

3 Les politiques en matière d'IA et le commerce

a) L'IA et le commerce : considérations de politique générale essentielles

Le débat sur la manière dont l'IA pourrait remodeler le commerce international soulève d'importantes questions de politique générale. L'avenir de l'IA et du commerce international dépend des choix des gouvernements en matière de politique générale et des stratégies et priorités des industries et des entreprises.

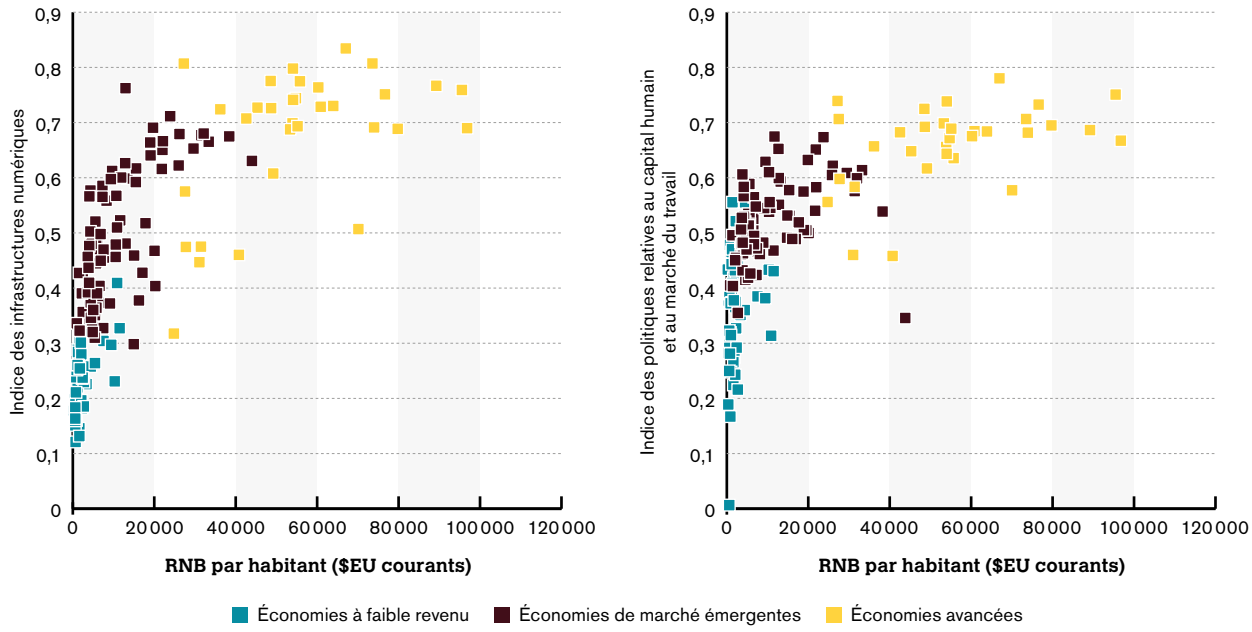
i) Remédier à la fracture grandissante en matière d'IA

Pour tirer parti des possibilités offertes par l'IA, il faut remédier à la fracture numérique entre les économies, en termes tant d'infrastructures que de compétences numériques. Comme nous l'avons vu au chapitre 2, il faut une infrastructure numérique solide et un capital humain formé pour faire en sorte que les travailleurs et les entreprises soient préparés pour adopter l'IA. L'infrastructure numérique est un déterminant essentiel de l'adoption des technologies de l'information et de la communication (TIC), et elle peut jeter les bases de la diffusion et de l'application localisée de la technologie de l'IA (Nicoletti *et al.*, 2020). Néanmoins, cette infrastructure est d'une utilité limitée sans une main-d'œuvre qualifiée capable de tirer parti des plates-formes numériques pour des applications innovantes sur le lieu de travail.

Les économies les plus riches, dont les économies avancées et certaines économies émergentes, sont généralement mieux préparées que les économies à faible revenu pour adopter l'IA. Comme le montre la figure 3.1, l'Indice des infrastructures numériques et l'Indice des politiques relatives au capital humain et au marché du travail – des composantes de l'Indice de préparation à l'IA du FMI – sont corrélés positivement aux niveaux de revenu. Les économies à revenu plus élevé ont tendance à disposer d'une infrastructure numérique plus solide et de davantage de capital humain formé, ce qui les rend mieux à même d'adopter les technologies de l'IA.

Pour remédier à la fracture en matière d'IA, il est essentiel d'investir dans l'infrastructure numérique pour faire en sorte que les économies à faible revenu disposent des bases technologiques nécessaires pour soutenir l'adoption de l'IA. Les gouvernements et le secteur privé pourraient collaborer pour élargir l'accès à Internet à haut débit, améliorer l'infrastructure électrique, en particulier grâce à la production d'énergie renouvelable, améliorer les capacités de stockage des données et élaborer des mesures solides en matière de cybersécurité. Les politiques publiques doivent encourager le développement des infrastructures dans les zones mal desservies et la coopération internationale devrait être axée sur la fourniture d'une assistance technique et financière aux économies en développement. Outre l'infrastructure, réduire la fracture en

Figure 3.1 : L'état de préparation à l'IA est plus élevé dans les économies avancées



Source : Indice de préparation à l'IA du Fonds monétaire international (FMI) (Cazzaniga *et al.*, 2024a). L'échelle des indices est modifiée pour qu'ils soient compris entre 0 et 1.

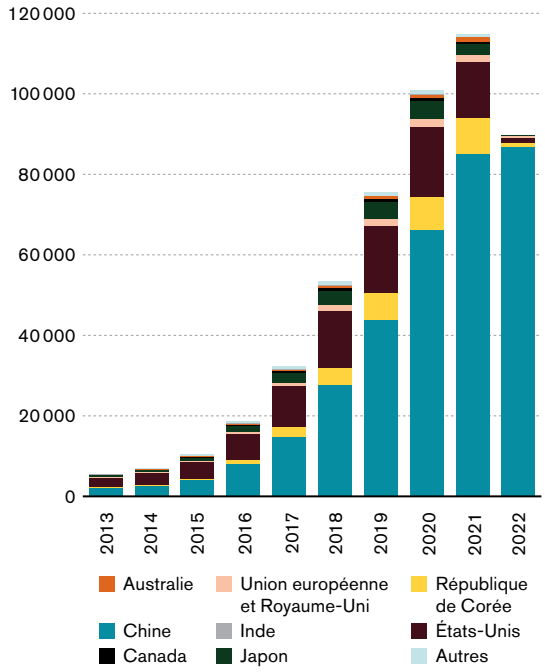
matière d'IA exige un investissement substantiel dans le capital humain pour doter les personnes des compétences dont elles ont besoin pour utiliser efficacement les technologies de l'IA. Les programmes d'enseignement et de formation devraient inclure la maîtrise de l'IA, le codage, l'analyse des données et d'autres compétences pertinentes. Les partenariats public-privé peuvent jouer un rôle clé dans ces efforts, car les entreprises peuvent offrir une formation pratique et des ressources, tandis que les gouvernements peuvent fournir le soutien réglementaire nécessaire, l'accès à des dispositifs et une connectivité à des coûts abordables, et des financements (voir l'article d'opinion de James Manyika).

