. Les lois sur la protection des données visent à protéger la vie privée des consommateurs, mais des approches incohérentes nuisent également à la capacité des consommateurs à participer pleinement à l'économie numérique. Les préoccupations des gouvernements en matière de sécurité nationale et de sûreté publique ont conduit à des restrictions sur les transferts de technologies et d'autres données vers l'extérieur et l'intérieur. Les gouvernements ont adopté des mesures de censure de l'internet à des degrés divers pour bloquer les médias et les communications personnelles transfrontalières. Certains gouvernements réglementent également les transferts de données transfrontaliers dans le cadre de leur politique industrielle et fiscale nationale.

Le cadre mondial de la gouvernance des données est donc actuellement fracturé et inefficace, reflétant de profondes fissures dans la confiance et des différences d'approches instillées entre les nations. Les décideurs des pays en développement ne peuvent pas à eux seuls forger la coopération internationale nécessaire, mais ils peuvent se concentrer sur leurs cadres de données nationaux et participer aux efforts internationaux pertinents.

Considérations à la lecture de cette note

1. Quels défis liés à l'accès aux flux de données transfrontaliers dans une économie numérique sont les plus importants sur votre marché, à la fois a) en général et b) pour les groupes historiquement mal desservis tels que les femmes et les personnes à faible revenu ?

2. Adressez-vous à la politique et à la réglementation en matière de flux de données transfrontaliers de votre pays :
   - **La numérisation :** L'application de la réglementation des flux de données transfrontaliers à l'économie numérique ?
   - **L'inclusivité :** Les défis spécifiques auxquels sont confrontés les femmes, les personnes à faible revenu et/ou d'autres groupes mal desservis en ce qui concerne les flux de données transfrontaliers ?

3. Quelles sont les entités responsables de la réglementation des flux de données transfrontaliers ? Les responsabilités sont-elles claires, et des mécanismes sont-ils en place pour éviter l'arbitrage réglementaire ? Dans la négative, comment cela pourrait-il être amélioré ?

Caractéristiques et étendue

Les flux de données transfrontaliers englobent tout transfert de données ou d'informations au-delà des frontières souveraines. Le commerce des biens et des services - ainsi que les voyages et les migrations humaines - impliquent des flux de données intégrés depuis des millénaires. Aujourd'hui, cependant, les flux de données transfrontaliers augmentent de manière exponentielle.

Les volumes de données transfrontalières étaient 20 fois plus importants en 2017 qu'en 2007, et ils devraient être quatre fois plus importants en 2022 qu'en 2017.[1] Le volume mondial de données stockées sur Internet devrait passer de 33 zettaoctets en 2018 à 175 zettaoctets en 2025, dont près de la moitié dans le **cloud**, un système de serveurs distribués et connectés à l'échelle mondiale.[2]

Le contenu généré ou consommé par des humains représente l'essentiel du volume de données transfrontalières. En 2020, la vidéo, les jeux et le partage social représenteront 80 % du trafic internet.[3] Les services axés sur les données, tels que l'informatique, les télécommunications, les médias, la finance, les services professionnels et autres, représentent désormais la moitié du commerce transfrontalier des services, soit à peu près l'équivalent des voyages, des transports et des autres services traditionnels réunis.[4]

Les données peuvent entrer, sortir ou simplement traverser un pays en transit. Les passages de frontières peuvent être intentionnels (comme lorsqu'un résident des Fidji partage des fichiers avec un résident du Bangladesh) ou involontaires (comme lorsqu'un résident de Gambie envoie un courriel à un autre résident de Gambie, mais que le réseau fait passer le message par l'Europe). Un passage de frontière peut se produire avant que l'utilisateur n'accède aux données si un fournisseur mondial a mis en cache des copies de contenu, comme le contenu de médias sociaux populaires, sur des serveurs nationaux pour réduire la latence.[5]

Moteurs et réponses politiques

La valeur des flux de données transfrontaliers

Les données ne présentent pas de caractéristiques de rareté comme les biens ou les services.[6] Elles sont partageables, réutilisables et non épuisables.[7] Les entreprises peuvent rassembler, stocker, traiter, récupérer et transmettre de grandes quantités de données à un coût minimal. Au lieu de diminuer, la valeur des données augmente avec l'accès et l'utilisation répétés en raison de l'accumulation et des effets de réseau : la valeur des données augmente à mesure que le volume et la variété des données augmentent et que davantage d'utilisateurs y contribuent et y ont accès. Par exemple, l'agrégation des données relatives à la santé et au comportement des individus permet de détecter des corrélations et éventuellement des liens de causalité entre les activités, les conditions de vie et la santé. La valeur des actifs incorporels - ou actifs fondés sur la connaissance[8] – représente une part très importante de l'ensemble des actifs dans les économies développées et on peut s'attendre à ce qu'elle augmente à mesure que les économies des pays en développement reposent de plus en plus sur les données.[9]

Les flux transfrontaliers peuvent améliorer les économies nationales et le niveau de vie des pays en développement en tirant parti des connaissances mondiales pour faciliter l'intégration nationale dans l'économie mondiale.[10] Une étude de l'OCDE 2020 a révélé que la participation des économies émergentes à la chaîne de valeur mondiale rendue possible par les flux de données transfrontaliers a fait augmenter les salaires locaux et attiré des investissements dans les infrastructures, les machines et les équipements locaux, même si la part de la valeur ajoutée par les biens incorporels locaux a diminué.[11] Une autre étude de l'OCDE de 2020 a conclu que les gouvernements peuvent stimuler la production locale de biens incorporels à valeur ajoutée en renforçant l'attrait de leur pays pour les activités de la chaîne de valeur mondiale et en consolidant les écosystèmes de production et d'innovation locaux et les connexions avec d'autres pays.[12] La réalisation de ces objectifs nécessite une ouverture aux flux de données transfrontaliers.

L'industrie de l'habillement en est un bon exemple. Un détaillant de vêtements en ligne basé aux États-Unis peut se procurer de nouveaux modèles auprès d'un créateur en Italie, revoir et modifier les modèles à New York et transmettre les modèles finaux à des fabricants de vêtements au Salvador et au Pakistan. Le détaillant peut communiquer avec les transporteurs pour le transport des tissus et autres intrants de la Chine, de l'Inde et du Japon vers les fabricants de vêtements et pour le transport des vêtements terminés vers les centres de distribution mondiaux en Europe et en Amérique du Nord. Le suivi en temps réel des commandes et des ventes peut permettre au détaillant de répondre rapidement aux changements de la demande en communiquant aux fabricants les ajustements de style, de taille et de quantité.[13]

Les flux de données transfrontaliers peuvent également contribuer à améliorer la santé publique, la production agricole et l'application de la loi. COVID-19 a souligné l'importance du partage des données au niveau mondial pour surveiller la propagation et l'impact des maladies infectieuses et pour développer et administrer des vaccins et des traitements.[14] Les avancées technologiques en matière de collecte et d'analyse des données peuvent aider les petits exploitants agricoles des pays en développement à répondre à la demande alimentaire croissante dans des conditions climatiques plus difficiles. Les données obtenues à partir de l'imagerie satellitaire, des mesures sur site de l'état des sols et des marchés de produits de base peuvent être combinées par des modèles informatiques pour prédire les schémas de l'offre et de la demande et les rendements des cultures afin de guider les agriculteurs via des applications pour smartphones dans le choix des semences, la plantation et la récolte.[15] Le partage transfrontalier des données peut également aider les gouvernements à lutter contre l'évasion fiscale, la criminalité internationale et le terrorisme.[16]

Réglementation des flux de données transfrontaliers

Comme pour le commerce des biens et services et la circulation des personnes, les flux de données transfrontaliers non réglementés peuvent compromettre les mesures de protection internes mises en place par les différents pays pour protéger leurs industries, leurs populations et leurs territoires. Ces menaces amènent les gouvernements à réagir en réglementant les

flux de données concernés. Parfois, la nature transfrontalière des données est accessoire aux préoccupations sous-jacentes, alors que d'autres fois, elle est la source de ces préoccupations.

Protéger la propriété intellectuelle pour favoriser l'innovation et l'investissement

Les gouvernements adoptent des lois sur la **propriété intellectuelle (PI)** pour favoriser l'investissement, l'innovation et la concurrence.[17] Le développement et la mise sur le marché de connaissances et de technologies précieuses nécessitent souvent des investissements importants dans la recherche et le développement, avec des retours incertains. Une législation forte en matière de propriété intellectuelle pour les droits d'auteur, les dessins et modèles industriels, les brevets, les secrets commerciaux, les marques et les indications géographiques peut aider les pays en développement à attirer des flux de technologie et d'investissement.[18]

Les lois sur le droit d'auteur, les dessins et modèles industriels et les brevets récompensent la création et le partage d'informations en accordant aux auteurs, concepteurs et inventeurs des droits économiques exclusifs sur leurs œuvres publiées pendant des périodes limitées.[19] En réponse à l'importance croissante des données, la protection du droit d'auteur a été étendue aux sélections ou arrangements originaux de **bases de données** publiées (collections de données), mais pas aux données sous-jacentes, dans l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC).[20] L'Union européenne,[21] le Méxique[22] et la Corée du Sud[23] reconnaissent également ce que l'on appelle les droits **sui generis** sur les bases de données, c'est-à-dire les droits sur un ensemble de données qui a été obtenu, vérifié ou présenté au prix d'un investissement substantiel, même s'il ne présente pas d'originalité digne du droit d'auteur. À l'inverse, la Chine,[24] les États-Unis[25] et d'autres parties à l'Accord sur les ADPIC exigent l'originalité pour protéger les bases de données publiées. Une consultation publique menée en 2020 par l'Office américain des brevets et des marques sur la manière dont les lois sur la PI peuvent promouvoir l'innovation dans le domaine de l'intelligence artificielle a suscité des réponses mitigées quant à l'efficacité des droits sui generis sur les bases de données.[26]

Les droits relatifs aux secrets d'affaires, qui protègent les informations dont la valeur commerciale découle du fait qu'elles sont gardées secrètes,[27] permettent à une entreprise d'être la première sur le marché ou d'offrir des biens ou des meilleurs services, plus rapides ou moins chers que ses rivaux. Les secrets commerciaux peuvent inclure des données brutes et traitées provenant de la collecte, de l'observation, de la mesure, du test, de l'étude ou de l'enquête, des formules, des processus, des algorithmes, des outils et des méthodes de productivité, et des informations internes sensibles de l'entreprise.[28] Les droits relatifs aux secrets commerciaux protègent les entreprises qui investissent dans la recherche et le développement, ce qui favorise l'innovation numérique dans les économies de marché. Les lois sur les marques et les indications géographiques visent également à prévenir la concurrence déloyale en protégeant contre les contrefaçons ou les imitations de qualité inférieure.[29] La concurrence est généralement abordée sur notre note de synthèse, « Le rôle de la concurrence dans l›économie numérique » .

