1 TRANSMISSION MONDIALE DE DONNÉES ET CADRES DE RESPONSABILITÉ

A | INFRASTRUCTURE NUMÉRIQUE PERMETTANT LA TRANSMISSION MONDIALE DE DONNÉES 21

B | ALIGNEMENT MONDIAL SUR LA RÉGLEMENTATION DES CONTENUS CONCERNANT LES DONNÉES ET SUR LES CADRES DE RESPONSABILITÉ POUR SOUTENIR LES FLUX DE DONNÉES TRANSFRONTIÈRES 26

La transmission mondiale de données est nécessaire :

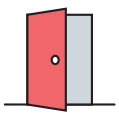
- pour l'exercice d'activités commerciales (c'est-à-dire la fourniture internationale de services et le suivi du fret international franchissant les frontières) :
- pour la coordination d'opérations sur l'ensemble des chaînes de valeur mondiales (c'est-à-dire la gestion des ressources humaines et l'optimisation des processus internes);
- pour l'échange de renseignements liés au commerce entre parties prenantes d'une chaîne d'approvisionnement.

Cependant, les flux de données transfrontières peuvent être limités : i) par l'accès à des capacités de transmission de données à un prix abordable, avec la largeur de bande et la fiabilité nécessaires, ainsi que par l'accès aux compétences numériques;

« La fracture numérique habituelle entre pays développés et pays en développement en termes de connexion et d'accès à Internet et d'utilisation de ce réseau reste importante. Alors que 90% de la population des pays développés utilisait Internet en 2021, le taux d'utilisateurs n'était que de 27% dans les pays les moins avancés. »

et ii) la réglementation des contenus concernant les données si le problème de la fragmentation réglementaire n'est pas résolu au moyen d'un alignement mondial sur la réglementation en matière de contenus et de données et sur un cadre de responsabilité. Une coordination mondiale sera requise pour garantir une connectivité rapide et abordable, sans compromettre la vie privée, la confidentialité et la sécurité.

A | INFRASTRUCTURE NUMÉRIQUE PERMETTANT LA TRANSMISSION MONDIALE DE DONNÉES



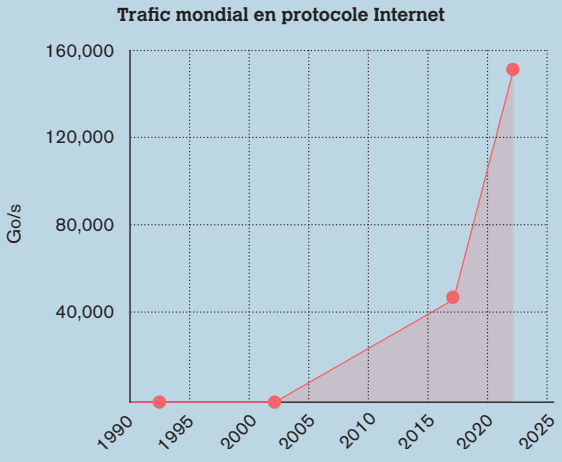
Au vu du nombre toujours plus important d'appareils connectés, la demande de couverture à large bande ne cesse d'augmenter (voir l'encadré 3). Cependant, la connectivité progresse à des rythmes différents à travers le monde. La fracture numérique habituelle entre pays développés et pays en développement en termes de connectivité et d'accès à Internet et d'utilisation d'Internet reste importante.

Les données les plus récentes de l'Union internationale des télécommunications (UIT, 2021) estiment que 63% de la population mondiale (soit 4,9 milliards de personnes) utilisait Internet en 2021. Alors que 90% de la population des pays développés utilisait Internet en 2021, le taux d'utilisateurs n'était que de 27% dans les pays les moins avancés.

ENCADRÉ 3

L'AUGMENTATION DU TRAFIC INTERNET MONDIAL IMPLIQUE UNE APPROCHE GLOBALE DE LA CONNECTIVITÉ NUMÉRIQUE

Le trafic mondial en protocole Internet, qui est un indicateur des flux de données, a augmenté de manière spectaculaire depuis 2000. De 100 gigaoctets (Go) par jour en 1992, 100 Go par seconde en 2002 à 46 000 Go par seconde en 2017, le trafic mondial en protocole Internet devrait atteindre 150 000 Go par seconde en 2022 (Cisco, 2018).* Les demandes de connexions fiables et rapides devraient continuer d'augmenter compte tenu du nombre toujours plus important de dispositifs de l'IdO connectés à Internet. Selon une estimation, l'IdO sera constitué de plus de 30 milliards de dispositifs d'ici à 2025 (soit plus de quatre objets par personne), ce qui représente une croissance mondiale de plus de 150% sur 5 ans à compter de 2020.**



* *Source* : Calculs de la Banque mondiale; et Cisco (2018).

** Voir https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide.

> « Le commerce contribue au transfert de technologie au-delà des frontières et aide à réduire la fracture numérique. »

Tous les pays connaissent une fracture numérique entre zones urbaines et zones rurales. Si pratiquement toutes les zones urbaines dans le monde sont couvertes par des réseaux mobiles à large bande, dans les zones rurales, les lacunes sont nombreuses. L'arrivée de la technologie 5G offrant aux appareils un accès aux services à large bande pourrait aggraver encore la fracture numérique, puisque les appareils des anciennes générations, comme la 3G, pourraient ne pas être en mesure d'accéder à ces services.

Le coût élevé de l'accès à Internet par rapport au revenu reste l'un des principaux obstacles à l'utilisation des services des TIC dans le monde entier. Le coût moyen d'un forfait de données mobiles de 1,5 Go dans les pays en développement, les pays les moins avancés, les pays en développement sans littoral et les petits États insulaires en développement est le plus souvent supérieur à 2% du revenu national brut mensuel par habitant (objectif fixé pour 2025 par la Commission « Le large bande au service du développement numérique »). En plus de l'abordabilité, l'utilisation effective d'Internet peut être entravée par des facteurs tels que :

- le faible niveau d'éducation;
- l'absence de contenus pertinents et dans la langue locale;
- l'absence de compétences numériques;
- une connexion Internet de faible qualité.