Outre les différences dans la capacité d'adopter les technologies de l'IA, la fracture en matière d'IA entre les différentes économies, qui transparaît dans la recherche-développement (R-D), l'investissement et l'expertise dans le domaine de l'IA, met en lumière la nécessité de remédier aux écarts dans les capacités en matière d'IA. Il y a une fracture importante entre les économies chefs de file en ce qui concerne la recherche-développement dans le domaine de l'IA et les autres, en particulier les économies en développement et les pays les moins avancés (PMA). Comme le montre la figure 3.2, la Chine est de loin la première économie en termes du nombre de brevets enregistrés, avec 86 663 demandes de brevet déposées et 15 869 brevets accordés dans le domaine de l'IA en 2022, suivie par la République de Corée et les États-Unis.[1] Cette disparité reflète les différences technologiques sous-jacentes entre les économies et souligne qu'il est important de faciliter la diffusion des technologies et l'assistance technique pour combler l'écart au niveau mondial. Il existe une division marquée entre là où a lieu l'activité en matière de recherche, de brevets et d'investissement dans le domaine de l'IA et là où elle fait défaut, et il y a un risque croissant d'exacerber davantage cette division, qui existe à la fois entre les économies et au sein de celles-ci, ainsi qu'entre les zones urbaines et les zones rurales, moins connectées au numérique.

Le nombre d'articles publiés sur l'IA a régulièrement augmenté, le secteur privé prenant la tête. Le nombre d'articles publiés sur l'IA a régulièrement augmenté, sauf aux États-Unis, où il a baissé en 2022. Bien que la Chine soit en tête s'agissant du volume des articles scientifiques publiés, il convient de noter que les États-Unis se classent au premier rang pour ce qui est du nombre de citations, un indicateur de l'influence de la littérature.[2] Comme le montre la figure 3.3, l'affiliation des équipes menant des recherches et publiant des textes sur des systèmes d'IA qui « démontrent la capacité d'apprendre, montrent des résultats expérimentaux tangibles et contribuent à des avancées qui repoussent les limites des technologies de l'IA existantes » a connu un important changement dans la deuxième partie des années 2010 : alors que la plupart des recherches étaient menées par les milieux universitaires avant 2016, le secteur privé a pris la tête s'agissant du nombre de publications par la suite.

L'investissement dans l'IA s'accélère rapidement, les États-Unis se classant au premier rang des investissements privés. Le financement de l'IA provient

Figure 3.2 : Nombre de demandes de brevet en matière d'IA par région géographique, 2013-2022



Source : Centre for Security and Emerging Technology (2024).

de diverses sources, dont des sociétés privées, des sociétés de capital-risque, des fonds publics, des établissements universitaires, des sociétés en nom collectif et des investisseurs providentiels. Les États-Unis se classent au premier rang s'agissant de l'investissement privé total dans l'IA. En 2023, 67,2 milliards de dollars EU ont été investis dans l'IA aux États-Unis, soit environ 8,7 fois plus que dans le deuxième pays du classement, la Chine (7,8 milliards de dollars EU) et 17,8 fois plus qu'au Royaume-Uni (3,8 milliards de dollars EU). Depuis 2022, les États-Unis ont connu une augmentation notable de l'investissement privé dans l'IA (22,1 %) (Maslej *et al.*, 2024).

La disparité des investissements privés dans l'IA devient particulièrement marquée s'agissant de l'IA générative. Malgré une baisse récente de l'investissement privé global dans l'IA, le financement de l'IA générative s'est envolé, atteignant 25,2 milliards de dollars EU en 2023 (Maslej *et al.*, 2024). Toutefois, cette augmentation est fortement concentrée dans quelques économies, les États-Unis figurant en tête. En 2023, les États-Unis ont dépassé les investissements combinés de l'Union européenne et du Royaume-Uni dans l'IA générative d'environ 21,1 milliards de dollars EU. Ils ont également dominé les investissements en capital-risque dans l'IA générative, les investissements dans les réseaux antagonistes génératifs (modèles d'apprentissage machine qui génèrent de nouvelles données imitant un ensemble de données particulier) pour l'entraînement de l'IA et dans l'IA générative pour la production de textes, d'images et de sons ayant bondi dans le pays en 2023 pour atteindre plus de 16 milliards de dollars EU.[3]

Article d'opinion

La technologie au service d'une prospérité partagée

James Manyika

Premier Vice-Président en charge de la recherche, de la technologie et de la société chez Google ; Coprésident de l'Organe consultatif de haut niveau du Secrétaire général des Nations Unies sur l'intelligence artificielle

L'intelligence artificielle est la technologie la plus importante de l'ère actuelle ; elle offre la possibilité de faciliter la vie quotidienne des gens, de stimuler la croissance économique, d'aider les travailleurs de la classe moyenne et à faible revenu, de favoriser des avancées dans les domaines scientifique et sanitaire et de relever des défis de longue date en matière de développement. Dans un monde qui est en voie d'atteindre seulement 15% des Objectifs de développement durable (ODD) de l'ONU, l'IA offre la possibilité d'inverser cette tendance et de contribuer à réaliser des progrès sur 79% de nos objectifs mondiaux communs (Hoyer Gosselink *et al.*, 2024).

Toutefois, si les possibilités économiques et sociétales offertes par l'IA sont immenses, nous devons toujours garder à l'esprit que les avantages des nouvelles technologies ne sont pas automatiques. Alors que l'heure est à l'enthousiasme, il est important de prendre un peu de recul et d'examiner l'histoire du commerce et de la technologie, et de faire un effort concerté pour bâtir un système commercial inclusif autour de l'IA qui évite la création d'une « fracture en matière d'IA ».

Les forces conjuguées de la technologie et du commerce ont contribué à extraire plus d'un milliard de personnes de l'extrême pauvreté – un accomplissement sans précédent dans l'histoire de l'humanité.[4] Cette évolution a radicalement modifié le développement mondial, accélérant le flux des données et permettant aux petites entreprises et économies de participer au commerce. En 2016, les flux numériques – souvent un aspect essentiel d'autres flux mondiaux tels que les flux de produits manufacturés et de services ainsi que les flux financiers et d'autres biens incorporels – avaient commencé à avoir une plus grande incidence sur la croissance du PIB que les échanges de marchandises qui ont lieu depuis plusieurs siècles (Manyika *et al.*, 2016), le secteur des services, les industries manufacturières et le secteur du commerce de détail retirant une part surprenante des avantages issus du commerce numérique (Maison Blanche, 2024). Ces tendances concernant les flux mondiaux numériques et fondés sur le numérique n'ont fait que s'accélérer depuis 2016, certains estimant qu'une part du PIB allant jusqu'à 40% dépend d'ores et déjà des flux mondiaux (Seong *et al.*, 2022).