Dans l'économie numérique, les droits relatifs aux secrets d'affaires sont devenus un outil essentiel pour protéger des données précieuses non publiées.[30] Les contreparties de la chaîne d'approvisionnement peuvent, sans renoncer à la protection de la PI, partager des secrets commerciaux en toute confiance au niveau national et au-delà des frontières dans les 164 États contractants de l'ADPIC qui les protègent. Une étude réalisée par l'OCDE en 2014 sur 37 pays développés et en développement entre 1985 et 2010 a révélé une relation positive et statistiquement significative entre les protections des secrets commerciaux d'un pays et ses performances économiques en matière d'innovation, de transfert international de technologie et d'accès aux intrants à forte intensité technologique et aux produits connexes.[31]

Les décideurs politiques réexaminent l'adéquation de leurs protections en matière de secrets commerciaux pour l'économie numérique.[32] Les lois sur les secrets commerciaux ont été mises à jour par l'Union européenne.[33] et les États-Unis[34] en 2016, le Japon en 2018[35] et la Chine en 2019.[36] Ces mises à jour des lois sur les secrets commerciaux reflètent un changement significatif de l'attention des entreprises vers les données en tant qu'actif clé dans une économie de l'information et la reconnaissance par les gouvernements qu'un partage efficace et effectif des secrets commerciaux nécessite des cadres juridiques solides pour faire respecter les engagements de confidentialité.[37]

L'Organisation mondiale de la propriété intellectuelle (OMPI) réunit 193 pays au sein d'un forum mondial pour les services, la politique, l'information et la coopération en matière de PI, afin de mettre en place un cadre de PI équilibré et efficace.[38] Les droits de propriété intellectuelle sont reconnus au niveau national et les propriétaires doivent enregistrer leurs droits (ou prendre d'autres mesures juridiques nécessaires pour s'assurer que leurs droits seront reconnus) dans tous les pays concernés. L'OMPI administre des traités qui harmonisent et rationalisent les enregistrements multinationaux de brevets, de droits d'auteur et de marques.[39] Les titulaires de droits de propriété intellectuelle s'appuient sur l'application des lois nationales pour se protéger contre les violations de licence, la contrefaçon et le piratage. Les restrictions aux flux transfrontaliers illicites de données font partie du cadre international de la propriété intellectuelle, qui vise à contribuer à l'innovation mondiale et au partage licite des connaissances.[40]

Les titulaires de droits de propriété intellectuelle peuvent accorder des licences d'utilisation à d'autres, avec ou sans limitations géographiques ou autres, ce qui facilite la répartition mondiale des rôles dans la chaîne d'approvisionnement. Par exemple, le titulaire d'un droit d'auteur vidéo peut restreindre l'endroit où un licencié peut visionner ou autoriser le visionnement du contenu sous licence. De même, un donneur de licence de code logiciel lisible par une machine (protégé par le droit d'auteur) peut facturer les licenciés en fonction du nombre d'utilisateurs autorisés et du lieu d'utilisation et peut choisir de ne pas divulguer le code logiciel lisible par l'homme (protégé en tant que secret commercial).

Les titulaires de droits de propriété intellectuelle disposent d'un large pouvoir discrétionnaire sur la distribution et

l'utilisation de leur savoir-faire et de leur contenu à l'échelle mondiale. En octobre 2020, la société de biotechnologie Moderna s'est engagée publiquement à ne pas faire valoir ses brevets sur l'ARNm contre ceux qui fabriquent des vaccins destinés à combattre le COVID-19 et, une fois la pandémie terminée, à concéder des licences sur ses brevets sur l'ARNm à d'autres. En réponse à cette offre, la société sud-africaine Afrigen Biologics a réussi à produire son propre vaccin à ARNm en utilisant la technologie Moderna.[41] En janvier 2022, l'artiste canadien Neil Young a demandé à la société suédoise Spotify, le plus grand service de diffusion de musique en continu au monde, de retirer sa musique de son site mondial plateforme pour protester contre la décision de Spotify de diffuser des podcasts de l'humoriste Joe Rogan, qui avait été accusé de promouvoir la désinformation sur le vaccin COVID-19.[42]

La croissance des volumes de propriété intellectuelle offre une mesure de la croissance de l'innovation, les secrets commerciaux et les brevets servant de mesures clés de l'impact de l'économie numérique. La valeur ou le volume des secrets commerciaux ne peuvent pas être facilement mesurés,[43] mais l'OMPI suit de près les demandes de brevets. 15,9 millions de brevets étaient en vigueur dans 135 juridictions en 2020, soit une augmentation de 5,9% par rapport à 2019. En 2020, les cinq pays ayant le plus de brevets en vigueur étaient les États-Unis (3,3 millions), la Chine (3,1 millions), le Japon (2 millions), la Corée du Sud (1,1 million) et l'Allemagne (800 000). En 2020, les innovateurs ont déposé 3,3 millions de demandes de brevet dans le monde, dont 1,5 million en Chine. Le total des demandes mondiales pour des inventions uniques a doublé entre 2010 et 2018, pour atteindre 2,1 millions. La technologie informatique a fait l'objet du plus grand nombre de demandes de brevet de 2017 à 2019 en Chine, au Royaume-Uni et aux États-Unis, et dans le monde en 2019, avec 284 146 demandes publiées. Parmi les grands pays à revenu intermédiaire, les déposants de l'Inde et du Mexique ont déposé le plus de demandes dans le domaine des produits pharmaceutiques, les déposants du Brésil dans celui des autres machines spéciales et les déposants de la Turquie dans celui des transports. Les demandes de brevet africaines les plus nombreuses en 2020 provenaient d'Afrique du Sud (915) et du Cameroun (672).[44]

Les pays en développement critiquent depuis longtemps le cadre de l'OMPI, qui permet aux entreprises étrangères de s'approprier les **savoirs autochtones** sans dédommager équitablement les populations locales.[45] La Convention sur la biodiversité de 1993[46] et le Protocole de Nagoya de 2010[47] reconnaissent les droits des autochtones sur les connaissances traditionnelles et demandent la réciprocité pour le partage. L'Accord de Marrakech de 1994 instituant l'Organisation mondiale du commerce (OMC)[48] et la Déclaration de Doha de 2001 traitent des conflits liés au commerce. Les pays en développement contrôlent désormais les savoirs autochtones à l'intérieur de leurs frontières et deviennent plus vigilants quant à leur utilisation à l'étranger.[49] I En 2009, l'Inde a placé ses connaissances médicinales autochtones dans le domaine public, en publiant 200 000 formules à usage libre, empêchant ainsi efficacement les entreprises étrangères d'obtenir des brevets.[50] Le Pérou reconnaît des droits de PI *sui generis* sur les savoirs autochtones[51] et protège activement ces droits en contestant et en invalidant les brevets étrangers.[52] En 2020, le Mexique a

conféré aux communautés autochtones des droits d'auteur sur les œuvres collectives issues de la culture populaire et les dessins traditionnels autochtones et, en 2021, a instauré des amendes et des peines d'emprisonnement en cas de violation.[53] Les efforts se poursuivent pour favoriser un partage mondial équitable des connaissances autochtones,[54] qui, si elles sont préservées et numérisées, pourraient aider à lutter contre le changement climatique, les maladies et le déclin de la biodiversité.[55]

Protection des données personnelles et de la vie privée

Les gouvernements adoptent des lois sur la protection des données afin de protéger la vie privée et les consommateurs de leurs citoyens, appelés « **personnes concernées** », dont les données personnelles sont collectées par des **contrôleurs de données** (qui déterminent la finalité et les moyens du **traitement des données** personnelles) ou traitées par des sous-traitants de données (qui traitent les données personnelles sous la direction ou au nom d'un contrôleur). 128 pays ont adopté des lois sur la protection des données ou la vie privée.[56] Une compilation de données à caractère personnel provenant de plusieurs personnes concernées comprend un ensemble complexe de droits qui se chevauchent et sont adjacents. Par exemple, un contrôleur de données peut avoir des droits de propriété intellectuelle sur une base de données, tandis que les personnes concernées peuvent avoir des droits de protection des données ou de la vie privée sur les données personnelles qui les concernent.

Le Règlement général sur la protection des données (RGPD) de l'UE de 2018, qui remplace la directive sur la protection des données de 1995[57] est devenu en pratique un modèle international en raison de l'importance de l'UE dans l'ouverture des marchés mondiaux.[58] Le GDPR s'attache à fournir aux personnes concernées (les individus auxquels se rapportent les données personnelles) un choix informé sur la collecte et le traitement des données personnelles les concernant. Toutefois, le GDPR et de nombreuses autres lois sur la protection des données n'accordent pas aux individus la pleine propriété ou le contrôle des données personnelles les concernant.[59] Ces lois imposent aux responsables du traitement et aux sous-traitants certaines obligations qui priment sur le choix de la personne concernée,[60] tout en énumérant des contextes dans lesquels les règles de protection des données peuvent ne pas s'appliquer du tout.[61]

De nombreux régimes de protection des données s'appliquent aux flux transfrontaliers. Le RGPD s'applique (1) aux traitements effectués à l'étranger par des responsables de traitement de l'UE ; et (2) à certains traitements effectués par des responsables de traitement ou des sous-traitants étrangers en rapport avec des personnes concernées de l'UE[62] Le RGPD interdit les restrictions aux flux de données licites au sein de l'Union européenne, mais pas aux flux sortants.[63] Affirmant les avantages du commerce et de la coopération à l'échelle mondiale,[64] le RGPD permet les flux de données sortants compatibles avec les protections de l'UE,[65] autorisant expressément les transferts vers un pays tiers qui assure une **protection adéquate**, telle que déterminée par la Commission.[66] Les données personnelles peuvent également être transmises en dehors de l'UE si le responsable du

traitement ou le sous-traitant fournit des **garanties appropriées**.[67] Les garanties appropriées comprennent :

- les règles d'entreprise contraignantes (BCR) pour les transferts au sein d'un groupe d'entreprises ou d'une entreprise commune au sein desquels les données peuvent circuler.;[68]
- des clauses contractuelles types, approuvées par la Commission ou par l'autorité de contrôle nationale, à conclure entre les parties qui envoient et reçoivent les données ; ou
- la certification dans le cadre d'un mécanisme approuvé.[69]

Au moins 14 pays - Afrique du Sud, Argentine, Arménie, Bahreïn, Barbade, Brésil, Colombie, Géorgie, Israël, Malaisie, Pérou, Suisse, Turquie et Ukraine - ont largement suivi le site RGPD pour réglementer les flux de données transfrontaliers.[70] D'autres sont plus rigoureux. Par exemple, l'Algérie[71] et le Maroc[72] exigent une approbation réglementaire préalable pour s'assurer que l'autre État offre une protection juridique suffisante.[73]

Certains pays, comme le Rwanda, exigent que toutes les données personnelles soient stockées sur le territoire national (**localisation des données**), à moins que l'autorité de contrôle n'autorise le responsable du traitement ou le sous-traitant à les stocker en dehors du Rwanda.[74] La Chine autorise certains transferts vers l'extérieur mais exige que les entreprises traitant de grandes quantités de données stockent les données personnelles localement, à moins qu'elles ne réussissent une évaluation de la sécurité par le gouvernement.[75] Ces exigences croissantes en matière de localisation des données limitent les flux de données personnelles à travers certaines frontières mais pas à d'autres, en fonction de l'origine et de la destination, et contribuent à la fragmentation d'Internet.