Renforcer la concurrence dans les pays en développement pourrait améliorer la qualité des services à large bande internationaux. L'UIT[1] indique que :

> « Cette difficulté est aggravée par le fait que certains pays en développement, voire des régions entières, ne sont pas encore desservis par les câbles de communication sous-marins, ce qui les rend tributaires de l'accès par satellite, qui est plus cher. Le problème du coût est exacerbé lorsque la passerelle internationale qui transmet les données IP vers d'autres pays n'est disponible qu'auprès d'un fournisseur monopolistique historique qui n'est confronté à aucune concurrence en matière de tarifs. … En conséquence, les prix tendent à rester élevés. »

Quel rôle les accords commerciaux peuvent-ils jouer pour aider à réduire la fracture numérique en termes d'infrastructure?

Les accords commerciaux ont contribué aux changements de grande ampleur intervenus depuis 2010 sur le marché des télécommunications, tant pour le matériel que pour les logiciels. Les efforts multilatéraux, plurilatéraux et régionaux mis en lumière dans les sous-sections ci-après devraient être poursuivis plus avant par les gouvernements pour promouvoir la connectivité mondiale pour tous. Le commerce, sous toutes ses formes, y compris l'investissement étranger direct, peut accroître la concurrence, en poussant à la baisse les coûts de la connectivité et en améliorant la qualité. Le commerce contribue aussi au transfert de technologie au-delà des frontières, et aide ainsi à réduire la fracture numérique. Certains accords commerciaux ont apporté des contributions substantielles à cet égard.

Les engagements en matière d'accès aux marchés dans le domaine des services de télécommunication

Plus de 120 Membres de l'OMC ont pris des engagements en faveur de l'ouverture des marchés dans le domaine des services de télécommunication, dont la plupart s'applique aux services de base tels que la téléphonie fixe et mobile et la transmission de données en temps réel. Ces engagements englobent des garanties concernant, par exemple, l'établissement de nouvelles sociétés de télécommunications, l'investissement étranger direct dans des sociétés existantes et la transmission transfrontières de services de télécommunication. Cependant, de nombreuses restrictions des échanges persistent dans le domaine des services de télécommunication (voir le tableau 1) et les procédures restent souvent complexes et lourdes sur le plan administratif (par exemple, le nombre de documents nécessaires pour obtenir une licence commerciale va de 2 à 19). D'autres engagements en matière d'accès aux marchés pourraient réduire ces obstacles.

Concurrence dans les secteurs de services de télécommunication

Plus de 100 Membres de l'OMC se sont engagés à respecter les principes réglementaires énoncés dans le document de référence distribué en 1996 par le Groupe de négociation sur les télécommunications de base.[2] Les sauvegardes en matière de concurrence qui

TABLEAU 1

OBSTACLES À L'ACCÈS DANS LE SECTEUR DES TÉLÉCOMMUNICATIONS

Description de l'obstacle	Nombre de gouvernements maintenant un obstacle de ce type
La part des actions pouvant être acquises par des investisseurs étrangers dans des sociétés publiques est limitée.	18
L'acquisition et l'utilisation de terrains et de propriétés immobilières par des étrangers sont soumises à restrictions.	32
Des quotas s'appliquent aux fournisseurs de services indépendants.	10
Un examen des besoins du marché du travail s'applique pour les personnes transférées à l'intérieur d'une société.	36
Un examen des besoins du marché du travail s'applique pour les fournisseurs de services contractuels.	34
S'agissant des marchés publics, des préférences sont explicitement prévues pour les fournisseurs nationaux.	23
S'agissant des marchés publics, des seuils s'appliquent au-dessus desquels l'appel d'offres est assorti de conditions de concurrence favorisant les entreprises nationales.	20
Le gouvernement central ou les autorités des États ou des provinces contrôlent au moins une des grandes entreprises du secteur.	22

Source : Base de données sur l'indice de restrictivité des échanges de services numériques de l'Organisation de coopération et de développement économiques (OCDE).

y figurent garantissent que les fournisseurs de services de transmission de données peuvent interconnecter leurs systèmes à des conditions raisonnables et non discriminatoires dans un environnement réglementaire à la fois impartial et transparent, ce qui contribue à soutenir le développement de réseaux de transmissions sur un territoire et tient largement compte des meilleures pratiques en matière de réglementation des télécommunications. La concurrence est un moteur essentiel de l'investissement et, partant, de l'accès à la large bande à un prix abordable.

Adoptant une autre façon de stimuler la concurrence, certains ACR ont mis en place des sauvegardes en matière de concurrence concernant les fournisseurs d'accès à Internet (par exemple l'Accord sur l'économie numérique (SADEA)) ou les opérateurs contrôlant les systèmes de câbles sous-marins internationaux (par exemple l'Accord de partenariat transpacifique global et progressiste), soutenant ainsi l'interconnexion à des conditions commerciales non discriminatoires. Pour promouvoir le développement de l'infrastructure de connectivité, le SADEA met en place des obligations de transparence et simplifie les procédures de délivrance des licences requises pour l'installation, la maintenance ou la réparation des systèmes de câbles sous-marins. À l'OMC, les Membres participant à l'initiative conjointe sur le commerce électronique examinent également une éventuelle révision du document de référence de l'OMC pour inclure tous les services de télécommunication et d'accès à Internet.[3]

Neutralité du réseau

Les ACR les plus récents ont introduit un principe de neutralité du réseau pour veiller à ce que les fournisseurs de services d'accès à Internet traitent de manière égale toutes les transmissions de données. Ce résultat s'appuie sur l'annexe sur les télécommunications[4] figurant dans l'Accord général sur le commerce des services (AGCS), qui dispose, à son article 5, ce qui suit :

> « a) Chaque Membre fera en sorte que tout fournisseur de services de tout autre Membre se voie accorder l'accès aux réseaux et services publics de transport des télécommunications et l'usage de ces réseaux et services suivant des modalités et à des conditions raisonnables et non discriminatoires, pour assurer la fourniture d'un service (…) ».

L'inclusion systématique de la neutralité du réseau dans les accords commerciaux aiderait à faire en sorte que les utilisateurs aient accès à Internet à des conditions raisonnables et non discriminatoires.