Avec l'IA, les économies sont maintenant sur le point de connaître une transformation économique et scientifique encore plus profonde, qui pourrait fondamentalement modifier et transformer la structure des échanges. Mais il est essentiel d'éviter de créer une « fracture en matière d'IA » (Ossa, 2023). En 2023, la part de la population utilisant Internet était de 93% dans les économies à revenu élevé, contre seulement 27% dans les économies à revenu faible (UIT, 2023). L'Organe consultatif de l'ONU sur l'IA a conclu à juste titre que ces fractures ne pouvaient pas persister à l'ère de l'IA (ONU, 2024a).

Nous devons travailler ensemble – entreprises, gouvernements et société civile – pour exploiter l'IA en vue de concrétiser la vision d'une prospérité partagée. Au niveau national, cela implique de donner accès à une infrastructure en nuage capable de prendre en charge l'IA, à des capacités de calcul, à des outils de développeur et à des ensembles de données pertinents pour le développement de l'IA, tout en dotant les travailleurs et les étudiants des compétences fondamentales en matière d'IA qui ouvrent des voies vers la main-d'œuvre moderne. Surtout, nous devons placer les petites entreprises et les industries traditionnelles telles que le secteur manufacturier et l'agriculture à l'avant-garde en matière d'IA.

Au niveau international, progresser vers la vision d'une prospérité partagée exigera d'élargir notre notion du « commerce » ; il s'agira non seulement d'éliminer les obstacles aux échanges transfrontières de biens et de services, mais aussi de mettre en place une stratégie mondiale visant à favoriser la cohérence de la gouvernance et des mesures de sécurité concernant l'IA, à soutenir des flux de données dignes de confiance, à permettre l'intégration économique et à trouver des solutions aux défis transfrontières. Une stratégie inclusive en matière d'IA doit aussi stimuler l'investissement dans les câbles sous-marins et terrestres qui permettent la participation à l'économie moderne (Quigley, 2024).

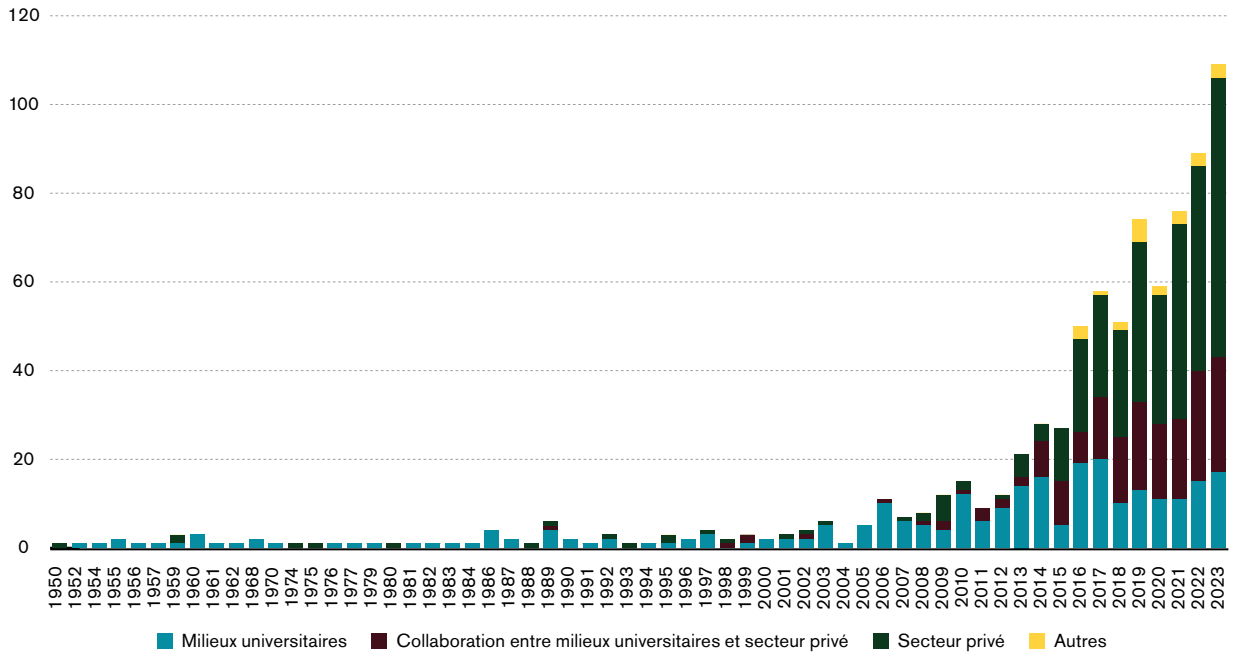
Fondamentalement, il s'agit là d'une forme moderne de renforcement des capacités, les gouvernements, le secteur privé et la société civile travaillant ensemble pour investir dans l'infrastructure d'IA, construire une ressource mondiale pour la recherche sur l'IA et élaborer des programmes de formation qui favorisent la diffusion de l'IA entre les secteurs et les régions géographiques.

En revanche, si les économies ne parviennent pas à mettre le commerce au service de la mission visant une prospérité partagée, l'IA risque de n'être adoptée que par les économies riches et par les industries les plus riches au sein de ces économies. Cela serait préjudiciable non seulement du point de vue de l'équité mais aussi d'un point de vue économique : pour que les avantages économiques que peut offrir l'IA, qui se chiffrent en milliers de milliards de dollars, se concrétisent, il faut que ces technologies soient largement adoptées, et non utilisées par seulement quelques privilégiés.

À nous de choisir. Ensemble, mettons au point un programme sur le commerce qui mette à profit le pouvoir de transformation de l'IA pour tous, indépendamment de la situation géographique ou économique.

Avertissement
Les articles d'opinion relèvent de la seule responsabilité de leurs auteurs. Ils ne reflètent pas nécessairement les opinions ou les vues des Membres ou du Secrétariat de l'OMC.

Figure 3.3: Affiliation des équipes de recherche et de publication, 1950-2022



Source : Epoch (2024).

Les professionnels ayant des compétences en matière d'IA sont en grande partie des hommes se trouvant en Europe et en Amérique du Nord. Selon une enquête réalisée auprès de développeurs par Stack Overflow, une plate-forme de questions-réponses pour les programmeurs,[5] 94,24 % des experts en science des données et des professionnels de l'apprentissage machine sont des hommes, et la plupart se trouvent en Europe et en Amérique du Nord (OECD.AI, 2024). En outre, des données de la Computing Research Association,[6] bien que limitées aux États-Unis et au Canada, montrent que la représentation des femmes parmi les nouveaux doctorats en IA et en informatique a stagné, la part des femmes restant proche de 20 % depuis 2010. Cet écart persistant entre les hommes et les femmes met en évidence un défi permanent dans ce domaine.