En l'absence d'une approche multilatérale, les approches basées sur RGPD exigent que chaque pays détermine le caractère approprié des flux transfrontaliers à destination et en provenance de chaque autre pays. Si 194 pays adoptaient cette approche (les 28 pays de l'UE agissant comme un seul bloc), plus de 14 000 déterminations bilatérales seraient nécessaire.[76] En janvier 2022 - un quart de siècle après la directive initiale sur la protection des données et quatre ans après RGPD[77] - la Commission européenne n'avait reconnu que 14 juridictions comme offrant une protection adéquate : Andorre, l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernesey, Israël, l'île de Man, le Japon, Jersey, la Nouvelle-Zélande, la Corée du Sud, la Suisse, le Royaume-Uni et l'Uruguay.[78]

Certaines initiatives régionales de protection des données ont vu le jour, mais aucune n'aborde les problèmes de confiance entre gouvernements mis en évidence par la Cour de justice des Communautés européennes (CJCE) dans l'affaire **Schrems** (voir encadré). Le forum de coopération économique Asie-Pacifique (APEC), qui compte 21 membres, a mis au point un système de règles transfrontalières de protection de la vie privée (CBPR), avec neuf pays participants : Australie, Canada, Japon, Mexique, Philippines, Singapour, Corée du Sud, Taïwan et États-Unis.[79] Cette approche implique une autocertification par les entreprises sur la base de normes de confidentialité convenues, mais elle n'oblige

pas les autorités publiques à respecter une norme minimale. En janvier 2021, l'Association des nations de l'Asie du Sud-Est (ANASE) a approuvé un cadre de gestion des données qui fait des flux transfrontaliers de données une priorité stratégique.[80] La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, qui n'est pas encore entrée en vigueur, fixerait des normes de protection des données mais n'établirait pas de marché intérieur ouvert entre les pays membres comme en Europe, laissant aux autorités nationales la seule discrétion sur les transferts transfrontaliers.[81]

En ce qui concerne les questions de confiance entre gouvernements, le Comité des politiques de l'économie numérique de l'OCDE a annoncé en décembre 2020 qu'il prévoyait de réunir un groupe de rédaction composé de représentants des gouvernements et d'experts afin d'examiner la possibilité d'élaborer un instrument définissant des principes de haut niveau ou des orientations politiques pour un accès gouvernemental de confiance aux données personnelles détenues par le secteur privé. Aucun résultat de ce groupe de rédaction n'a encore été communiqué.[82] En décembre 2021, l'OCDE a également publié une "boîte à outils" destinée à soutenir les efforts visant à améliorer l'interopérabilité transfrontalière des cadres nationaux de protection de la vie privée et des données.[83] Aujourd'hui, les approches internationales de la protection des données restent largement fragmentées, ne sont pas harmonisées et sont inefficaces.

Les pays en développement qui cherchent à tirer parti des possibilités offertes par les flux transfrontaliers devront participer aux efforts visant à simplifier et à harmoniser les approches de ces initiatives.

Schrems et la sphère de sécurité UE-USA

Malgré les mesures prises pour permettre les flux de données transfrontaliers, les défis rencontrés par l'Union européenne et les États-Unis mettent en évidence les obstacles inhérents à l'absence de confiance mutuelle. En vertu de la directive de 1995 sur la protection des données, la Commission européenne a approuvé, en juillet 2000, l'adéquation du cadre de la sphère de sécurité UE-États-Unis permettant aux entreprises américaines d'autocertifier leur conformité aux principes de protection de la vie privée du ministère américain du commerce.[84]

En 2013, Maximillian Schrems, qui vivait en Autriche, a intenté un procès au commissaire irlandais à la protection des données pour interdire à Facebook Ireland de traiter des données personnelles sur des serveurs américains. Sur saisine de la Haute Cour irlandaise, la Cour de justice de l'Union européenne (CJUE) a déclaré la décision d'adéquation de la Commission invalide en octobre 2015. La CJUE a estimé que la sphère de sécurité ne liait pas les autorités publiques américaines, dont l'accès aux données personnelles n'était pas strictement limité à ce qui était nécessaire ou proportionné à la sécurité nationale. La CJUE a estimé que cela violait les droits à la vie privée et à la protection des données personnelles des citoyens de l'UE.[85]

Toujours en vertu de la directive, la Commission européenne a approuvé en juillet 2016 le caractère adéquat du bouclier de protection de la vie privée UE-États-Unis, qui s'appuyait sur les principes de protection de la vie privée de la sphère de sécurité, avec un engagement du gouvernement américain à mettre en place un médiateur de surveillance indépendant de la communauté du renseignement.[86]

Sur un autre renvoi de la Haute Cour irlandaise dans le cadre du litige Schrems en cours, la CEJ a appliqué en juillet 2020 les dispositions de RGPD pour invalider la décision d'adéquation de la Commission. La CJE a estimé que le Privacy Shield ne protégeait pas suffisamment la vie privée des citoyens de l'UE contre le traitement des données par les autorités publiques américaines et que le système de médiation ne garantissait pas un recours effectif ou un procès équitable.[87] La CJCE a également émis des doutes quant à la capacité des clauses contractuelles types à fournir des garanties appropriées.[88]

Assurer la sécurité nationale et sécurité publique

Les préoccupations des gouvernements en matière de sécurité nationale et sécurité publique ont conduit à des restrictions importantes sur les transferts de technologies vers l'extérieur. Depuis plus de 70 ans, les gouvernements limitent les transferts de technologies d'armement vers des acteurs hostiles.[89] Quelque 28 traités de non-prolifération sont aujourd'hui en vigueur.[90] Quatre cadres multilatéraux de non-prolifération subsistent également.[91] Une adhésion stricte implique de limiter les transferts vers l'extérieur de **technologies à double usage**, c'est-à-dire de technologies qui peuvent être utilisées à la fois pour des applications pacifiques et militaires. Les contrôles des exportations de technologies peuvent nuire aux pays bénéficiaires potentiels à court terme et à la compétitivité économique du pays qui les impose à long terme.[92]

Les gouvernements sont également préoccupés par la cybersécurité internationale, qui consiste à empêcher des acteurs étrangers hostiles d'intercepter ou de compromettre des données précieuses ou d'utiliser les canaux de communication internationaux pour perpétrer des actes de terrorisme et de criminalité. En 2020, le gain financier était le principal motif des cyberattaques, et les organisations criminelles étaient à l'origine de 80 % des attaques.[93] Les réponses typiques des gouvernements consistent à renforcer les lois pénales locales et les capacités d'application de la loi, à améliorer la coopération internationale, à créer des équipes d'intervention en cas d'urgence informatique et à éduquer les entreprises et les citoyens.[94] Parmi les efforts internationaux, le Groupe d'action financière (GAFI) lutte contre le blanchiment d'argent et le financement du terrorisme en aidant les autorités nationales à retracer les flux de fonds. Ses 37 pays membres comprennent des économies en développement rapide comme l'Argentine, la Chine, l'Inde, l'Indonésie (observateur), le Mexique, la Russie, l'Afrique du Sud et la Turquie.[95]

Bien que les acteurs étatiques soient à l'origine de moins de 10 % des cyberattaques documentées,[96] les gouvernements sont préoccupés par les menaces à la

cybersécurité que représentent les acteurs étatiques et les acteurs privés parrainés ou soutenus par l'État.[97] Le gouvernement canadien considère que les États-nations sont les acteurs les plus sophistiqués en matière de menaces, avec des ressources et du personnel dédiés, une planification et une coordination étendues, et des relations de travail avec des acteurs privés et des criminels.[98] Les experts américains affirment que la ligne de démarcation entre les États-nations et les acteurs criminels est de plus en plus floue, car les États-nations abritent des proxies criminels et s'en servent pour projeter leur puissance.[99] On s'inquiète de plus en plus du vol de secrets commerciaux par des acteurs étrangers qui accèdent aux données dans le nuage et dans les réseaux.[100] Certains acteurs étatiques[101] se livrent à la cybercriminalité pour soutenir des programmes d'armement et d'autres activités sanctionnées par l'ONU.[102]

Dans le cadre de leur réponse, certains gouvernements restreignent désormais le routage et la propriété des réseaux utilisés pour la transmission transfrontalière de données, considérés comme vulnérables à la surveillance, à l'interception et à la perturbation par l'État.[103] Des préoccupations de sécurité nationale ont également été invoquées pour bloquer les fournisseurs d'équipements et d'installations.[104]

La crainte des acteurs étatiques étrangers est également la principale justification offerte par l'Union européenne, la Chine et une liste croissante de pays pour les exigences de localisation des données qui limitent les flux sortants de données personnelles. Dans l'affaire Schrems (voir encadré), la CJCE s'est concentrée sur le risque que les agences de sécurité nationale américaines traitent les données des citoyens européens. La loi chinoise de 2021 sur la sécurité des données interdit le transfert de données personnelles chinoises à des autorités judiciaires ou d'exécution étrangères sans l'approbation du gouvernement.[105] La suite logique de ces mesures est de restreindre le traitement des données nationales par les entreprises à capitaux étrangers, d'autant plus que certains pays étendent la portée de leurs services de renseignement et d'application de la loi aux données personnelles détenues dans d'autres pays. Par exemple, les difficultés rencontrées par le gouvernement américain en 2013 en utilisant un mandat de perquisition pour obtenir l'accès à des données détenues par Microsoft dans un centre de données en Irlande ont conduit à des modifications de la loi américaine en 2018 exigeant que les fournisseurs de données américains divulguent les données à l'étranger sous leur contrôle.[106] Le responsable français de la cybersécurité a depuis plaidé pour que l'Europe exclue les fournisseurs de cloud américains - Google, Amazon, Facebook, Apple et Microsoft - du traitement des données personnelles sensibles.[107] Cependant, même lorsque de telles mesures sont en place, l'espionnage parrainé par un État peut employer des logiciels espions pour franchir clandestinement les frontières et capturer des données.[108]