L'Accord sur les technologies de l'information de l'OMC

Initialement signé par 29 Membres de l'OMC en 1996, l'ATI a contribué à la suppression des droits de douane sur les produits des technologies de l'information et couvre 97% du commerce mondial de ces produits (OMC, 2017). En 2015, plus de 50 Membres de l'OMC sont convenus d'un élargissement de l'ATI, qui porte maintenant sur 201 produits supplémentaires. En 2020, les exportations mondiales de produits visés par l'ATI et par l'élargissement de l'ATI ont représenté plus de 20% des exportations mondiales de produits manufacturés.[5]

Les petites entreprises ont beaucoup à gagner d'un meilleur accès aux TIC grâce à l'ATI, car elles voient une dynamisation de leur compétitivité et une amélioration de leurs chances d'accéder au marché international. Ezell et Wu (2017) indiquent que « [l]es entreprises des pays en développement basées sur les TIC étaient deux fois plus rentables que les entreprises qui ne les utilisaient pas; leur productivité était supérieure de 65%, et elles créaient 25% d'emplois de plus. »

Cet accord plurilatéral et son élargissement sont ouverts à l'ensemble des Membres de l'OMC et plusieurs d'entre eux examinent la possibilité d'y adhérer. En juillet 2021, la République démocratique populaire lao a annoncé qu'elle adhèrerait à l'ATI et à l'ATI élargi, devenant ainsi le premier PMA à accéder à ces deux accords.[6]

Il importe de noter que les gains en termes d'accès aux marchés découlant de la libéralisation tarifaire peuvent perdre tout leur sens s'ils sont fragilisés par des mesures non tarifaires discriminatoires ou non nécessaires. Simplifier et rationaliser les mesures non tarifaires, telles que les procédures d'évaluation de la conformité ou les prescriptions en matière d'étiquetage pour les produits informatiques, devraient donc être un objectif essentiel, parallèlement à la libéralisation tarifaire.

Cohérence et coopération réglementaire au sujet des règles de cybersécurité

Il y a eu une augmentation récente des notifications de mesures liées aux obstacles techniques au commerce (OTC) portant sur la cybersécurité de l'IdO, de la technologie 5G, des dispositifs d'impression 3D, des drones et des véhicules autonomes, mesures qui visent à pallier les abus éventuels pour des raisons de sécurité du public et de sécurité nationale, de sûreté et de performance des produits 5G et d'interopérabilité (Hoe Lim, 2021).

Afin d'améliorer la cybersécurité de l'équipement, de l'infrastructure et des produits reposant sur des logiciels et connectés à un réseau, les gouvernements s'appuient dans une large mesure sur des systèmes de certification et d'étiquetage. Bien que les approches réglementaires de la certification de la cybersécurité soient généralement envisagées comme des méthodes volontaires, une tendance émerge selon laquelle les systèmes et leurs prescriptions pourraient devenir obligatoires. Des approches réglementaires divergentes pourraient faire obstacle au transfert de technologie et ainsi empêcher une réduction de la fracture numérique.

L'Accord OTC encourage une cohérence réglementaire au niveau mondial (grâce au partage et à l'examen des normes internationales avant leur mise en œuvre) et une coopération réglementaire au niveau mondial (grâce aux bonnes pratiques réglementaires, à l'équivalence et à la reconnaissance mutuelle). Cependant, si on les compare à d'autres domaines réglementaires comme la cybersécurité, les normes internationales sont souvent complétées par des règlements et normes nationaux, ce qui entretient la fragmentation réglementaire.

Les accords commerciaux pourraient encourager l'utilisation et l'élaboration de normes et de systèmes de reconnaissance mutuelle internationaux, comme les Critères communs (voir l'encadré 4) afin de promouvoir la convergence réglementaire. L'interopérabilité entre les normes internationales devrait aussi être envisagée. Tout comme la fragmentation réglementaire, des normes internationales non interopérables augmenteront les coûts de vérification et de mise en conformité à charge des entreprises.

Les principes de l'OMC devant régir l'élaboration de normes, guides et recommandations internationaux visent à éviter d'élaborer des normes contradictoires.[7] Ces six principes ont été convenus par le Comité OTC en 2000 afin de donner des orientations aux Membres de l'OMC lorsqu'ils élaborent des normes internationales :

1. transparence
2. ouverture
3. impartialité et consensus
4. efficacité et pertinence
5. cohérence
6. dimension développement

Bien que ces principes aient été adoptés dans le contexte de l'Accord OTC, qui s'intéresse au commerce des marchandises, ils sont également pertinents pour les normes internationales relatives au commerce numérique des services. Les six principes sont désormais si largement acceptés par les Membres de l'OMC, tant au niveau multilatéral qu'au niveau régional, qu'un nombre croissant d'ACR les incluent dans les chapitres qu'ils consacrent aux OTC et, qui plus est, les rendent obligatoires (McDaniels *et al.*, 2018).

Certains organismes internationaux à activité normative, comme l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI), ont également adopté ces principes.

Utiliser le Comité OTC pour examiner les préoccupations commerciales ayant trait aux règles de cybersécurité pourrait aider à répondre à ces préoccupations avant qu'elles ne se transforment en des différends formels à l'OMC, et donc permettre de résoudre ces problèmes plus rapidement, ce qui profiterait au transfert de technologie et à la réduction de la fracture numérique.