Ce déséquilibre peut être encore exacerbé par la course pour favoriser l'IA à l'aide de subventions publiques. Comme on l'a vu au chapitre 3 b), un certain nombre de gouvernements lancent des initiatives nationales visant à promouvoir l'IA, soutenues par un soutien généreux de l'État. Or, ce soutien étant fourni pour l'essentiel par des économies à revenu élevé, il risque d'exacerber la fracture en matière d'IA entre les économies. La concentration relative des chaînes d'approvisionnement de l'IA peut aussi entraîner des déséquilibres commerciaux dans les biens et services liés à l'IA.

Au-delà de la fracture numérique entre les économies, la concentration industrielle dans le domaine de l'IA s'observe au sein des économies en raison des rendements d'échelle croissants et des effets de réseau. Comme il est indiqué dans la section 2 b) iv), à mesure que le développement des modèles d'IA progresse et que les coûts associés à leur développement augmentent, seules les grandes entreprises peuvent se permettre d'effectuer les investissements de départ substantiels nécessaires. Cela crée un obstacle important pour les nouveaux arrivants et les petites entreprises et fait qu'il leur est difficile de soutenir la concurrence. Les coûts initiaux élevés du développement de modèles d'IA de pointe et la nécessité de disposer de nombreuses données et d'importantes ressources de calcul consolident encore la domination des acteurs établis.

L'adoption généralisée de l'IA sur les marchés peut renforcer le risque de collusion entre entreprises. Les systèmes d'IA intégrés dans les stratégies de fixation des prix et l'analyse des marchés peuvent permettre aux entreprises de surveiller le comportement de leurs concurrents en matière de fixation des prix et d'ajuster leurs propres prix en conséquence. Si cela peut permettre d'optimiser les bénéfices sur le plan individuel, il peut collectivement en résulter des accords tacites ou une collusion entre concurrents visant à maintenir des prix plus élevés (Assad *et al.*, 2024 ; OCDE, 2021a). En outre, la capacité de l'IA de traiter de vastes quantités de données et de prédire les tendances du marché risque de renforcer la coordination des stratégies de fixation des prix des différentes entreprises, accentuant ainsi la concentration du marché.[7]

Les caractéristiques particulières de l'IA posent des problèmes aux autorités chargées de la concurrence. L'opacité des algorithmes d'IA et le volume même des données qu'ils traitent peuvent occulter des pratiques anticoncurrentielles telles que la collusion en matière de prix ou des pratiques d'exclusion ou de discrimination. En

outre, les fusions et acquisitions motivées par l'IA peuvent susciter des préoccupations au sujet de positions dominantes sur les marchés et d'obstacles à l'entrée, à mesure que les algorithmes et les données deviennent des actifs indispensables pour disposer d'un avantage concurrentiel. Les cadres antitrust traditionnels pourraient peiner à s'adapter au caractère dynamique des marchés portés par l'IA, obligeant les autorités chargées de la concurrence à mettre au point de nouveaux outils d'analyse, de nouveaux mécanismes d'accès aux données et de nouveaux cadres réglementaires pour protéger efficacement la concurrence et le bien-être des consommateurs à l'ère de l'IA (voir l'article d'opinion de Shin-yi Peng).

Les fusions sur le marché de l'IA sont de plus en plus étroitement surveillées et il y a une volonté croissante de mieux comprendre les conséquences de l'IA pour la concurrence.[8] Les politiques antitrust traditionnelles, qui s'appliquent après coup, lorsque la concurrence sur le marché a déjà été affectée, sont lentes et axées sur les prix et ne suffisent pas à traiter les questions de concurrence soulevées par l'IA. Les enjeux de concurrence liés à l'IA ont conduit à renouveler les appels en faveur d'une approche internationale collective de la réglementation et du respect des règles relatives à la concurrence sur les marchés numériques.

Article d'opinion

L'IA amplifie les questions relatives au commerce numérique

Shin-yi Peng

Professeur de droit émérite,
Université nationale Tsing Hua

Bon nombre des défis posés par les technologies numériques que l'OMC a rencontrés au cours des dernières décennies sont maintenant amplifiés par l'IA, y compris des questions liées à la classification, à la non-discrimination, à la gouvernance des données et à la politique de la concurrence.

Tout d'abord, l'IA joue le rôle de facilitatrice pour des produits complexes qui regroupent des marchandises et des services, ce qui exige de réfléchir plus avant à la manière d'ajuster les cloisonnements juridiques entre marchandises et services dans le cadre de l'OMC pour traiter les questions découlant de la fusion des sphères physique et numérique. Il semble probable que la dichotomie marchandises/services dans l'application des règles commerciales donnera de plus en plus lieu à des niveaux d'incohérence et d'incertitude juridique inédits.

Deuxièmement, de plus en plus de services fondés sur l'IA seront en mesure de faire directement concurrence à des professionnels humains ou de les remplacer. Des questions telles que la mesure dans laquelle les outils de conseil juridique automatisés et les avocats humains devraient être considérés comme des « fournisseurs de services similaires » pourraient se poser plus tôt que prévu. Il reste à voir dans quelle mesure des notions telles que la « neutralité technologique » ou l'« interprétation évolutive » peuvent servir à clarifier la portée des engagements en matière d'accès aux marchés et de traitement national pris au titre de l'AGCS.

Troisièmement, l'IA présente de nouveaux défis pour la gouvernance des données. Les algorithmes publicitaires des plates-formes numériques ou, plus généralement, leurs modèles économiques en général, intensifient les périls associés à l'économie fondée sur les données. Les règles de l'OMC peuvent jouer un rôle plus actif dans la réduction de ces périls. La gouvernance des données à l'ère de l'IA nécessite des conceptions qui préservent les valeurs sociales, dont la protection de la vie privée, la sécurité, la liberté d'expression, l'expression culturelle et l'éthique algorithmique.

Enfin, les autorités chargées de la concurrence dans le monde entier adoptent ou envisagent de plus en plus des approches qui imposent des obligations additionnelles aux grandes entreprises technologiques reposant sur l'IA. Les abus de position dominante auxquelles celles-ci peuvent se livrer, y compris les pratiques d'autofavoritisme qui mettent en avant leurs propres services parmi les résultats de recherche, les cartels algorithmiques et d'autres arrangements collusoires transfrontières, peuvent être traités de manière plus significative par le biais de disciplines relatives à la concurrence au niveau international. Dans quelle mesure la pratique algorithmique constitue-t-elle un obstacle au commerce pour les marchandises ou les services et comment les concentrations anticoncurrentielles sur les marchés excluent-elles les fournisseurs étrangers d'un marché ? Il est plus urgent que jamais de réactiver le Groupe de travail de l'OMC sur le commerce et la politique de la concurrence. Si un ensemble de disciplines générales ou sectorielles relatives à la concurrence pouvait être établi à l'OMC, il serait moins nécessaire que les autorités chargées de la concurrence des pays en développement et des PMA fassent respecter le droit de la concurrence après coup.