L'invasion de l'Ukraine par la Russie en février 2022 a entraîné les sanctions internationales et les restrictions les plus sévères jamais imposées aux flux de données transfrontaliers.[109] L'Union européenne a notamment exclu les principales banques russes du système de messagerie de paiement transfrontalier exploité par la Society for Worldwide Interbank Financial Telecommunication (SWIFT)[110] et les réseaux de paiement internationaux privés tels

qu'American Express, Mastercard et Visa ont volontairement coupé la route à la Russie.[111] Pourtant, à la mi-mars 2022, l'Union européenne, les États-Unis et d'autres alliés n'avaient pas interdit aux services d'information de se rendre accessibles en Russie. Influencés en partie par le désir de tenir les citoyens russes informés face à la désinformation des médias d'État, les fournisseurs de services d'information tels qu'Akamai (mise en cache du contenu), Amazon Web Services (informatique en nuage), Cloudflare (centres de données), Facebook (médias sociaux), Telegram (messagerie), Twitter (médias sociaux) et WhatsApp (messagerie) ont continué à opérer en Russie.[112]

Réglementation des contenus inappropriés

De par sa nature, l'internet permet d'accéder à de vastes volumes de contenus en ligne provenant d'autres pays. Certains gouvernements font un usage intensif de la technologie pour filtrer les contenus qui peuvent entrer et sortir du pays. Au cours du premier mois de l'invasion de l'Ukraine en février 2022, la Russie a bloqué plus de 270 sites d'information et sites financiers étrangers.[113]

La Déclaration universelle des droits de l'homme consacre le droit à la liberté d'opinion et d'expression sans interférence et le droit de chercher, de recevoir et de répandre des informations et des idées par quelque moyen que ce soit et sans considération de frontières.[114] Ce droit est soumis à des limitations destinées à assurer la reconnaissance et le respect des droits et libertés d'autrui et à établir les justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique.[115]

Les différents gouvernements ont adopté des degrés divers de censure de l'Internet dans l'interprétation et la mise en œuvre de ces limitations. À une extrémité du spectre, les États-Unis et d'autres pays imposent peu de restrictions à l'expression en ligne.116 À l'autre extrémité, la Chine, l'Érythrée, la Corée du Nord, l'Arabie saoudite, le Turkménistan et d'autres pays limitent strictement la liberté d'expression.[117] Au milieu se trouvent des pays comme la Papouasie-Nouvelle-Guinée, qui interdit la publication de **contenus inappropriés**, qu'elle définit comme incluant les contenus qui encouragent ou incitent au terrorisme ou qui présentent de manière offensante le sexe, la consommation de drogues, le crime, la cruauté, le blasphème, l'immoralité, la violence ou des phénomènes révoltants ou odieux.[118]

Poursuivre une politique industrielle et fiscale nationale

Certains gouvernements étudient les moyens de réglementer les activités de données transfrontalières dans le cadre de la politique industrielle et fiscale nationale.

L'Inde, parmi d'autres pays en développement, a adopté une politique de localisation des données qui se reflète actuellement dans une série de lois et de réglementations sectorielles et pourrait bientôt être plus largement incluse dans la législation en cours sur la protection des données, proposée pour la première fois en 2019 et susceptible de devenir une loi en 2022.[119] L'une des raisons invoquées pour justifier cette exigence est de générer une croissance économique et des opportunités d'emploi en augmentant la probabilité que le traitement des données à valeur ajoutée ait lieu en Inde plutôt que le pays se contente de fournir des données brutes

aux plateformes mondiales. En 2021, une évaluation quantitative de l'impact probable du projet de loi selon différents scénarios a montré qu'un cadre de localisation impliquant un stockage local des données et un traitement mondial serait le plus à même de permettre la croissance économique envisagée, mais que l'impact global sur le PIB n'était pas clair s'il fallait importer des équipements de stockage de données locaux.[120] Une simulation économique de 2014 a suggéré que l'impact sur le PIB de l'Inde pourrait en fait être négatif.[121]

Dans le même ordre d'idées, l'Union européenne a commencé à exprimer son désir de **souveraineté numérique** - pour devenir moins dépendante des entreprises technologiques américaines et chinoises.[122] Cette notion a plusieurs objectifs, selon le Conseil européen. Un objectif central est de construire un marché unique numérique. Un autre est de renforcer la capacité de l'Europe à définir ses propres règles, à faire des choix technologiques autonomes et à développer et déployer des capacités et des infrastructures numériques stratégiques, tout en préservant ses valeurs, ses droits fondamentaux, sa sécurité et son équilibre social. L'UE cherche également à tirer parti de ses outils et de ses pouvoirs réglementaires pour contribuer à l'élaboration de règles et de normes mondiales, en ne restant ouverte qu'aux entreprises qui respectent les règles et les normes de l'UE.[123]

La localisation des données a également des implications fiscales, car il est plus facile pour les autorités fiscales nationales opérant dans le cadre de régimes fiscaux traditionnels basés sur la présence physique de taxer les services de traitement des données fournis par des entreprises étrangères.[124]

Toutefois, le cadre international de taxation des services numériques, approuvé par 136 pays en octobre 2021, peut contribuer à combler l'écart fiscal sans les inconvénients de la localisation des données en réaffectant certains droits d'imposition sur les grandes entreprises multinationales de leur pays d'origine aux marchés où elles ont des activités commerciales numériques et réalisent des bénéfices.[125]

Développer un cadre international de gouvernance des données

Le cadre actuel de la **gouvernance mondiale des données**[126] est fragmenté et inefficace (à l'exception du cadre de la propriété intellectuelle de l'OMPI), reflétant de profondes fissures dans la confiance et des différences inhérentes d'approche entre les nations alliées et non alliées.

Les flux de données transfrontaliers ont traditionnellement été abordés dans les accords commerciaux. L'OMPI et l'OMC offrent donc des forums bien établis pour améliorer la gouvernance des données dans le contexte commercial. Mais cela s'est avéré insuffisant jusqu'à présent. La mission de l'OMPI se limite à la propriété intellectuelle, tandis que l'OMC a perdu de son influence en raison de la montée du protectionnisme commercial, des critiques selon lesquelles les dispositions de l'Accord sur les ADPIC en matière de brevets limitent l'accès aux médicaments dans les pays en développement, et de la réémergence de blocs commerciaux bilatéraux et multilatéraux concurrents.[127]

Dans son Rapport sur le développement dans le monde 2021, la Banque mondiale a appelé les gouvernements à forger de

nouveaux contrats sociaux nationaux pour les données et à coopérer au niveau international pour harmoniser et coordonner la gouvernance des données.[128] Lors de la réunion annuelle 2019 du Forum économique mondial, le Premier ministre japonais a invité les dirigeants à construire un ordre international pour la libre circulation des données avec confiance (DFFT). Lors de la réunion annuelle de 2020, les dirigeants ont fourni des contributions multipartites sur les processus mondiaux de gouvernance des données nécessaires pour concrétiser les avantages de l'augmentation des flux de données transfrontaliers. Le Forum économique mondial a récemment publié un livre blanc contenant les cinq principaux groupes de recommandations suivants :

1. Les gouvernements devraient mettre en place des mécanismes de protection des données personnelles et de confiance pour les transferts transfrontaliers ;
2. Les gouvernements devraient s'abstenir de restreindre les informations non personnelles et les données entre machines, et ils devraient coopérer à l'élaboration et à la mise en œuvre d'une législation sur l'accès gouvernemental aux informations numériques à l'étranger pour l'application de la loi ;
3. Les parties prenantes devrait s'engager dans une normalisation technique dirigée par le marché;
4. Les gouvernements devraient poursuivre les négociations commerciales internationales sur diverses questions relatives aux données ; et
5. Les gouvernements des pays développés, les entreprises et les organisations internationales doivent fournir une assistance technique aux pays en développement pour élaborer des normes élevées en matière de protection des données, en veillant à ce que les coûts n'empêchent pas les micro, petites et moyennes entreprises de participer au commerce mondial.[129]

En attendant, les décideurs des pays en développement ne peuvent pas forger seuls la coopération internationale nécessaire, mais ils peuvent se concentrer sur leurs cadres de données nationaux, comme le suggère la Banque mondiale. Ils peuvent également participer aux efforts internationaux pertinents. Par exemple, le programme eTrade for All cherche à informer les pays en développement des possibilités de commerce numérique et d'accès à l'assistance technique.[130] Les pays peuvent miser sur les opportunités économiques liées aux données transfrontalières en adoptant des normes internationales, comme l'a fait l'île Maurice en adoptant une législation solide en matière de protection des données et en signant la Convention 108+ du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel.[131] I En Asie, le système CBPR de l'APEC fournit un cadre aux pays participants pour permettre les flux de données transfrontaliers, notamment dans le contexte du commerce numérique.[132] Les négociations de l'accord de libre-échange continental africain en cours sous les auspices de l'Union africaine comportent également un volet sur le commerce numérique.[133]

Thèmes émergents

Web3 (ou Web 3.0) est le concept d'une nouvelle itération du World Wide Web basée sur la technologie blockchain. Il décentraliserait l'internet et offrirait aux utilisateurs une plus grande capacité à participer à la gouvernance et au

fonctionnement des protocoles régissant leur expérience utilisateur, à la fois en tant que sources et destinataires de données. Certains pensent que le Web3 pourrait améliorer la sécurité, l'évolutivité et la confidentialité des données au-delà de ce qui est actuellement possible avec les plateformes Web 2.0. D'autres ont identifié des risques liés à l'auto-gouvernance, tels que la vulnérabilité au piratage des contrats intelligents, le cryptojacking, l'absence de bonnes pratiques réglementaires, les questions relatives à la qualité et au contrôle des informations, la manipulation des données dans les applications Web3 et les risques pour les portefeuilles mobiles, notamment la perte de fonds.[134] À l'heure actuelle, Web3 se limite à des applications de niche pour les crypto-monnaies.[135]

Ressources supplémentaires

Autres lectures

- UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economic Report 2021, https://unctad.org/system/files/official-document/der2021_en.pdf (EN)
- How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF (EN)
- We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty, Internet & Jurisdiction Policy Network (EN)
- Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, World Economic Forum (EN)
- A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, World Economic Forum (EN)
- Cross-Border Data Flows: Realising benefits and removing barriers, GSMA

Organisations

- United Nations Conference on Trade and Development / Conférence des Nations unies sur le commerce et le développement (UNCTAD)
- Organisation mondiale du commerce (OMC)
- Organisation mondiale de la propriété intellectuelle (OMPI)
- Organisation de coopération et de développement économiques (OCDS)
- G-20
- World Economic Forum (WEF)
- Global Data Alliance
- International Society of Chief Data Officers

Références

[1] World Bank, World Development Report 2021: Data for Better Lives at 237 (2021). Disponible sur :https://openknowledge.worldbank.org/handle/10986/35218.

[2] David Reinsel, John Gantz & John Rydning, Data age 2025: The Digitization of the World, from Edge to Core, IDC White Paper at 3-4 (IDC, Nov 2018). Disponible sur :https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

[3] Sandvine, The Global Internet Phenomena Report at 4 (May 2020). Disponible sur :https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2020/Phenomena/COVID%20Internet%20Phenomena%20Report%2020200507.pdf.