Transfert de technologie

Plusieurs dispositions des Accords de l'OMC mentionnent la nécessité d'un transfert de technologie entre les pays développés et les pays en développement Membres. Néanmoins, les modalités de ce transfert ne sont pas spécifiées. Par exemple, le transfert et la diffusion de technologie font partie des objectifs de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC) de l'OMC, qui prescrit spécifiquement aux pays développés Membres d'offrir des incitations à leurs entreprises pour promouvoir le transfert de technologie vers les pays les moins avancés. De même, l'article 6 de l'Annexe sur les télécommunications de l'AGCS dispose ce qui suit :

> « d) Les Membres accorderont une attention spéciale aux possibilités, pour les pays les moins avancés, d'encourager les fournisseurs étrangers de services de télécommunication à les aider en ce qui concerne le transfert de technologie, la formation et d'autres activités à l'appui du développement de leur infrastructure de télécommunication et de l'expansion de leur commerce des services de télécommunication. »

« Bien que les six principes devant régir l'élaboration de normes, guides et recommandations internationaux aient été adoptés dans le contexte de l'Accord OTC, qui s'intéresse au commerce des marchandises, ils sont également pertinents pour les normes internationales relatives au commerce numérique des services. »

ENCADRÉ 4

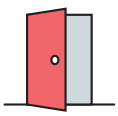
CRITÈRES COMMUNS

Les Critères communs donnent des conseils techniques relatifs à la cybersécurité et aux régimes de certification des produits et systèmes des TIC. Ils sont étayés par la Méthodologie commune pour l'évaluation de la sécurité des technologies de l'information (MCE), qui décrit de quelle manière les évaluations devraient être menées. L'Accord sur la reconnaissance de critères communs (CCRA) garantit l'acceptation mutuelle des certificats de sécurité au niveau international. Les produits des TIC qui obtiennent un certificat fondé sur les Critères communs peuvent être achetés ou utilisés sans évaluation supplémentaire. Par ailleurs, ces normes internationales contribuent grandement à renforcer la confiance dans la sécurité des produits des TIC à l'échelle internationale. Le CCRA a été signé en 1998 et compte aujourd'hui 31 parties.

Au niveau régional, un accord de reconnaissance mutuelle (ARM) équivalent a été signé en 1998 : l'ARM du Groupe de hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS) réunit 15 États membres de l'UE et de l'AELE.

Ces dispositions devraient être rendues pleinement opérationnelles et les accords commerciaux pourraient spécifier ces modalités. Les meilleures pratiques en matière d'incitations visant à réduire la fracture numérique pourraient être partagées au Groupe de travail sur le transfert de technologie de l'OMC.[8]

B | ALIGNEMENT MONDIAL SUR LA RÉGLEMENTATION DES CONTENUS CONCERNANT LES DONNÉES ET SUR LES CADRES DE RESPONSABILITÉ POUR SOUTENIR LES FLUX DE DONNÉES TRANSFRONTIÈRES



La seconde source d'obstacles aux flux de données transfrontières provient des mesures réglementaires concernant le contenu des données (c'est-à-dire les renseignements transmis proprement dits). La teneur des données peut être de nature personnelle, sensible ou confidentielle et peut exposer des particuliers ou des organisations à des risques tels que, par exemple, l'accès non autorisé à des renseignements personnels ou commerciaux confidentiels ou à un dispositif connecté à Internet et l'utilisation non autorisée de ces renseignements ou de ce dispositif; des menaces en matière de cybersécurité visant des infrastructures et des renseignements essentiels; une perte de connectivité; ou une discrimination en matière de prix fondée sur des renseignements personnels.

De nombreux incidents concernent des vulnérabilités en matière de cybersécurité, même si certaines menaces délictueuses dans ce domaine peuvent aussi affecter les entreprises au moyen d'un piratage direct (voir l'encadré 5) ou en ciblant une organisation de sa chaîne d'approvisionnement. À mesure que le nombre de personnes et de machines communiquant en ligne augmente, la probabilité de risques liés aux données et la gravité de leurs répercussions augmenteront elles aussi, en particulier pour les petites entreprises, qui sont les plus vulnérables.

Dans le monde numérique, les vulnérabilités d'une entreprise ont une incidence sur les autres entreprises qui partagent des renseignements dans la même chaîne d'approvisionnement. D'une manière plus générale, les vulnérabilités d'une économie pourraient empêcher des entreprises étrangères d'offrir leurs technologies aux parties prenantes de cette économie. Ces niveaux différents de maturité en matière de cybersécurité des entreprises et des économies doivent être pris en compte pour soutenir l'adoption

ENCADRÉ 5

COMMENT LE PIRATAGE OU LES VULNÉRABILITÉS EN MATIÈRE DE CYBERSÉCURITÉ PEUVENT AFFECTER LE COMMERCE INTERNATIONAL

Dans le cadre d'un système de mainlevée électronique, les transporteurs émettent, sur présentation d'un connaissement, un code PIN généré par ordinateur, qui est envoyé par courrier électronique dans une note de consignation à l'attention des récepteurs ou de leurs agents et au terminal portuaire qui prennent livraison des marchandises.

À l'arrivée, au moment où l'agent tente de réceptionner les conteneurs, il découvre que deux d'entre eux ont déjà été réceptionnés par des personnes non autorisées. La question de savoir comment les voleurs ont eu accès aux codes reste floue – ce peut être via l'infrastructure informatique du destinataire ou de l'envoyeur.

Note: Voir l'affaire jugée en 2017 devant la Cour d'appel de l'Angleterre et du Pays de Galles, opposant la Mediterranean Shipping Company (MSC) et Glencore ([2017] EWCA Civ 365).

> « Les niveaux différents de maturité en matière de cybersécurité des entreprises et des économies doivent être pris en compte pour soutenir l'adoption et l'évolutivité mondiales des technologies au service du commerce.

et l'évolutivité mondiales des technologies au service du commerce. La cybersécurité doit être traitée comme si elle était un bien public mondial.

Les technologies de pointe rendent encore plus difficile l'application des lois sur la protection des données. Par exemple, identifier les responsables du contrôle et du traitement des données[9] peut être très compliqué dans des systèmes basés sur des chaînes de blocs sans permission. Les participants saisissant des données personnelles dans des blocs du registre peuvent évidemment être considérés comme responsables du contrôle des données qu'ils ont fournies ou auxquelles ils ont accès via le système, à moins qu'ils interviennent en tant que fournisseurs de services technologiques soutenant le système, auquel cas ils seraient plutôt considérés comme responsables du traitement des données.

Étant donné que les juridictions répondent à ces menaces de manière unilatérale, la fragmentation réglementaire pourrait freiner la transmission mondiale de données et, au final, affecter l'accès aux marchés pour les entreprises qui dépendent du mouvement transfrontières des données. Pour les consommateurs, cette situation pourrait entraîner une diminution du nombre de produits, une augmentation des prix et une baisse de la qualité (voir l'encadré 6).

Comment les gouvernements gèrent-ils la réglementation des contenus et des données tout en préservant les flux de données transfrontières et les objectifs légitimes?