Avertissement
Les articles d'opinion relèvent de la seule responsabilité de leurs auteurs. Ils ne reflètent pas nécessairement les opinions ou les vues des Membres ou du Secrétariat de l'OMC.

ii) Empêcher la création de nouveaux obstacles au commerce numérique

Les flux de données transfrontières sont essentiels à l'IA. Comme nous l'avons vu dans la section 2 a) i), il est essentiel de réunir de vastes ensembles de données pour entraîner les algorithmes, et les flux de données font partie intégrante de l'utilisation en temps réel des technologies de l'IA. L'étendue et la diversité des données sont aussi importantes que le volume.[9] Pour que l'IA soit efficace et fournisse des prédictions exactes qui ne soient pas susceptibles de partialité et de discrimination, les algorithmes doivent être fondés sur des données exactes, représentatives et de grande qualité.

Les restrictions aux flux de données transfrontières peuvent avoir une incidence négative sur le développement de l'IA et l'innovation en la matière et risquent de faire augmenter les coûts pour les entreprises. Ces restrictions ont, d'une manière générale, une incidence négative sur la productivité, la croissance économique et l'innovation aux niveaux national et mondial (Aaronson, 2019 ; Goldfarb et Tucker, 2012 ; Luintel et Khan, 2009 ; Maskus et Reichman, 2004 ; OCDE, 2016), mais elles sont particulièrement préoccupantes pour le développement de l'IA et l'innovation dans ce domaine. Comme l'IA nécessite de vastes quantités de données de bonne qualité pour être entraînée, ce qui suppose souvent de combiner différentes sources de données, les restrictions aux flux de données transfrontières sont susceptibles d'influer de manière significative sur la qualité et l'exactitude des modèles d'IA et sur la possibilité de déployer les applications de l'IA à plus grande échelle. En limitant la capacité des entreprises étrangères d'accéder aux données provenant d'une juridiction donnée, ces mesures pourraient favoriser les entreprises nationales, mais risquent de le faire aux dépens de la qualité globale, compromettant ainsi l'innovation et la réalisation du plein potentiel de l'IA (Goldfarb et Trefler, 2018).[10] Les restrictions à la circulation transfrontières de données imposent aussi des coûts supplémentaires aux entreprises souhaitant mener des activités au niveau international. Selon une récente étude relative aux répercussions des restrictions aux flux de données sur le PIB et le commerce au niveau mondial, si toutes les économies restreignaient pleinement leurs flux de données, cela pourrait entraîner une réduction de 5 % du PIB mondial et une baisse de 10 % des exportations (OCDE et OMC, 2024). Pour se conformer aux restrictions aux flux de données, les entreprises pourraient devoir établir une présence et dupliquer leurs activités dans différentes juridictions, et concevoir un système pour faire en sorte que les données ne soient pas acheminées au niveau international. Bien que techniquement réalisable, cela peut être particulièrement coûteux, en particulier pour les petites entreprises (Goldfarb et Trefler, 2018).

Toutefois, les vastes ensembles de données requis par les modèles d'IA soulèvent d'importantes préoccupations en matière de protection de la vie privée. L'IA donne lieu à de nouvelles questions de confidentialité pour les particuliers et les consommateurs, conduisant à un arbitrage entre la nécessité d'accéder à de grandes quantités de données pour entraîner les modèles d'IA et la protection de la vie privée. Le suivi et le profilage continus des interactions en ligne et hors ligne des personnes par des algorithmes d'IA suscitent d'importantes préoccupations au sujet de la confidentialité des données, du consentement et de la maîtrise des informations personnelles. En outre, les algorithmes d'IA devenant de plus en plus sophistiqués dans leur capacité d'inférer des informations et de prédire les comportements sur la base des données des utilisateurs, il est urgent de disposer de réglementations solides en matière de protection de la vie privée, de pratiques transparentes en matière de données et de mécanismes de contrôle utilisateur renforcés pour sauvegarder le droit au respect de la vie privée des personnes et assurer un déploiement éthique et responsable de l'IA.[11] L'IA suscite également de nouvelles préoccupations en matière de confidentialité pour les consommateurs (voir l'encadré 3.1), et l'utilisation de données comme intrants dans les modèles d'IA soulève aussi des préoccupations en matière de propriété intellectuelle (voir la section 3 a) iv)). En conséquence, il y a un équilibre délicat à trouver entre les préoccupations liées à la protection de la vie privée et la nécessité d'accéder à de grandes quantités de données pour entraîner les modèles d'IA (voir aussi l'article d'opinion de Shin-yi Peng).

Les restrictions aux flux de données transfrontières ont aussi une incidence négative sur le commerce des produits reposant sur l'IA. Bien qu'il existe des données empiriques indiquant que l'IA renforce nettement le commerce international des services numériques, la réglementation des flux de données transfrontières peut entraver ce commerce. Sun et Trefler (2023) constatent que les restrictions concernant les flux de données peuvent réduire l'intérêt que présentent les applications reposant sur l'IA, les rendant moins attrayantes pour les utilisateurs internationaux. Alors que l'IA entraîne un décuplement du nombre d'utilisateurs étrangers, son incidence sur ces utilisateurs est réduite de moitié si ceux-ci se trouvent dans une économie imposant de fortes restrictions sur les flux de données transfrontières. Ainsi, les économies qui appliquent une réglementation stricte en matière de données risquent de se priver de débouchés commerciaux offerts par l'IA. Il est donc essentiel de trouver le juste équilibre entre la protection de la vie privée et la promotion de l'innovation afin de maximiser les avantages de l'IA pour le commerce international. Cela étant, les mesures concernant les flux de données transfrontières, lorsqu'elles visent à protéger la vie privée, peuvent contribuer à renforcer la confiance dans les systèmes d'IA et à favoriser leur utilisation plus large. Il ressort d'une étude de l'OCDE et de l'OMC (2024) sur les implications des restrictions en matière de flux de données que, même si la suppression des réglementations relatives aux flux de données dans toutes les économies réduirait les coûts du commerce, elle affaiblirait également la confiance, ce qui rendrait les consommateurs moins disposés à payer pour des produits et aurait un effet négatif sur le PIB.

Encadré 3.1 : L'IA et la protection des consommateurs

L'IA ouvre d'importantes possibilités aux consommateurs, mais elle accroît aussi les possibilités d'influence occulte, ce qui suscite d'importantes préoccupations concernant l'exploitation des informations personnelles ainsi que la violation de la vie privée, la manipulation et la désinformation.

L'IA peut apporter des avantages majeurs aux consommateurs, tels que des recommandations individualisées et des économies de temps (par exemple, les assistants vocaux à intelligence artificielle peuvent commander des articles d'épicerie instantanément, évitant aux consommateurs des heures d'achats). La capacité des modèles d'IA d'établir des corrélations entre les données des consommateurs et leurs réponses possibles aux annonces publicitaires afin de prédire le comportement des consommateurs offre aux entreprises qui utilisent l'IA la capacité sans précédent de déclencher des réactions précises au moyen de publicités et de communications individualisées. Toutefois, cela peut aussi exacerber l'asymétrie de l'information entre les entreprises et les consommateurs et peut conduire à la manipulation et à l'exploitation du comportement de ces derniers.