[4] World Bank, World Development Report 2021: Data for Better Lives, supra, at 238.

[5] For a discussion of the concepts of where data is and how it moves, Voir, e.g., Javier Lopez Gonzalez, "Hitchhiker's Guide to Cross-Border Data Flows," Opinion (OECD, 3 Jun 2019). Disponible sur :https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/.

[6] Voir James Heskett, "What Happens When the Economics of Scarcity Meets the Economics of Abundance?" Working Knowledge (Harvard Business School, 4 Aug 2006). Disponible sur :https://hbswk.hbs.edu/item/what-happens-when-the-economics-of-scarcity-meets-the-economics-of-abundance.

[7] Voir United Nations Conference on Trade and Development (UNCTAD), Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, Box 1.1 at 6 (2021). Disponible sur :https://unctad.org/system/files/official-document/der2021_en.pdf.

[8] Voir, e.g., Ali Alsamawi, Charles Cadestin, Alexander Jaax, Joaquim José Martins Guilhoto, Sébastien Miroudot & Carmen Zürcher, Returns to intangible capital in global value chains: New evidence on trends and policy determinants §2.1 at 7, DSTI/CIIE(2020)27/FINAL (OECD, 5 Nov 2020). Disponible sur :https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CIIE(2020)27/FINAL&docLanguage=En.

[9] La valeur des actifs incorporels détenus par les grandes sociétés cotées aux États-Unis est passée de 122 milliards USD en 1975 à 21 000 milliards USD en 2018, passant de 17 % du total des actifs en 1975 à 90 % en 2020. La valeur des actifs incorporels en 2020 a atteint 75 % du total. valeur des actifs en Europe, 57 % en Corée, 44 % en Chine et 32 % au Japon. Ocean Tomo, Intellectual Asset Market Value Study (Ocean Tomo LLC, 2022) (évaluant les entreprises incluses dans le S&P 500 aux États-Unis, le S&P Europe 350, le KOSDAQ en Corée, le Shanghai Shenzhen CSI 300 et le Nikkei-225 au Japon). Disponible sur :https://www.oceantomo.com/intangible-asset-market-value-study/.

[10] Voir, e.g., Joshua Meltzer & Peter Lovelock, Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia, Global Economy & Development Working Paper 113 (Brookings, Mar 2018). Disponible sur :https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf.

[11] Ali Alsamawi et al., Returns to intangible capital in global value chains: New evidence on trends and policy determinants, supra, §4.2 at 24-26.

[12] Ari Van Assche, Trade, investment and intangibles: The ABCs of global value chain-oriented policies, TAD/TC/WP(2020)5/FINAL (OECD, 23 Nov 2020). Disponible sur :https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)5/FINAL&docLanguage=En.

[13] L'exemple dans le texte principal est hypothétique et simplifie excessivement les éléments de la chaîne d'approvisionnement et le rôle des flux de données. Pour une analyse plus approfondie et générique des flux de données transfrontaliers dans le sourcing, la fabrication et la distribution, voir : Swedish National Board of Trade, No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods (Mar 2015). Disponible sur :https://unctad.org/system/files/non-official-document/dtl_ict4d2016c02_Kommerskollegium_en.pdf.

[14] Pour une discussion sur les avantages et les obstacles au partage transfrontalier des données de santé publique, voir Marco Liverani, Srey Teng, Minh Sat Le & Richard Coker, "Sharing public health data and information across borders: lessons from Southeast Asia." Global Health at 14 (Springer Nature, 29 Sep 2018). Disponible sur :https://globalizationandhealth.biomedcentral.com/articles/10.1186/s12992-018-0415-0.

[15] Pour une discussion sur le potentiel des technologies numériques pour aider les petits agriculteurs, voir Kenneth Iversen, Hoi Wai, Jackie Cheng, Kristinn Helgason & Marcelo LaFleur, "Frontier technologies for smallholder farmers: addressing information asymmetries and deficiencies," Frontier Technology Issues (UN Department of Economic and Social Affairs, 17 Nov 2021). Disponible sur :https://www.un.org/development/desa/dpad/publication/frontier-technology-issues-frontier-technologies-for-smallholder-farmers-addressing-information-asymmetries-and-deficiencies/.

[16] Par exemple, la Convention des Nations Unies contre la criminalité transnationale et organisée et ses protocoles, avec 143 signataires et 190 parties, contient plusieurs articles visant à améliorer la coopération internationale en matière d'application de la loi grâce au partage de données. Voir Convention des Nations Unies contre la criminalité transnationale organisée, adoptée par la résolution 55/25 de l'Assemblée générale du 15 novembre 2000, ouverte à la signature le 12 décembre 2000 (entrée en vigueur le 29 septembre 2003). Disponible sur :https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

[17] Voir, e.g., WTO > Trade Topics > TRIPS > What are IPRs (2022). Disponible sur :https://www.wto.org/english/tratop_e/trips_e/intel1_e.htm.

[18] Voir, e.g., Keith Maskus, "Intellectual Property: Balancing Incentives with Competitive Access," in Global Economic Prospects and the Developing Countries at 129 (World Bank, 2002). Disponible sur :https://openknowledge.worldbank.org/handle/10986/14050.

[19] Voir WTO Secretariat, Primer 1: Economic Concept Relevant to Intellectual Property Rights at 2-3, The Economics of Trips Series (WTO, undated). Disponible sur :https://www.wto.org/english/tratop_e/trips_e/trips_econprimer1_e.pdf.

[20] Voir Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC), ouvert à la signature le 15 avril 1994, art. 10.2 (entré en vigueur le 1er janvier 1995 et amendé le 23 janvier 2017), joint en annexe 1C de l'Accord de Marrakech instituant l'Organisation mondiale du commerce, ouvert à la signature à Marrakech, Maroc le 15 avril 1994 (entré en vigueur le 1er janvier 1995). Disponible sur :https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm. L'article 10.2 exige que les bases de données soient protégées par le droit d'auteur lorsque la sélection ou l'arrangement de leur contenu constituent des créations intellectuelles.

[21] Voir Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 relative à la protection juridique des bases de données art. 7 (1996). Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009.

[22] Voir Mexique Loi fédérale sur le droit d'auteur art. 108 (Ley Federal del Derecho de Autor) (initialement publié au Journal officiel de la Fédération le 24 décembre 1996, tel que modifié jusqu'au 1er juillet 2020) (offrant aux créateurs de bases de données non originales une protection de 5 ans à compter de la date de publication). Disponible sur :https://wipolex.wipo.int/en/text/579009.

[23] Voir Loi sud-coréenne sur le droit d'auteur, art. 91-98 (initialement promulguée par la loi n° 8101 du 28 décembre 2006, telle que modifiée jusqu'au 21 mars 2017) (accordant aux créateurs de bases de données non originales une protection pendant 5 ans à compter de l'année suivant la publication). Disponible sur :https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42726&lang=ENG.

[24] Voir Loi sur le droit d'auteur de la République populaire de Chine art. 14 (initialement adoptée lors de la 15e réunion du Comité permanent du septième Congrès national du peuple le 7 septembre 1990 et promulguée par l'ordonnance n° 31 du président de la République populaire de Chine le 7 septembre 1990, telle qu'amendée). Disponible sur :http://www.asianlii.org/cn/legis/cen/laws/cloproc372/.

[25] Voir Loi américaine sur le droit d'auteur de 1976, 17 U.S.C. §§101 ("compilation"), 103(b) et suivants. (édicté par Pub. L. No. 94-553, 90 Stat. 2541, 19 oct. 1976, tel que modifié). Disponible sur :https://www.law.cornell.edu/uscode/text/17/chapter-1.

[26] Voir Office américain des brevets et des marques, Public Views on Artificial Intelligence and Intellectual Property Policy (octobre 2020). Disponible sur :https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf.

[27] L'article 39.2 de l'Accord sur les ADPIC exige que les informations non divulguées bénéficient de la protection si les informations (1) sont secrètes, (2) ont une valeur commerciale parce qu'elles sont secrètes et (3) ont fait l'objet de mesures raisonnables pour les garder secrètes. L'Accord sur les ADPIC n'exige pas que les informations non divulguées soient traitées comme une forme de propriété, mais exige qu'une personne légalement en possession de ces informations ait la possibilité d'empêcher qu'elles soient divulguées, acquises ou utilisées par d'autres sans son autorisation. consentement d'une manière contraire aux pratiques commerciales honnêtes, telles que la rupture ou l'incitation à rompre le contrat ou la confidentialité, ou l'acquisition d'informations non divulguées par des tiers qui savaient, ou ont fait preuve d'une négligence grave en ne sachant pas, que de telles pratiques étaient impliquées dans leur acquisition.

[28] Voir, e.g., Pricewaterhouse Coopers, The scale and impact of industrial espionage and theft of trade secrets through cyber at 10 (European Commission, Dec 2018). Disponible sur : https://ec.europa.eu/docsroom/documents/34841/attachments/1/translations/en/renditions/native.

[29] Voir, e.g., WTO > Trade Topics > TRIPS > What are IPRs, supra.

[30] Voir, e.g., Entretien du Magazine de l'OMPI avec Francis Gurry, directeur général de l'OMPI (Oct 2019). Disponible sur :https://www.wipo.int/wipo_magazine/en/2019/05/article_0001.html.

[31] Douglas Lippoldt & Mark Schultz, "Uncovering Trade Secrets - An Empirical Assessment of Economic Implications of Protection for Undisclosed Data," OECD Trade Policy Papers, No. 167 (OECD Publishing, 2014). Disponible sur :https://www.oecd-ilibrary.org/docserver/5jxzl5w3j3s6-en.pdf?expires=1643808693&id=id&accname=guest&checksum=-D87637AEE68EB5B27643835C736B56A4.

[32] Voir Entretien du Magazine de l'OMPI avec Francis Gurry, directeur général de l'OMPI, supra (Oct 2019).

[33] Voir Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 relative à la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre leur acquisition, leur utilisation et leur divulgation illicites. Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943.

[34] Voir Loi américaine sur la défense des secrets commerciaux de 2016, 18 U.S.C. §1386 (ajouté par Pub. L. No. 114-153, 11 mai 2016, 130 Stat. 376).Disponible sur : https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf.

[35] Voir Loi japonaise sur la prévention de la concurrence déloyale, loi n° 47 de 1993, telle que modifiée par la modification de la loi n° 33 de 2018 et les lois modificatives antérieures (2018). Traduction française non officielle. Disponible sur : http://www.japanese-lawtranslation.go.jp/law/detail/?id=3629&vm=02&re=02.