De nombreux gouvernements ont mis en place des lois et réglementations pour atténuer ces types de risques liés aux données, y compris des mesures de protection des données personnelles, des mesures visant les flux de données transfrontières, des mesures relatives à la sécurité des produits et des mesures de cybersécurité.

La fragmentation réglementaire peut créer un climat d'incertitude pour les consommateurs et les acteurs de la chaîne d'approvisionnement, qui ne savent pas si et comment ils peuvent avoir accès à des mesures correctives à l'étranger, et sur quel cadre régissant la responsabilité ils peuvent compter (voir l'encadré 7).

Certaines lois et réglementations s'appliquent à de nombreux secteurs, comme c'est le cas par exemple pour le Règlement général de l'UE sur la protection des données ou la Loi de la Chine sur la cybersécurité, qui a trait à des secteurs d'infrastructures essentielles. D'autres lois s'appliquent à des secteurs ou des technologies particulières, tels que les règlements relatifs à l'intelligence artificielle, aux véhicules autonomes et aux drones.

Certaines mesures utilisent une approche fondée sur les risques, tandis que d'autres adoptent une approche prescriptive. D'après des experts en cybersécurité, compte tenu de la nature évolutive des menaces dans ce domaine, une approche fondée sur les risques peut s'avérer plus efficace. Traiter la question de la cybersécurité dans le domaine des TIC au moyen d'une réglementation par produit ne se justifie sans doute pas, étant donné que toute évolution de la technologie rendrait cette réglementation très rapidement obsolète (Direction nationale du commerce de la Suède, 2018). Les approches réglementaires fondées sur les risques peuvent être bénéfiques pour les entreprises (notamment les petites entreprises) car elles évitent l'imposition de charges disproportionnées. En effet, plus l'entreprise est petite, plus la charge de mise en conformité est lourde.

Pour réglementer l'intelligence artificielle qui utilise des données personnelles, certains gouvernements ont adopté une approche fondée sur les risques. La Commission européenne propose un cadre d'évaluation de la conformité *ex-ante* qui imposerait aux entreprises de s'assurer que leurs produits et services faisant appel à l'IA adhèrent à certaines prescriptions spécifiques à l'UE avant de les proposer sur le marché européen ou de les mettre en service.

ENCADRÉ 6

PRESCRIPTIONS EN MATIÈRE DE DONNÉES BLOQUANT L'ENTRÉE SUR DE NOUVEAUX MARCHÉS

Dorae* propose un système logiciel flexible à ses clients pour numériser les documents commerciaux, automatiser les processus et assurer le suivi de l'origine des matières premières et des étapes de fabrication. Les clients décident des données qu'ils saisissent dans le système, sans vérification de la part de Dorae. Pour des raisons de sécurité et par commodité pour les clients, le système de Dorae est basé sur l'informatique en nuage, avec une infrastructure dans des centres de données commerciaux répartis dans le monde entier.

Dans le cadre de sa stratégie de croissance, Dorae a évalué son entrée sur un nouveau marché. Une grande partie de cette évaluation a été axée sur les prescriptions en matière de localisation des données sur le marché cible. Ces prescriptions imposaient que certains types de données soient stockées d'une certaine façon et qu'elles ne soient pas transmises à l'étranger pour des raisons de sécurité.

Étant donné que ce sont les clients qui décident des données qu'ils saisissent dans le système, Dorae ne pouvait pas être sûre à 100% que des renseignements proscrits ne seraient pas traités. Pour autant, Dorae serait quand même responsable en cas de violation.

Afin d'atténuer le risque, Dorae pouvait : limiter des fonctionnalités telles que le partage de renseignements entre clients; construire une infrastructure supplémentaire; ou modifier les conditions et modalités locales. Cependant, ces solutions étaient incomplètes ou coûteuses ou se traduisaient par une expérience utilisateur inférieure qui était incompatible avec la réputation de Dorae et la qualité de ses produits.

Dorae a conclu que les coûts initiaux et les risques juridiques non mesurables l'emportaient sur les perspectives de croissance à court terme, de sorte que l'entrée sur le nouveau marché a été suspendue. Il ne s'agissait pas simplement d'un débouché perdu pour l'entreprise, mais aussi d'une occasion manquée pour les parties prenantes à la chaîne d'approvisionnement qui auraient pu tirer avantage de chaînes d'approvisionnement jouissant d'une visibilité et d'une transparence accrues.

* Voir https://www.dorae.com.

ENCADRÉ 7

RESPONSABILITÉ

La capacité d'identifier spécifiquement et sans ambiguïté la personne responsable de tout dommage causé est essentielle pour garantir l'accès aux mesures correctives. Idéalement, le transfert de responsabilité doit être facilité, indépendamment de la solution numérique utilisée.

Du fait de l'opacité, de la connectivité et de l'autonomie des systèmes d'IA, qui peuvent impliquer plusieurs arrangements contractuels complexes (souvent transfrontières) faisant intervenir de nombreux acteurs, déterminer qui est responsable en remontant le fil des actions préjudiciables des systèmes d'IA jusqu'à l'élément humain de la saisie ou de la conception est extrêmement difficile. Par ailleurs, de nombreux modèles d'apprentissage automatique utilisent des systèmes d'apprentissage graduel qui sont impossibles à interpréter par les humains et la réglementation existante ne tient pas suffisamment compte de la nature dynamique de ces modèles d'apprentissage automatique qui, pourrait-on dire, « n'en font qu'à leur tête ».

Une autre difficulté concerne les éventuels dysfonctionnements dans le langage de programmation et le code machine exécutable, ou entre les deux, qui pourraient empêcher le code de faire ce qu'il est censé faire lorsqu'il est exécuté. Bien entendu, le risque d'un dysfonctionnement existe dans tout programme d'ordinateur. Le problème principal de la détermination de la responsabilité dans les systèmes de chaîne de blocs (sans permission) est la difficulté à déterminer la relation entre les nombreuses parties impliquées : i) le groupe restreint, qui se charge de la conception du code; ii) les propriétaires de serveurs supplémentaires sur lequel tourne le code de la DLT à des fins de validation; iii) les utilisateurs de la DLT; et iv) les tierces parties affectées par le système sans dépendre directement de la technologie.