L'utilisation d'algorithmes pour fixer les prix peut conduire à des gains d'efficacité en matière de prix qui sont répercutés sur les clients, mais les algorithmes peuvent aussi être utilisés pour exploiter la disposition des consommateurs à payer un certain prix dans l'intérêt de l'entreprise.

En outre, si les technologies de l'IA peuvent contribuer à une modération effective dans l'intérêt des consommateurs, elles peuvent aussi fournir des réponses inexactes, partiales ou discriminatoires qui peuvent porter préjudice aux consommateurs.

Enfin, les vendeurs peuvent ne pas tenir pleinement compte des préjudices qui peuvent être causés aux consommateurs du fait de l'utilisation abusive de leurs données en raison de la difficulté de déterminer qui a initialement collecté les données et est à l'origine des préjudices. Les consommateurs ne peuvent donc pas contester l'utilisation des données après que celles-ci ont été collectées (Agrawal *et al.*, 2019).

Bien que les lois traditionnelles sur la protection des consommateurs puissent s'appliquer à la plupart des cas d'utilisation de l'IA et prévoient souvent des recours juridiques adéquats sans qu'il soit nécessaire d'adopter de nouvelles réglementations, des mesures destinées à réglementer les préjudices algorithmiques et à protéger les consommateurs ont été adoptées ces dernières années dans différentes juridictions. Dans le cadre du Règlement général de l'UE sur la protection des données, par exemple, les personnes ont le droit de contester les décisions prises par des algorithmes, de demander un contrôle humain et de se retirer de la publicité personnalisée reposant sur des méthodes algorithmiques. La Chine s'est également dotée d'une réglementation complète régissant l'utilisation d'algorithmes. D'autres législations visant à encadrer les algorithmes et à protéger les consommateurs sont examinées dans différentes juridictions, dont l'Union européenne[12] et le Royaume-Uni (Holmes, 2024).

Toutefois, les approches nationales ne protègent pas de manière adéquate les consommateurs dans le cas des transactions transfrontières (Jones, 2023). Obtenir réparation en cas de préjudice reste particulièrement difficile dans le cas de transactions internationales. Bien qu'une collaboration et des discussions en matière de réglementation aient lieu dans une certaine mesure au niveau international entre organismes nationaux, cette coopération reste fragmentée et n'établit pas de cadre efficace et transparent pour faire respecter les droits des consommateurs de part et d'autre des frontières (Goyens, 2020), ce qui amène certains experts à appeler à de nouvelles formes de réglementation et de coopération internationales pour la protection des consommateurs, en particulier contre les préjudices causés par l'IA (Jones, 2023).

Outre les atteintes potentielles à la vie privée et à l'intégrité personnelle, la désinformation et la manipulation, la difficulté d'évaluer la sécurité et la sûreté des produits et services fondés sur l'IA rendent encore plus complexe la protection des consommateurs à l'ère de l'IA (voir le chapitre 3 a) iii)).

iii) Faire en sorte que l'IA soit digne de confiance sans entraver le commerce

Les normes et les règlements techniques jouent un rôle clé pour faire en sorte que l'IA soit digne de confiance et, ainsi, promouvoir le commerce des produits reposant sur l'IA. Il existe un consensus de plus en plus large au sujet du rôle central que les règlements, les normes et les autres interventions des pouvoirs publics peuvent jouer pour faire en sorte que l'IA soit digne de confiance, c'est-à-dire qu'elle réponde aux attentes en ce qui concerne des critères tels que la fiabilité, la sécurité, la protection de la vie privée, la sûreté, la redevabilité et la qualité d'une manière vérifiable.[13] En fin de compte, cela implique de trouver un équilibre en matière de réglementation pour mettre à profit les avantages de l'IA tout en atténuant les risques qu'elle présente. Faire en sorte que l'IA soit digne de confiance n'est pas seulement important pour ce qui se passe au sein des économies. Cela revêt aussi un intérêt pour ce qui se passe en dehors des économies et de part et d'autres des frontières. En effet, la réglementation intérieure que les gouvernements adoptent pour protéger leurs consommateurs peut aider à renforcer la confiance des consommateurs, des importateurs et des autres parties prenantes dans les produits reposant sur l'IA, favorisant ainsi le commerce de ces produits.

Il peut être particulièrement difficile de trouver un équilibre entre la réglementation de l'IA pour des raisons légitimes de politique générale et le fait de favoriser autant que possible la bonne marche des échanges commerciaux. Bien que la difficulté de trouver le juste équilibre entre la réglementation et le libre-échange ne soit pas nouvelle, la nature évolutive, opaque et multidimensionnelle de l'IA, ainsi que les nouveaux types de risques qui y sont associés, rendent particulièrement complexe cet exercice d'équilibriste concernant la réglementation et la gouvernance de l'IA (voir aussi l'article d'opinion d'Eduardo Paranhos).

Pour réglementer l'IA, il faut réglementer le « comportement » d'un produit. Comme il est indiqué au chapitre 2, l'« autonomie » est l'une des caractéristiques uniques de l'IA. Étant donné que les systèmes d'IA peuvent conférer aux produits divers degrés d'« autonomie », ces produits peuvent engendrer de nouvelles formes de risques découlant non pas de problèmes liés à leurs composants physiques, mais plutôt de la manière dont l'IA peut les faire se « comporter ».[14] Ces risques ne sont pas faciles à prévoir, à contrôler ni même à quantifier.[15] Comme l'indiquent Judge *et al.* (2024), l'une des caractéristiques techniques uniques qui définissent l'IA est que, contrairement à tous les autres systèmes conçus par l'homme, son « comportement » n'est pas dicté ou prédéterminé par le code de son programme ; il s'agit d'une propriété « émergente ». Par conséquent, les produits reposant sur l'IA peuvent générer des risques pour des raisons autres que celles qui sont inhérentes aux éléments matériels des produits eux-mêmes. Par exemple, certains considèrent que le « comportement » des cobots (c'est-à-dire des robots collaboratifs ou de compagnie) utilisant l'IA, s'il n'est pas surveillé, pourrait provoquer des problèmes de santé mentale chez les personnes qu'ils accompagnent.[16]