[36] Voir Loi anti-concurrence déloyale de la République populaire de Chine art. 9 (Adoptée à la 3e réunion du Comité permanent de la huitième Assemblée populaire nationale le 2 septembre 1993, révisée à la 30e réunion du Comité permanent de la douzième Assemblée populaire nationale le 4 novembre 2017 et amendée conformément à la Décision sur Révision de la loi sur la construction de la République populaire de Chine et des sept autres lois lors de la 10e réunion du Comité permanent du treizième Congrès national du peuple le 23 avril 2019). Traduction française non officielle. Disponible sur :https://wipolex.wipo.int/en/text/547027.

[37] Voir, e.g., International Chamber of Commerce, Protecting Trade Secrets – Recent EU and US Reforms at 5-6 (ICC, 2019). Disponible sur :https://iccwbo.org/content/uploads/sites/3/2019/04/final-icc-report-protecting-trade-secrets.pdf.

[38] WIPO > About WIPO (2022). Disponible sur :https://www.wipo.int/about-wipo/en/.

[39] Voir, generally, WIPO > About IP > Copyright, Disponible sur :https://www.wipo.int/copyright/en/; WIPO > About IP > Patents, Disponible sur :https://www.wipo.int/patents/en/; WIPO > About IP > Trademarks, Disponible sur :https://www.wipo.int/trademarks/en/.

[40] Pour une discussion des éléments des éléments complexes constituant le cadre juridique international de la propriété intellectuelle, voir Henning Grosse Ruse-Khan, "Intellectual Property and International Law: A Research Framework," in Irene Calboli and Maria Lillà Montagnani, eds., Handbook of Intellectual Property Research: Lenses, Methods, and Perspectives (Oxford University Press, Sep 2021). Disponible sur :https://oxford.university-pressscholarship.com/view/10.1093/oso/9780198826743.001.0001/oso-9780198826743-chapter-2.

[41] Voir "Covid: South Africa makes its own version of Moderna vaccine," BBC News (BBC, 4 Feb 2022). Disponible sur :https://www.bbc.com/news/health-60258088.

[42] Voir Ben Sisario, "Spotify Is Removing Neil Young Songs After He Complains of 'Misinformation,'" The New York Times (26 Jan 2022). Disponible sur :https://www.nytimes.com/2022/01/26/arts/music/spotify-neil-young-joe-rogan.html.

[43] Voir David S. Almeling, "Seven Reasons Why Trade Secrets Are Increasingly Important," 27 Berkeley Technology Law Journal 1091, 1093 (University of California, 2012). Disponible sur :https://lawcat.berkeley.edu/record/1125065/files/fulltext.pdf.

[44] Voir WIPO, World Intellectual Property Indicators 2021 at 11-22 (World Intellectual Property Organization, 2021). Disponible sur :https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2021.pdf.

[45] Voir, e.g., Ian Vincent McGonigle, "Patenting nature or protecting culture? Ethnopharmacology and indigenous intellectual property rights," 3 Journal of Law and the Biosciences 217 (Oxford University Press, 2016). Disponible sur :https://academic.oup.com/jlb/article/3/1/217/1751287.

[46] The Convention on Biological Diversity, opened for signature 5 Jun 1992, art. 18 (entered into force 29 Dec 1993). Disponible sur :https://www.cbd.int/convention/articles/?a=cbd-18.

[47] Protocole de Nagoya sur l'accès aux ressources génétiques et le partage juste et équitable des avantages découlant de leur utilisation relatif à la Convention sur la diversité biologique, ouvert à la signature le 29 octobre 2010 (entré en vigueur le 12 octobre 2014). Disponible sur :https://www.cbd.int/abs/text/.

[48] Voir TRIPS Agreement art. 27.3(b).

[49] Pour un point de vue sur les tensions entre la libre circulation de l'information et la préservation et la protection des savoirs traditionnels, voir Professor Dr. Erica-Irene A. Daes, "The impact of globalization on Indigenous Intellectual Property and Cultures," Lecture at Museum of Sydney, Sydney, Australia (25 May 2004). Disponible sur :https://humanrights.gov.au/about/news/speeches/impact-globalization-indigenous-intellectual-property-and-cultures.

[50] Voir Randeep Ramesh, "India moves to protect traditional medicines from foreign patents," The Guardian (22 Feb 2009). Disponible sur :https://www.theguardian.com/world/2009/feb/22/india-protect-traditional-medicines. L'Inde a publié une vaste base de données des remèdes traditionnels pour servir de contrôle contre les bio-prospecteurs..

[51] WIPO, Intellectual Property and Traditional Knowledge, WIPO Publication No. 920, Booklet No. 2 at 21-22 (2005). Disponible sur :https://www.wipo.int/edocs/pubdocs/en/tk/920/wipo_pub_920.pdf.

[52] Voir Nicolás Gutiérrez, "Latin America - How Latin America countries protect their traditional knowledge through IP," News Article (European Commission, 16 Jan 2020) (discussing Peru's successful challenges to patent validity in Europe and Japan). Disponible sur :https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/how-latin-america-countries-protect-their-traditional-knowledge-through-ip-2020-01-16_en.

[53] Voir Amy Guthrie, "Mexico Fights Cultural Appropriation with New Intellectual Property Law," Law.Com (ALM Media Properties, 6 Dec 2021). Disponible sur :https://www.law.com/international-edition/2021/12/06/mexico-fights-cultural-appropriation-with-new-intellectual-property-law/.

[54] Voir WIPO > WIPO Media Center > Background Briefs > Traditional Knowledge and Intellectual Property (2022). Disponible sur :https://www.wipo.int/pressroom/en/briefs/tk_ip-.html.

[55] Voir, e.g., J. Michael Finger & Philip Schuler, eds., Poor People's Knowledge: Promoting Intellectual Property in Developing Countries (World Bank & Oxford University Press, 2004). Disponible sur :https://openknowledge.worldbank.org/bitstream/handle/10986/15049/284100PAPER0Poor0peoples0knowledge.pdf?sequence=1. Voir aussi Indigenous Knowledge: Local Pathways to Global Development (World Bank, 2004). Disponible sur :https://documents1.worldbank.org/curated/en/981551468340249344/pdf/307350ENGLISH0ik0local0pathways.pdf.

[56] UNCTAD > Data Protection and Privacy Legislation Worldwide (2021). Disponible sur :https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[57] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données). Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL#d1e1384-1-1. Comme indiqué dans son titre, le RGPD a abrogé et remplacé la directive européenne de 1995 sur la protection des données. Directive 95/46/CE. Bien que conforme aux objectifs et principes de 1995, le GDPR cherchait, entre autres objectifs, à remédier à la fragmentation de l'interprétation et de l'application qui s'était produite au sein de l'Union européenne. Voir GDPR recital 9.

[58] Voir Elizabeth M. Renieris, "The GDPR at Two — Global Floor or Global Ceiling?" Berkman Klein Center Collection (Medium, 9 Jul 2020). Disponible sur :https://medium.com/berkman-klein-center/the-gdpr-at-two-global-floor-or-global-ceiling-9dc9a43d1780.

[59] Pour une discussion sur la relation entre les droits sur les données personnelles et les droits de propriété intellectuelle, voir, par exemple, Leon Trakman, Robert Walters & Bruno Zeller, "Is Privacy and Personal Data Set to Become the New Intellectual Property?" International Review of Intellectual Property and Competition Law, University of New South Wales Research Paper No. 19-70 (3 Sep 2019). Disponible sur :https://ssrn.com/abstract=3448959.

[60] Par exemple, le considérant 39 du RGPD énonce plusieurs exigences de protection des données qui ne sont pas négociables, ce qui signifie que les responsables du traitement et les sous-traitants sont automatiquement liés par ces exigences, quels que soient les accords fondés sur le consentement qu'ils concluent avec les personnes concernées. Ces exigences non négociables incluent des exigences selon lesquelles (1) tout traitement de données à caractère personnel doit être licite et équitable, (2) des normes spécifiques de transparence et de divulgation doivent être satisfaites, (3) la portée des données à caractère personnel traitées doit être limitée aux finalités pour lesquelles elles sont traitées, (4) limiter la durée de conservation des données à caractère personnel et exiger la communication du délai aux personnes concernées, (5) autoriser le traitement des données à caractère personnel uniquement si la finalité du traitement ne peut être réalisée par d'autres moyens , (6) exiger que toutes les mesures raisonnables soient prises pour rectifier ou supprimer les données personnelles inexactes, et (7) assurer une confidentialité et une sécurité appropriées lors du traitement des données personnelles. De même, le considérant 86 exige qu'un responsable du traitement informe les personnes concernées des violations de données..

[61] Par exemple, le RGPD écarte ses dispositions en matière de protection des données pour (1) les activités concernant la sécurité nationale et commune (considérant 16), (2) le traitement de données par des personnes physiques dans le cadre d'activités personnelles ou domestiques (considérant 18), (3) les activités criminelles (considérant 19), (4) les données anonymes (considérant 26), (5) les données des personnes décédées (considérant 27), (6) les autorités publiques dans le cadre de leurs missions officielles (considérant 31) et certains autres contextes.

[62] RGPD considérants 23 & 24 & art. 3. Le RGPD s'applique également dans les cas où le droit des États membres de l'UE s'applique en vertu du droit international, comme les activités au sein des ambassades et des bureaux consulaires à l'étranger, mais ces circonstances ont généralement une portée et un impact très limités et ne sont donc pas prises en compte dans la discussion actuelle..

[63] RGPD art. 1.3.

[64] RGPD recital 101.

[65] RGPD art. 44.

[66] RGPD art. 45. La détermination est faite par la Commission conformément aux critères énoncés à l'article 45.

[67] RGPD art. 46. Des garanties appropriées ne sont requises que pour le transfert de données vers un pays tiers dont il a été constaté qu'il n'offre pas une protection adéquate en vertu de l'article 45.

[68] L'exigence de règles d'entreprise contraignantes est énoncée dans l'art. 47.

[69] RGPD arts. 42.2 & 46.2(f).

[70] Voir UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 124 & note 10.

[71] Algérie Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel art. 44. Disponible en français sur https://www.joradp.dz/FTP/JO-FRANCAIS/2018/F2018034.pdf.

[72] Maroc Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données personnelles art. 43. Disponible en français sur https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf.

[73] Voir UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 124 & note 11.

[74] Rwanda Loi relative à la protection des données personnelles et de la vie privée, Nº 058/2021 du 13/10/2021, art. 50 (publié au Journal officiel le 15 octobre 2021). Disponible sur : https://www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/_2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf.

[75] Loi sur la protection des informations personnelles de la République populaire de Chine art. 40 (adoptée lors de la 30e réunion du Comité permanent du 13e Congrès national du peuple le 20 août 2021) (en vigueur le 1er novembre 2021). Traduction française non officielle. Disponible sur :https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[76] Le nombre de déterminations bilatérales avec 167 pays concernés serait égal à la somme de 166+165+164+ . . . +3+2+1 = 167(167+1)/2 = 14,028.

[77] Voir UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 104-105.