Habituellement, dans les chaînes de blocs sans permission, les utilisateurs de nœud ne savent même pas qui exploite les autres nœuds. En conséquence, il peut se révéler difficile d'identifier un défendeur potentiel auprès de qui demander réparation en droit, et encore plus difficile d'obtenir sa véritable identité. En revanche, les chaînes de blocs avec permission ont leurs propres règlements, qui définissent les responsabilités. Cette situation est toutefois problématique, puisque des plates-formes de chaînes de blocs et de DLT différentes peuvent adopter des méthodes différentes, ce qui peut affecter l'interopérabilité. Il pourrait être nécessaire de préciser ces points pour soutenir l'adoption plus large des chaînes de blocs et de la DLT dans le commerce.

De nombreuses responsabilités non contractuelles peuvent potentiellement découler des transactions effectuées dans le cadre de contrats intelligents (par exemple les plaintes pour fraude, pratiques commerciales déloyales, opérations d'initiés ou abus de marché), qui pourraient être un domaine de risque intéressant les compagnies d'assurance. Il sera toutefois délicat de déterminer les conditions auxquelles une assurance s'appliquera dans ce domaine.

La technologie au service du commerce exigera une adaptation des cadres de responsabilité existants ou l'élaboration de nouveaux cadres. Ces initiatives devraient être coordonnées à l'échelle mondiale afin d'éviter la fragmentation réglementaire, les obstacles au commerce et la méfiance des consommateurs. À cet égard, certains gouvernements envisagent d'étendre aux produits reposant sur des logiciels et connectés à un réseau leur cadre national de responsabilité du fait des produits et de sécurité des produits. Préciser la portée des cadres de responsabilité du fait des produits et de sécurité des produits pour ce qui concerne l'IdO offrirait aux consommateurs une protection accrue et une meilleure certitude juridique.

« Les accords commerciaux jouent un rôle essentiel dans la promotion de la convergence réglementaire concernant les flux de données. »

Que peuvent faire les accords commerciaux pour encourager une réglementation du contenu des données qui soutienne des flux de données transfrontières fiables?

Différents canaux ont été utilisés du point de vue des politiques commerciales pour promouvoir les transmissions de données mondiales, mais il subsiste des possibilités inexploitées.

Convergence réglementaire

Les accords commerciaux jouent un rôle essentiel dans la promotion de la convergence réglementaire concernant les flux de données. Quelque 105 ACR invitent les gouvernements à mettre en place des cadres nationaux pour la protection des données personnelles, et 47 d'entre eux exigent des gouvernements qu'ils tiennent compte des normes internationales.[10] De même, de nombreux ACR contiennent des dispositions sur la cybersécurité qui encouragent les gouvernements à renforcer les capacités dans ce domaine et à soutenir la coopération internationale. Il subsiste toutefois de nombreuses possibilités inexploitées.

S'agissant des règles régissant la vie privée, l'approche générale de la réglementation des flux de données transfrontières consiste à garantir un niveau approprié de protection des données sur deux territoires ou davantage. La coopération réglementaire entre certains gouvernements s'est traduite par l'introduction de systèmes d'équivalence (par exemple des décisions d'adéquation) et de systèmes de certification régionaux (par exemple le système de règles de confidentialité transfrontières du Forum de coopération économique Asie-Pacifique (APEC)) visant à établir ce niveau équivalent de protection, mais la portée de ces mécanismes reste limitée. Une coopération réglementaire internationale plus poussée est nécessaire pour que ces mécanismes aient réellement une portée globale.

Seuls quelques rares ACR facilitent l'interopérabilité entre les mécanismes de flux de données transfrontières. Par exemple, l'article 19.8 de l'Accord entre les États-Unis, le Mexique et le Canada fait explicitement référence au système de règles de confidentialité transfrontières de l'APEC et reconnaît que ce système est « un mécanisme valable pour faciliter les transferts transfrontières de renseignements tout en protégeant les renseignements personnels. » L'article 4.2 10) de l'Accord de partenariat pour l'économie numérique (DEPA) encourage aussi ses parties signataires à reconnaître mutuellement la protection des données des autres parties quand elle est formulée exactement dans les mêmes termes. Soutenir systématiquement la présence de ces mécanismes dans les accords commerciaux peut aider à les faire connaître aux entreprises et à encourager celles-ci à les utiliser. Une coordination au niveau multilatéral sera nécessaire pour empêcher les mécanismes de transfert de données de terminer en silos de données.

L'initiative « Osaka Track » est une initiative internationale majeure sur les flux de données, lancée par les chefs de gouvernements sous la direction du G-20 du Japon en 2019. Le cadre de « libre circulation des données en toute confiance » – le concept essentiel sous-tendant l'initiative « Osaka Track » – cartographie une architecture multidimensionnelle pour la coopération internationale en matière de flux de données, entre gouvernements et en impliquant les entreprises, et inclut des recommandations pour augmenter les niveaux de confiance en matière de gouvernance et renforcer l'ouverture au moyen de règles commerciales et d'autres outils (Forum économique mondial, 2020b).

S'agissant des règles sur l'IA, les lignes directrices internationales qui commencent à émerger visent aussi à promouvoir la cohérence réglementaire. On peut citer :

- les principes de l'OCDE sur l'IA (OCDE, 2022);
- le Plan d'action du G-20 pour une nouvelle révolution industrielle;
- La déclaration conjointe du G-20 sur une IA centrée sur l'humain et l'approbation ultérieure des principes de l'OCDE sur l'IA dans la Déclaration ministérielle du G-20 sur le commerce et l'économie numérique de juin 2019;
- le Partenariat mondial sur l'intelligence artificielle (PMIA) du G-7;
- le Comité d'experts du Conseil de l'Europe sur la dimension droits de l'Homme des traitements automatisés de données et différentes formes d'intelligence artificielle;
- la normalisation dans le domaine de l'IA par le Comité technique mixte ISO/CEI.