L'opacité du caractère « comportemental » de l'IA peut rendre la réglementation encore plus difficile. Les « comportements » risqués des produits reposant sur l'IA peuvent être liés à la façon dont leurs algorithmes sont conçus. Les algorithmes d'IA sont notoirement opaques (Lim, 2021 ; Lund *et al.*, 2023). Comme il est indiqué au chapitre 2, la transparence et l'explicabilité sont essentielles pour comprendre comment et pourquoi les systèmes d'IA fonctionnent et se comportent comme ils le font.[17] Ce problème est communément appelé problème de la « boîte noire » de l'IA, qui a été décrit comme présentant deux dimensions, juridique et technique. Pour traiter la dimension juridique, il faut accéder au code source. Cela peut se révéler difficile car les codes sources sont normalement exclusifs, c'est-à-dire protégés en tant que propriété intellectuelle, normalement sous la forme de secrets commerciaux. Il existe toutefois des moyens réglementaires de gérer cette difficulté, par exemple en autorisant la divulgation forcée du code source à des fins de réglementation ou d'application des lois,[18] même si, dans la pratique, cela peut ne pas être facile ni justifié.[19] Pour certains, la dimension technique du problème de la boîte noire peut être encore plus importante car l'opacité d'un système d'IA peut persister même lorsque l'accès au code source est libre ou a été accordé de manière volontaire ou forcée. En effet, il peut y avoir des cas où les applications de l'IA sont si complexes que même les programmeurs eux-mêmes sont incapables d'expliquer pourquoi et comment un système d'IA est parvenu à certaines décisions ou à certains classements d'après le code source et d'autres renseignements et données exclusifs. Pour certains, cela signifie que, tant que cette difficulté technique n'aura pas été résolue de manière satisfaisante, les solutions réglementaires fondées sur la libre divulgation du code source risquent de se heurter à d'« importants obstacles » (Lin, 2021 ; Mitchell *et al.*, 2023 ; Pasquale, 2015).

Le fait que la nature évolutive des produits reposant sur l'IA peut aussi être déclenchée par des facteurs externes rend d'autant plus difficile de localiser la source de vulnérabilité de ces produits. Parmi ces facteurs figurent la personnalisation : la capacité de millions de personnes de « personnaliser » leurs produits reposant sur l'IA d'un nombre presque infini de manières pose un problème aux organismes de réglementation pour ce qui est d'anticiper les risques potentiels associés à chaque produit personnalisé unique. Un autre facteur est la connectivité, qui peut rendre les produits vulnérables à des cyberattaques ou cybermenaces de la part d'acteurs malveillants qui peuvent se trouver n'importe où dans le monde. Ces facteurs rendent encore plus difficile pour les organismes de réglementation d'anticiper et de gérer le large éventail de risques imprévisibles et involontaires susceptibles de survenir tout au long du cycle de vie de ces produits (Lund *et al.*, 2023).

Le double usage qui peut être fait de l'IA peut ajouter un degré de complexité supplémentaire. Comme il est

Article d'opinion

Considérations relatives à la réglementation de l'IA : équilibre entre innovation, risques et défragmentation réglementaire

Eduardo Paranhos

Juriste, LL.M – Université de Londres (LSE) ; bénéficiaire du programme Chevening ; Chef du Groupe de travail de l'IA au sein de l'Association brésilienne de fabricants de logiciels (ABES)

Il n'est pas simple de déterminer quand un nouveau phénomène social ou économique justifie une réglementation. Ces difficultés peuvent être encore amplifiées lorsque les nouveaux scénarios prennent la forme de technologies innovantes, créant à la fois des risques et des possibilités. Pour y remédier, quelle que soit la nature des changements, il est important de réfléchir à quelques questions fondamentales : i) quels sont les risques et les possibilités en jeu ; ii) à quel point ces nouvelles technologies sont-elles bien comprises, de sorte que les outils nécessaires pour faire face aux risques éventuels puissent être correctement équilibrés ; et iii) quels aspects des progrès technologiques nécessitent effectivement de nouvelles règles vis-à-vis des lois existantes ?

L'IA transforme la façon dont nous travaillons, communiquons et créons des contenus plus rapidement que jamais auparavant. La promotion du développement et de la mise en œuvre de solutions d'IA peut accroître l'efficacité et la qualité des emplois, comme il a été noté, par exemple, dans de récentes études de l'Organisation internationale du travail et de la société de conseil McKinsey. Pourtant, pour que ces avantages se concrétisent, nous devrions examiner quels aspects des systèmes d'IA devraient vraiment être réglementés et nous employer à établir un modèle qui, dans le même temps, soit capable de protéger la société et d'encourager – au lieu de décourager – la recherche-développement.

Il est trop simplifié de dire que, pour réglementer l'IA, les économies envisagent pour l'essentiel soit des formats fondés sur le contexte, soit des modèles prescriptifs prévoyant un ensemble plus détaillé d'obligations et de sanctions.

Au Brésil, les débats relatifs à la réglementation de l'IA ont jusqu'à présent porté sur des aspects de chacune de ces structures possibles : un modèle prescriptif, ouvertement inspiré du régime européen, et une proposition de cadre fondé sur le contexte et reposant sur des principes largement reconnus en matière de gouvernance et d'atténuation des risques – par exemple ceux de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) et de l'Organisation de coopération et de développement économiques (OCDE) – réaffirmant le rôle de la législation existante.

De fait, il est possible que la plupart des situations qui suscitent des préoccupations au sujet du déploiement de l'IA puissent être traitées au moyen des lois fédérales existantes, en particulier en ce qui concerne la protection de la vie privée, la sécurité des produits, la protection des consommateurs et la réglementation relative à Internet, ainsi que certains règlements en aval, comme l'ordonnance de l'autorité sanitaire du Brésil sur les logiciels en tant que dispositif médical.[20] Par exemple, une violation de données résultant de l'utilisation d'un système d'IA fait l'objet des mêmes contrôles et mesures correctives que ceux qui sont prévus dans la loi brésilienne sur la protection de la vie privée pour d'autres infractions qui se produisent sans l'utilisation de l'IA. La loi sur la protection de la vie privée couvre également l'utilisation abusive potentielle de données personnelles sensibles qui génère des résultats biaisés de la même manière qu'un usage abusif similaire dans des contextes hors ligne.

Toutefois, il est primordial de cartographier clairement les lacunes de la législation actuelle, de sorte qu'une nouvelle réglementation sur l'IA puisse y remédier, en évitant les chevauchements et l'incertitude juridique qui en résulte. Un autre point essentiel qui pourrait faire que les modèles prescriptifs posent problème est le fait de réglementer principalement le « développement » de l'IA, au lieu de se concentrer sur les « utilisations » à haut risque de la technologie.

Une dernière considération a trait au degré de préparation dont la réglementation à venir devrait faire preuve pour pouvoir évoluer avec la technologie. Il semble plus réaliste que les réglementations fondées sur le contexte évoluent progressivement pour devenir plus strictes « si » et « quand » cela sera nécessaire, plutôt que l'inverse. De même, dans le contexte des préoccupations liées au commerce concernant les effets défavorables de la fragmentation réglementaire, la réglementation de l'IA qui se concentre sur les utilisations à haut risque – et non sur le développement de la technologie – pourrait faciliter la poursuite d'une approche plus harmonisée entre les marchés. Notamment, certaines économies qui sont des protagonistes mondiaux des investissements dans l'IA et de sa mise en œuvre[21] privilégient des formes de réglementation évolutives, équilibrant la gouvernance de l'IA avec des objectifs d'atténuation des risques, tout en contribuant à relever les niveaux de vie en créant des emplois de qualité et en améliorant les conditions de vie des populations grâce à l'innovation responsable.