[78] Voir European Commission > Law > Law by topic > Data protection > International dimension of data protection > Adequacy decisions. (2022). Disponible sur :https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[79] Cross Border Privacy Rules System > Government (2022). Disponible sur :http://cbprs.org/government/.

[80] ASEAN Data Management Framework: Data governance and protection throughout the data lifecycle, Final Copy Endorsed by the 1st ASEAN Digital Senior Officials' Meeting (Jan 2021). Disponible sur :https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf.

[81] La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, ouverte à la signature le 27 juin 2014, art. 12.2(k) (pas encore entré en vigueur). Disponible sur : https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. En outre, la Convention africaine n'entrera en vigueur qu'après avoir été signée et ratifiée par au moins 15 États. Voir Yarik Turianskyi, Africa and Europe: Cyber Governance Lessons, Policy Insights 77 at 2 (South African Institute of International Affairs, Jan 2020). Disponible sur :https://media.africaportal.org/documents/Policy-Insights-77-turianskyi.pdf. Mais à la date de la dernière signature, seuls 14 des 55 États membres de l'Union africaine l'avaient signé et seuls huit l'avaient ratifié. Voir Union africaine, Liste des pays qui ont signé, ratifié/adhéré à la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (dernière mise à jour le 18 juin 2020). Disponible sur :https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[82] OECD, Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy (Dec 2020). Disponible sur :https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm.

[83] Voir Lisa Robinson, Kosuke Kizawa & Elettra Ronchi, "Interoperability of privacy and data protection frameworks," Going Digital Toolkit Note, No. 21 (OECD, 8 Dec 2021). Disponible sur :http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf.

[84] 2000/520/CE, décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par les principes de la sphère de sécurité relative à la vie privée et aux questions fréquemment posées connexes émises par les États-Unis Département du Commerce.Disponible sur : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520.

[85] Affaire C-362/14, Maximillian Schrems c. Commissaire à la protection des données, EU:C:2015:650 (2015) (citant les articles 7 (droit à la vie privée) et 8 (droit à la protection des données personnelles) de la Charte européenne des droits fondamentaux). Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362.

[86] 2016/1215/UE, décision de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil sur le caractère adéquat de la protection assurée par l'UE-États-Unis. Bouclier de confidentialité. Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[87] Affaire C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, EU:C:2020:559 (2020) (citant l'article 47 de la Charte européenne des droits fondamentaux). Disponible sur :https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&from=en.

[88] Affaire C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, supra, ¶¶122-149.

[89] En 1949, l'OTAN a créé le Comité de coordination des contrôles multilatéraux à l'exportation (COCOM), établissant un régime de licences d'exportation administré par les pays participants pour empêcher l'Union soviétique d'acquérir des technologies essentielles à double usage pour son armée. Voir William Alan Reinsch & Emily Benson, Digitizing Export Controls: A Trade Compliance Technology Stack? (Center for Strategic and International Studies, Dec 2021). Disponible sur : https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/211201_Reinsch_Digitizing_ExportControls.pdf?EZ.7BrxaXtjvnwfiD79RZ5ptWs692Ua6.

[90] Pour une liste des traités de désarmement et leur statut, voir United Nations Office of Disarmament Affairs > Disarmament Treaties Database (2022). Disponible sur :https://treaties.unoda.org/.

[91] Ces quatre groupes internationaux sont les suivants : (1) Le Groupe des fournisseurs nucléaires de 48 membres créé en 1974. Voir Nuclear Supplier Group > About (2022). Disponible sur :https://www.nuclearsuppliersgroup.org/en/about-nsg. Le NSG comprend tous les membres du "club nucléaire", les principales économies et certains pays en développement tels que l'Argentine, la Biélorussie, le Brésil, la Bulgarie, la Chine, la Croatie, Chypre, le Kazakhstan, le Mexique, l'Afrique du Sud et la Turquie, entre autres. (2) Le groupe australien de 42 membres créé en 1985 et axé sur les armes biologiques et chimiques. Voir The Australia Group > Home (2022). Disponible sur : https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html. (3) Le régime de contrôle de la technologie des missiles, composé de 35 membres, a été créé en 1987. Voir MTCR > Home (2022). Disponible sur :https://mtcr.info/. (4) L'Arrangement de Wassenaar de 42 membres établi en 1996 et axé sur les armes conventionnelles et les technologies à double usage. Le cadre est officiellement connu sous le nom d'Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage. Voir The Wassenaar Arrangement > About Us (2022). Disponible sur :https://www.wassenaar.org/about-us/. L'arrangement de Wassenaar succède au COCOM.

[92] Voir, e.g., Stephen Ezell & Caleb Foote, How Stringent Export Controls on Emerging Technologies Would Harm the U.S. Economy (Information Technology & Innovation Foundation, May 2019). Disponible sur :https://www2.itif.org/2019-export-controls.pdf.

[93] Voir Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto & Suzanne Widup, 2021 Data Breach Investigations Report at 12 (Verizon, 2021). Disponible sur :https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.

[94] Voir, e.g., Pricewaterhouse Coopers, The scale and impact of industrial espionage and theft of trade secrets through cyber, supra, at 12.

[95] Voir FATF > About (2022). Disponible sur :https://www.fatf-gafi.org/about/.

[96] Voir Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto & Suzanne Widup, 2021 Data Breach Investigations Report at 12

[97] Un rapport de renseignement de 2020 a révélé que l'Allemagne était une cible récurrente de l'espionnage politique, de l'espionnage industriel et du terrorisme parrainés par l'État, désignant la Russie, la Chine, l'Iran et la Turquie comme principaux agresseurs. Voir German Federal Ministry of the Interior (Bundesamt für Verfassungsschutz), Building and Community, 2020 Report on the Protection of the Constitution: Facts and Trends at 39-45 (15 Jun 2021). Disponible sur :https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2021-06-brief-summary-2020-report-on-the-protection-of-the-constitution.pdf?__blob=publicationFile&v=11.

[98] Voir Canadian Centre for Cyber Security > Publications > Cyber threat and cyber threat actors (last updated 29 Jun 2021). Disponible sur :https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

[99] Témoignage de Mieke Eoyang, US Deputy Assistant Secretary of Defence for Cyber Policy, audiences du Armed Services Committee, US House of Representatives (14 mai 2021), rapporté par C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," DOD News (US Department of Defense, 14 May 2021). Disponible sur : https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/.

[100] Voir, e.g., US Government, Administration Strategy on Mitigating the Theft of US Trade Secrets at 3-5 & 7-10 (Feb 2013). Disponible sur :https://www.justice.gov/criminal-ccips/file/938321/download, and Interview by Pete Williams, NBC News, with Christopher Wray, Director, US Federal Bureau of Investigation, Washington, DC (1 Feb 2022). Disponible sur :https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369.

[101] Voir United Nations Panel of Experts on the Democratic People's Republic of Korea established pursuant to UN Security Council resolution 1874 of 2009, Report on Democratic People's Republic of Korea, S2021/211 at ¶¶156-166 (4 Mar 2021). Disponible sur :https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf.

[102] Voir Gabriel Bassett, et al., 2021 Data Breach Investigations Report, supra, at 13.

[103] Des tensions importantes sont apparues concernant les réseaux internationaux utilisés pour la transmission de données en raison de préoccupations concernant la surveillance ou l'interception illégale de données par d'autres gouvernements. Voir, e.g., Douglas Main, "Undersea Cables Transport 99 Percent of International Data," Newsweek (2 Apr 2015). Disponible sur :https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072. Voir aussi, US Department of Justice, Office of Public Affairs, "Team Telecom Recommends FCC Grant Google and Meta Licenses for Undersea Cable," Press Release (17 Dec 2021). Disponible sur : https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable. Voir aussi US Federal Communications Commission, Non-Streamlined Submarine Cable Landing License Applications Accepted for Filing, Report No. SCL-00328NS, Public Notice (13 Aug 2021). Disponible sur : https://docs.fcc.gov/public/attachments/DOC-374897A1.pdf.

[104] En 2020, les efforts pour bloquer la technologie fournie par des entreprises chinoises telles que Huawei et ZTE ont été étendus à la technologie 5G via l'initiative américaine Clean Network qui comprend désormais plus de 30 grands opérateurs mobiles de 20 pays. Voir, e.g., Roslyn Layton, "State Department's 5G Clean Network Club Gains Members Quickly," Forbes (4 Sep 2020). Disponible sur :https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/?sh=48ee7e387536. Des problèmes similaires se sont posés en ce qui concerne le financement des câbles sous-marins. Voir, e.g., Ethan Meick, Michelle Ker & Han May Chan, China's Engagement in the Pacific Islands: Implications for the United States, US-China Economic and Security Review Commission, Staff Research Report at 10 (14 Jun 2018). Disponible sur : https://www.uscc.gov/sites/default/files/Research/China-Pacific%20Islands%20Staff%20Report.pdf. David Wroe, "Australia refuses to connect to undersea cable built by Chinese company," The Sydney Morning Herald (26 Jul 2017). Disponible sur :https://www.smh.com.au/politics/federal/australia-refuses-to-connect-to-undersea-cable-built-by-chinese-company-20170726-gxj9bf.html.

[105] Loi sur la sécurité des données de la République populaire de Chine, telle qu'adoptée lors de la 29e session du Comité permanent du treizième Congrès national du peuple de la République populaire de Chine le 10 juin 2021 (entrée en vigueur le 1er septembre 2021) (texte officiel chinois et traduction anglaise non officielle). Disponible sur : https://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf. Voir aussi Luo, Yan. "China Enacts Data Security Law." Inside Privacy (14 Jul 2021). Disponible sur : www.insideprivacy.com/cybersecurity-2/china-enacts-data-security-law.

[106] Microsoft, basé aux États-Unis, gère un centre de données en Irlande pour les clients en Europe. En 2013, le gouvernement américain a délivré un mandat de perquisition à Microsoft pour des données associées au compte de messagerie msn.com d'un abonné européen. Le mandat a été émis en vertu de la US Stored Communications Act, 18 U.S.C. Type. 119 §§ 2701 et suiv. Ces dispositions de la Stored Communications Act ont été initialement adoptées dans le cadre de la loi Omnibus Crime Control and Safe Streets Act de 1968, ajoutée par Pub. L. n° 90-351, titre III, §802, 19 juin 1968, 82 Stat. 212. Le texte actuel et l'historique législatif sont disponible sur : https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119. Après qu'une cour d'appel américaine a jugé en 2016 que Microsoft n'était pas tenue de se conformer si les données étaient stockées en dehors des États-Unis, la loi américaine a été modifiée en 2018 pour obliger les fournisseurs de services américains à divulguer les données étrangères sous leur contrôle. Microsoft Corp c. États-Unis (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp), 829 F.3d 197 (2d Cir. 2016). Disponible sur :https://casetext.com/case/microsoft-corp-v-united-states-in-re-a-warrant-to-search-a-certain-endashmail-account-controlled-maintained-by-microsoft-corp. Voir aussi, Clarifying Lawful Overseas Use of Data Act §103(a)(1), 18 U.S.C. §2713 (added by Pub. L. 115–141, div. V, § 103(a)(1), 23 Mar 2018, 132 Stat. 1214). Disponible sur :https://www.justice.gov/dag/page/file/1152896/download.