Tandis que les gouvernements financent le développement de l'IA, il sera utile qu'une part de ces fonds soit consacrée à l'interopérabilité. Quelques rares accords commerciaux, comme le DEPA, contiennent des dispositions dans lesquelles les parties reconnaissent les avantages qu'il y a à élaborer une compréhension mutuelle et à veiller à ce que (voir les paragraphes 2 et 4 de l'article 8) :

> « les cadres éthiques et de gouvernance pour une utilisation responsable, sûre et en toute confiance des technologies d'IA … [soient] alignées au niveau international, afin de faciliter, dans toute la mesure du possible, l'adoption et l'utilisation de technologie d'IA dans les juridictions respectives des Parties … [et] … s'efforcent de prendre en considération les principes ou lignes directrices reconnus à l'échelle internationale, y compris l'explicabilité, la transparence, l'équité et les valeurs axées sur l'humain. »

Les accords commerciaux pourraient promouvoir des lignes directrices internationales sur la gouvernance de l'IA avant de constater une approche cloisonnée nationale ou régionale à la réglementation de l'IA. Une convergence réglementaire soutiendrait l'adoption et l'utilisation globales des technologies d'IA dans le domaine du commerce. Une fragmentation réglementaire conduira quant à elle à l'émergence d'obstacles supplémentaires.[11]

Coopération en matière de cybersécurité et échange de données entre gouvernements à des fins d'application des lois et de surveillance réglementaire

Avant que les accords commerciaux incluent la coopération en matière de cybersécurité pour répondre aux menaces sans frontières, plusieurs questions essentielles doivent encore être examinées. Quelque 50 ACR contiennent des règles qui encouragent le renforcement des capacités des entités nationales chargées de répondre aux incidents de sécurité informatique et de développer la main-d'œuvre au moyen de la reconnaissance mutuelle des qualifications et de l'échange transfrontières de renseignements pour déceler et réduire les cas d'intrusion malveillante ou de diffusion de codes malveillants affectant les réseaux électroniques à l'échelle mondiale. Cependant, ces dispositions sont axées sur les entités chargées de répondre aux incidents de sécurité informatique, et ignorent donc l'échange de renseignements entre organismes gouvernementaux, par exemple entre autorités chargées de l'application des lois. Les dispositions sur la cybersécurité font aussi l'objet de discussions dans le contexte de l'initiative conjointe de l'OMC sur le commerce électronique.

La coopération en matière de cybersécurité devrait viser à réduire les écarts de capacités des économies et des entreprises dans ce domaine. Compte tenu de la différence en termes de ressources d'information, et en termes de connaissances et d'infrastructure utilisées pour les protéger, certaines économies et certaines entreprises sont plus vulnérables que d'autres, ce qui compromet la fiabilité d'Internet au-delà des frontières. Renforcer les capacités de prévention, plutôt que de se contenter de réagir en cas de cyberattaque, est essentiel pour promouvoir la fiabilité transfrontières et garantir que les réponses réglementaires (par exemple les prescriptions en matière de certification) soient bien appliquées. Il n'est pas très utile d'élaborer, d'adopter et de mettre en place des réponses réglementaires (souvent complexes et coûteuses) s'il n'existe pas de processus d'exécution efficaces. Les accords commerciaux devraient encourager les gouvernements à renforcer les capacités d'exécution de la réglementation des parties prenantes auxquelles incombent des responsabilités en matière de cybersécurité.

Aucun accord commercial n'aborde la question de l'inefficacité des procédures d'assistance juridique mutuelle. Le long processus d'examen figurant dans les accords d'assistance juridique mutuelle (AAJM) va souvent à l'encontre de l'objectif des demandes de données présentées via ce mécanisme, puisque les organismes d'application de la loi ne sont pas à même d'obtenir des éléments de preuve essentiels dans un délai approprié. Il en résulte que certains gouvernements ont opté pour des mesures de localisation des données dans le but d'accélérer l'accès à ces éléments en rendant le gouvernement du pays cherchant à localiser les données moins tributaire du gouvernement étranger dans la juridiction duquel les données pertinentes sont stockées. Afin de limiter la prolifération des mesures de ce type, il est impératif que les décideurs et autres parties prenantes reconnaissent la nécessité d'un régime de partage international des données aux fins de l'application des lois plus efficace et plus performant que celui prévu par les AAJM existants. Pour faciliter l'échange de données en temps utile entre organismes gouvernementaux aux fins de l'application des lois, les négociateurs commerciaux pourraient tirer parti de l'élan politique généré par la négociation d'accords commerciaux pour réformer les AAJM. De plus, les accords commerciaux pourraient autoriser ou encourager les responsables de la réglementation à échanger directement entre eux des

documents électroniques plutôt qu'avoir recours au processus prévu par les AAJM.

Certains pays examinent unilatéralement d'autres solutions, que les accords commerciaux pourraient prendre en considération, voire mobiliser – de préférence au niveau multilatéral. Un exemple d'approche visant à faciliter l'accès des organismes gouvernementaux aux données aux fins de l'application des lois est le Décret législatif n° 56 de 2018 du Royaume de Bahreïn relatif à la fourniture de services d'informatique en nuage à des parties étrangères. En vertu de cet instrument législatif, les données stockées dans des centres de données dans le Royaume de Bahreïn sont assujetties au droit national de l'État où le consommateur réside (ou où il est constitué en société dans le cas d'une personne morale) et relèvent ainsi de la juridiction des tribunaux et autres autorités compétentes de l'État en question.

Collaboration et concurrence sur les marchés fondés sur les données

Les flux de données transfrontières peuvent aussi être freinés par certaines tendances oligopolistiques qui entraînent un enfermement du consommateur vis-à-vis des services de données. Bien que les données soient générées sur différents marchés, dans certains cas, elles sont principalement stockées, traitées et exploitées commercialement dans un petit nombre de régions. Le choix et la concurrence sont essentiels pour garantir que des éléments numériques infrastructurels importants et la numérisation du commerce mondial ne soient pas sous le contrôle d'une seule personne ou entreprise, d'un seul pays ou d'une seule région.