[107] Voir Laurens Cerulus, "France wants cyber rule to curb US access to EU data," Politico (13 Sep 2021). Disponible sur : https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/.

[108] Le logiciel espion Pegasus, développé par la société israélienne NSO Group, aurait été utilisé illégalement pour surveiller des fonctionnaires et des citoyens en Arménie, Azerbaïdjan, Bahreïn, Finlande, Allemagne, Hongrie, Inde, Israël, Jordanie, Kazakhstan, Mexique, Maroc, Panama, Palestine, Pologne, Rwanda, Arabie saoudite, Espagne, Togo, Ouganda, Émirats arabes unis, États-Unis et Yémen. Voir Stephen Shankland, "Pegasus spyware on State Department phones: What you need to know," cnet (3 Dec 2021). Disponible sur :https://www.cnet.com/tech/mobile/pegasus-spyware-on-state-department-phones-what-you-need-to-know/. Pegasus peut être installé secrètement sur des téléphones portables et d'autres appareils et capturer des données stockées sur ces appareils, telles que des textes, des messages vocaux, des mots de passe, des données de localisation et d'application et allumer le microphone ou la caméra.

[109] Voir, e.g., "Factbox: Putin's Russia hit with wall of international sanctions after Ukraine invasion," Reuters (7 Mar 2022). Disponible sur :https://www.reuters.com/markets/europe/putins-russia-hit-with-wall-international-sanctions-after-ukraine-invasion-2022-03-07/.

[110] Voir, e.g., Philip Blenkinsop, "EU bars 7 Russian banks from SWIFT, but spares those in energy," Reuters (2 Mar 2022). Disponible sur :https://www.reuters.com/business/finance/eu-excludes-seven-russian-banks-swift-official-journal-2022-03-02/.

[111] Voir, e.g., "Visa and Mastercard suspend Russian operations," BBC News (6 Mar 2022). Disponible sur :https://www.bbc.com/news/business-60637429.

[112] Voir, e.g., Frank Bajak & Barbara Ortutay, "War censorship exposes Putin's leaky internet controls," AP News (13 Mar 2022). Disponible sur :https://apnews.com/article/russia-ukraine-putin-technology-business-europe-1b8fec033200c33a2aef83b3d2d18713.

[113] Frank Bajak & Barbara Ortutay, "War censorship exposes Putin's leaky internet controls," supra.

[114] Ce droit est énoncé à l'article 19 de la Déclaration universelle des droits de l'homme proclamée par la résolution de l'Assemblée générale des Nations Unies en 1948.. Voir United Nations > About Us > Universal Declaration of Human Rights art. 19 (2022). Disponible sur :https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[115] Déclaration universelle des droits de l'Homme art. 29.

[116] L'article 230 de la loi américaine sur la décence des communications protège en grande partie les plateformes en ligne de toute responsabilité pour le contenu des utilisateurs. Voir 47 U.S.C. §230(c)(2). Disponible sur :https://www.govinfo.gov/content/pkg/USCODE-2020-title47/pdf/USCODE-2020-title47-chap5-subchapII-partI-sec230.pdf. Voir aussi Frances Burwell, "Free speech and online content: What can the US learn from Europe?" New Atlanticist (Atlantic Council, 1 Feb 2021). Disponible sur :https://www.atlanticcouncil.org/blogs/new-atlanticist/free-speech-and-online-content-what-can-the-us-learn-from-europe/.

[117] Sur la Chine, Voir Beina Xu & Eleanor Albert, « Media Censorship in China », Document d'information (Council of Foreign Relations, dernière mise à jour le 17 février 2017). Disponible sur :https://www.cfr.org/backgrounder/media-censorship-china. On Eritrea, Voir Committee to Protect Journalists, "10 Most Censored Countries," Special Report (10 Sep 2019). Disponible sur :https://cpj.org/reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist/#1. On North Korea, Voir Freedom House, Freedom in the World 2022: North Korea (accessed 18 Mar 2022). Disponible sur :https://freedomhouse.org/country/north-korea/freedom-world/2022. On Saudi Arabia, Voir Freedom House, Freedom in the World 2021: Saudi Arabia (accessed 18 Mar 2022). Disponible sur :https://freedomhouse.org/country/saudi-arabia/freedom-world/2021. On Turkmenistan, Voir International Partnership for Human Rights, "Turkmenistan: new internet restrictions, new cases of persecution of outspoken activists" (4 May 2021). Disponible sur :https://www.iphronline.org/turkmenistan-dec_20_mar_21.html.

[118] Voir Papua New Guinea Classification of Publications (Censorship) Act No. 18 of 1989 as amended. Disponible sur :http://www.paclii.org/pg/legis/consol_act/copa1989393/.

[119] Voir, e.g., Stephen Pritchard, "India's Personal Data Privacy Bill: What does it mean for individuals and businesses?" The Daily Swig (23 Feb 2022). Disponible sur :https://portswigger.net/daily-swig/indias-personal-data-privacy-bill-what-does-it-mean-for-individuals-and-businesses.

[120] Voir Anirudh Burman & Upasana Sharma, How Would Data Localization Benefit India? Carnegie India Working Paper at 30 (Carnegie Endowment for International Peace, Apr 2021). Disponible sur :https://carnegieendowment.org/files/202104-Burman_Sharma_Data-Localization_final.pdf.

[121] Voir Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel & Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper No. 3/2014 (European Centre for International Political Economy, 2014). Disponible sur :https://citeVoirrx.ist.psu.edu/viewdoc/download?doi=10.1.1.1047.8696&rep=rep1&type=pdf.

[122] Voir UNCTAD, Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, supra, at 105.

[123] Voir General Secretariat of the Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, Note to Delegations, EUCO 13/20 ¶7 at 4 (2 Oct 2020). Disponible sur :https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

[124] Voir, e.g., "Data localisation – protection or protectionism?" The Hindu BusinessLine (8 Aug 2021). Disponible sur :https://www.thehindubusinessline.com/business-laws/data-localisation-protection-or-protectionism/article35801546.ece.

[125] Voir OECD/G20 Base Erosion and Profit Shifting Project, Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy (8 Oct 2021). Disponible sur :https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf.

[126] Ce document utilise le terme data governannce / gouvernance des données dans le même sens que la Banque mondiale, à savoir pour décrire le cadre politique, juridique et réglementaire régissant la collecte, la transmission, le stockage, le traitement, l'utilisation et la suppression des données, à la fois à l'intérieur et au-delà des frontières. Le terme est également utilisé depuis longtemps dans un autre sens par les professionnels des données pour décrire l'exercice de l'autorité et du contrôle (planification, surveillance et application) dans la gestion des actifs de données d'une entreprise..Voir Susan Earley, ed., The DAMA Dictionary of Data Management (DAMA International, 2nd ed., 2011). Disponible sur :https://www.dama.org/cpages/body-of-knowledge (achat obligatoire). DAMA International est une association mondiale à but non lucratif, indépendante des fournisseurs, de professionnels techniques et commerciaux dédiés à l'avancement des concepts et des pratiques de gestion de l'information et des données.

[127] James McBride & Anshu Siripurapu, "What's Next for the WTO?" Backgrounder (Council on Foreign Relations, mis à jour le 13 décembre 2021). Disponible sur :https://www.cfr.org/backgrounder/whats-next-wto.

[128] World Bank, World Development Report 2021: Data for Better Lives, supra, at xi-xii.

[129] World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper at 17 (World Economic Forum, May 2020). Disponible sur :https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

[130] Voir https://etradeforall.org/.

[131] "Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data." Council of Europe, Strasbourg. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[132] Voir notes 82 et 83.

[133] Voir https://au.int/en/cfta.

[134] Voir, e.g., Pablo Blanco, "Web3 Security and its Cybersecurity Risks," 22 April 2022. Disponible sur :https://www.rootstrap.com/blog/web3-security-and-the-cybersecurity-risks/.

[135] Voir, e.g., Ethereum > Developers > Docs > Foundational Topics > WEB2 VS WEB3 (last edited 11 Dec 2021). Disponible sur :https://ethereum.org/en/developers/docs/web2-vs-web3/.

À propos de l'UNCDF

Le Fonds d'équipement des Nations Unies (UNCDF) est la principale entité de financement catalytique des Nations Unies pour les 46 pays les moins avancés (PMA) à travers le monde. Dans le cadre de son mandat unique en matière de capital et en mettant l'accent sur les PMA, l'UNCDF s'efforce d'investir et de catalyser des capitaux afin d'aider ces pays à atteindre la croissance durable et l'inclusion envisagées par le Programme de développement durable à l'horizon 2030 et le Programme d'action de Doha pour les pays les moins avancés, 2022—2031.

L'UNCDF établit des partenariats avec d'autres organisations des Nations Unies, ainsi qu'avec des acteurs des secteurs privé et public, afin d'avoir un plus grand impact sur le développement, notamment en débloquant des ressources supplémentaires et en renforçant les mécanismes et les systèmes de financement contribuant aux voies de transformation, en se concentrant sur des thèmes de développement tels que l'économie verte, la numérisation, l'urbanisation, les économies inclusives, l'égalité ente les sexes et l'autonomisation économique des femmes.

En tant qu'institution de financement du développement hybride et agence de développement, l'UNCDF utilise une combinaison d'instruments de capital (déploiement, conseil financier et commercial et catalysation) et d'instruments de développement (assistance technique, renforcement des capacités, conseils politiques, plaidoyer, leadership intellectuel, analyse et cadrage du marché) qui sont appliqués dans cinq domaines prioritaires (économies numériques inclusives, finance transformatrice locale, autonomisation économique des femmes, financement du climat, de l'énergie et de la biodiversité, et financement des systèmes alimentaires durables).

À propos de Macmillan Keck

Macmillan Keck Attorneys & Solicitors conseille ses clients en matière de stratégie, de plaidoyer, d'affaires controverses et réformes dans l'économie numérique. Les clients du cabinet comprennent des opérateurs de télécom les fournisseurs de services financiers numériques, les fournisseurs de services de santé et d'éducation en ligne fournisseurs de contenu, d'applications et de services numériques, des gouvernements et des autorités de régulation de la concurrence et des organisations internationales. Le cabinet a mené à bien de nombreux projets complexes dans une majorité de pays sur tous les continents.

Disclaimer

Les appellations utilisées sur cette carte et la présentation des données qui y figurent n'impliquent aucune prise de position de la part du Secrétariat de l'Organisation des Nations Unies ou de l'UNCDF quant au statut juridique des pays, territoires, villes ou zones.

Cette publication a été révisée pour la dernière fois en Janvier 2023.

Impact Capital
for Development

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US