Quelque 40 ACR conviennent d'examiner des approches adéquates pour promouvoir et protéger la concurrence sur les marchés numériques et de renforcer les mécanismes de collaboration afin d'identifier et d'atténuer les distorsions du marché résultant d'abus de position dominante sur le marché. Cependant, seul un ACR à ce jour envisage des solutions à l'enfermement à l'égard des services de données. Le paragraphe 3 de l'article 9.4 du DEPA encourage les parties à « collaborer sur des projets et des mécanismes de partage de données et sur des démonstrations de faisabilité pour de nouveaux usages des données, tels que les laboratoires de réglementation en matière de données, afin de promouvoir une innovation fondée sur les données ». La question de la concurrence sur les marchés numériques est aussi abordée dans le contexte de l'initiative conjointe de l'OMC sur le commerce électronique.

Il existe d'autres initiatives gouvernementales qui pourraient être mobilisées par des accords commerciaux, comme le laboratoire de réglementation transfrontières entre l'Abu Dhabi Global Market (ADGM) et le Réseau d'innovation financière de l'Association des nations de l'Asie du Sud-Est (ASEAN), où de jeunes entreprises et des organismes financiers peuvent tester des technologies et des idées tout en partageant des données dans un environnement prévisible et réglementé; ou encore le laboratoire de réglementation entre l'ASEAN et des ministres responsables des TIC où les entreprises peuvent tester leurs services sans porter atteinte aux règles régissant la confidentialité des données ni craindre de sanctions réglementaires. Les accords commerciaux pourraient encourager les gouvernements à échanger leurs meilleurs pratiques sur les mécanismes existants de partage de données et sur la manière de résoudre au mieux les difficultés juridiques et techniques.

Processus réglementaires cohérents

La coordination bilatérale et internationale entre organismes gouvernementaux pour la conception et la mise en œuvre de la réglementation en matière de gouvernance des données contribue à promouvoir la cohérence réglementaire et, partant, la transmission mondiale de données. L'absence de coordination de la réglementation entre les autorités compétentes engendre non seulement une complexité juridique, mais peut aussi involontairement compromettre les possibilités économiques associées aux données.

Par exemple, une approche de la protection des données personnelles qui rend la mise en conformité difficile et coûteuse risque de réduire la valeur du partage des données, par exemple dans la fourniture de services transfrontières ou le suivi d'expéditions, de conteneurs et de produits tout au long des chaînes d'approvisionnement (voir l'encadré 8). De même, les organismes gouvernementaux travaillant dans le domaine de la réglementation de la cybersécurité se concentrent généralement sur la sûreté, la sécurité et la résilience des éléments et infrastructures essentiels et n'ont pas nécessairement conscience des implications sur l'ouverture, l'interopérabilité et le commerce. Comme d'autres initiatives concernant la politique et la réglementation dans le domaine de l'économie numérique, la réglementation des données doit être conçue en collaboration avec de multiples parties prenantes, y compris les responsables de la politique commerciale.

ENCADRÉ 8

L'INCIDENCE DE LA RÉGLEMENTATION DES DONNÉES ET DES CONTENUS SUR LA VISIBILITÉ DU TRANSPORT MARITIME

Les renseignements sur les volumes et les positions du fret permettent aux négociants d'optimiser la logistique en anticipant les congestions et en choisissant les routes maritimes en conséquence. En raison de la pandémie de COVID-19, la forte hausse de la demande de marchandises et la pénurie de conteneurs ont entraîné des perturbations dans les ports du monde entier, rendant les données sur le transport maritime encore plus importantes pour déterminer les délais de transport des expéditions.

Les nouvelles réglementations mises en place dans certaines juridictions ont poussé les fournisseurs nationaux de ces juridictions à cesser de communiquer des informations sur le transport à des entreprises étrangères, ce qui a eu de fortes répercussions sur la visibilité du transport maritime.

Source : Saul et Baptista (2021).

Les accords commerciaux pourraient encourager les gouvernements à promouvoir un dialogue entre leurs organismes réglementaires et les responsables de la politique commerciale et à favoriser l'échange des bonnes pratiques réglementaires. Cette approche aiderait : i) à établir une vision commune; ii) à améliorer la cohérence de la mise en œuvre et de la coordination; iii) à produire de la valeur à partir des données; et iv) à réduire les coûts des échanges. Cela revêt une importance toute particulière dans les cas où plusieurs entités sont impliquées dans la réglementation des données, ce qui pourrait involontairement entraîner l'apparition de nouveaux obstacles au commerce.

NOTES DE FIN

1. Voir https://www.itu.int/en/ITU-T/studygroups/2013-2016/03/Pages/iic.aspx.
2. Le Document de référence est un ensemble de principes réglementaires juridiquement contraignants pour les Membres de l'OMC qui se sont engagés à les appliquer en les annexant, en totalité ou en partie, à leur liste d'engagements. Voir https://www.wto.org/french/tratop_f/serv_f/telecom_f/tel23_f.htm.
3. Voir https://www.wto.org/french/news_f/news21_f/ecom_20apr21_f.htm.
4. L'annexe sur les télécommunications concerne les réseaux et services publics de transport des télécommunications : le terme « services de transport » s'entend des services de transmission de données ; le terme « services publics » s'entend des services de transport des télécommunications qui doivent être proposés au public de manière générale. Ce terme fait référence à la structure du capital d'une société.
5. Voir https://www.wto.org/french/news_f/news21_f/ita_02dec21_f.htm.
6. Voir https://www.wto.org/french/news_f/news21_f/ita_30jul21_f.htm.
7. Voir https://www.wto.org/french/tratop_f/tbt_f/principles_standards_tbt_f.htm.
8. Voir https://www.wto.org/french/tratop_f/devel_f/dev_wkgp_trade_transfer_technology_f.htm.
9. Les définitions des responsables du contrôle des données et des responsables du traitement des données varient entre les différentes juridictions. En l'occurrence, ces termes devraient être compris dans le contexte du Règlement général de l'UE sur la protection des données.
10. Ensemble de données du TAPED en date du 25 janvier 2022, disponible à l'adresse https://www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped.
11. Certains font valoir, par exemple, que la proposition de l'UE en faveur d'un cadre d'évaluation de la conformité *ex ante* pourrait devenir un obstacle au commerce numérique fondé sur l'IA même si les produits sont utilisés en toute sécurité et avec efficacité dans d'autres juridictions (Forum économique mondial, 2020a).