Avertissement

Les articles d'opinion relèvent de la seule responsabilité de leurs auteurs. Ils ne reflètent pas nécessairement les opinions ou les vues des Membres ou du Secrétariat de l'OMC.

indiqué au chapitre 2 a), la dualité d'usage de l'IA fait que celle-ci peut être employée à la fois à des fins civiles et militaires. Cela peut ajouter une dimension de sécurité nationale et de géopolitique à la gouvernance de l'IA, rendant les interventions et la coopération en matière de réglementation d'autant plus complexes (Csernatoni, 2024 ; Klein et Stewart, 2024 ; Pouget, 2023 ; Raul et Mushka, 2024). Une question connexe concerne la politique et la réglementation dans le domaine de l'IA et de la cybersécurité (voir l'encadré 3.2).

En ce qui concerne les marchandises, les règlements et normes « traditionnels » qui sont normalement axés sur des prescriptions concernant des aspects matériels, visibles et statiques des produits peuvent ne pas être en mesure de traiter les risques découlant de l'intégration de l'IA dans les produits « traditionnels ». En ce qui concerne les marchandises, les règlements et normes « traditionnels » qui sont normalement axés sur des prescriptions concernant des aspects matériels, visibles et statiques des produits peuvent ne pas être en mesure de traiter les risques découlant de l'intégration de l'IA dans les produits « traditionnels ». La nature changeante des produits reposant sur l'IA, résultant du caractère évolutif de celle-ci, fait de la réglementation une éternelle cible mouvante. Les systèmes d'IA confèrent de nouvelles propriétés et fonctions aux produits dans lesquels ils sont incorporés. Comme il a été souligné au chapitre 2, ces propriétés et fonctions des produits peuvent être décrites comme « dynamiques », c'est-à-dire qu'elles changent au fil du temps comme conséquence de changements constants qui ont lieu tout au long du cycle de vie du système d'IA du fait de mises à jour logicielles ou d'autres auto-améliorations résultant du processus d'« apprentissage » algorithmique. Cela contraste avec les propriétés « statiques » des produits plus traditionnels, qui, normalement, restent essentiellement les mêmes tout au long de leur cycle de vie. Bon nombre des changements constants des propriétés et des fonctions des produits reposant sur l'IA sont censés être des améliorations bénéfiques (certains appellent même cela « évolution »).[22] Toutefois, ce processus dynamique signifie que les risques et préoccupations connus pourraient aussi être en constante évolution, ou qu'il pourrait être en train d'en apparaître de nouveaux. Pour les produits

Encadré 3.2 : IA, cybersécurité et obstacles techniques au commerce (OTC)

La capacité de l'IA d'analyser de grands ensembles de données peut aider à lutter contre les cybermenaces et à répondre aux cyberattaques malveillantes. Toutefois, le risque d'une prise de décisions partiale et d'utilisation malveillante ou abusive, ainsi que le manque de transparence et d'explicabilité des systèmes d'IA, donne lieu à des préoccupations. Des acteurs malveillants peuvent utiliser l'IA pour créer de nouveaux logiciels malveillants, concevoir de nouvelles attaques d'hameçonnage sophistiquées ou ciblées, identifier de nouveaux canaux d'attaque et créer des hypertrucages (« deep fakes »). Sans surprise, la cybersécurité est une préoccupation centrale exprimée non seulement dans les politiques nationales relatives à l'IA, mais aussi dans les principes et les discussions sur la gouvernance concernant l'IA au niveau international.

Les risques de vulnérabilité en matière de cybersécurité augmentent à mesure que les technologies numériques se diffusent au sein de plus en plus de sociétés et d'économies. En réponse, les gouvernements adoptent de plus en plus de mesures et de politiques liées à la cybersécurité, dont beaucoup revêtent la forme de mesures OTC, c'est-à-dire de règlements techniques, de normes et de procédures d'évaluation de la conformité.

De fait, les mesures OTC liées à la cybersécurité sont récemment devenues l'une des questions relatives aux technologies numériques les plus importantes examinées au Comité OTC de l'OMC. À ce jour, plus de 90 mesures OTC liées à la cybersécurité ont été notifiées au Comité, dont environ 65% au cours des 3 dernières années et demie. Au Comité OTC, les Membres ont en outre soulevé de plus en plus de préoccupations commerciales spécifiques (PCS) contre des mesures OTC liées à la cybersécurité : sur les 29 PCS soulevées depuis 1995, 38% l'ont été au cours des trois dernières années et demie seulement.

La cybersécurité a pour la première fois fait l'objet d'une séance thématique spécifique du Comité OTC, organisée en 2023. Compte tenu du caractère mondial du problème, à cette séance, il a été fait valoir que les interventions unilatérales des pouvoirs publics dans ce domaine devraient être évitées, car elles pourraient en fin de compte compromettre les efforts mondiaux en matière de cybersécurité. La nécessité pour les gouvernements et le secteur privé de travailler de manière plus coordonnée et collaborative pour remédier à la fragmentation et aux divergences croissantes de la réglementation dans ce domaine et trouver de meilleurs moyens de lutter contre la cybercriminalité et les cyberincidents, qui sont en hausse, a également été soulignée. Les efforts visant à élaborer des normes internationales ambitieuses, équitables et inclusives en matière de cybersécurité ont été mis en lumière.

reposant sur l'IA, comme c'est le cas pour la plupart des autres produits, des spécifications et des prescriptions continueront d'être nécessaires pour faire face aux risques liés à leurs aspects « physiques » (par exemple les dangers liés aux composants mécaniques défectueux d'un véhicule autonome). Toutefois, pour certains, ces spécifications et prescriptions « traditionnelles » peuvent être mal adaptées ou insuffisantes pour faire face aux situations dans lesquelles la cause profonde d'un risque n'est pas une défaillance mécanique ou « physique », mais un défaut de conception algorithmique ou un autre problème dans le système d'IA incorporé dans le produit qui peut l'amener à avoir un « comportement » risqué (par exemple un véhicule autonome qui blesse des personnes ou cause des dégâts matériels).

Les produits reposant sur l'IA peuvent présenter des risques non seulement matériels mais aussi immatériels. Un produit reposant sur l'IA peut présenter à la fois des risques matériels, qui sont faciles à quantifier et à mesurer (par exemple des dommages corporels ou des dégâts matériels) et des risques immatériels (par exemple des atteintes à la vie privée ou à d'autres droits fondamentaux), qui sont plus difficiles à quantifier et à mesurer. Les risques matériels et immatériels peuvent parfois même découler de la même situation. Par exemple, des dysfonctionnements mécaniques et/ou des défauts algorithmiques dans les caméras internes et externes d'un véhicule autonome utilisant l'IA peuvent à la fois causer des dommages corporels (préjudices matériels) et affecter la vie privée des passagers ou de piétons (préjudices immatériels).[23] De même, les spécifications de produits énoncées dans des règlements et normes identiques pour tous les cas peuvent être mal adaptées pour réglementer les produits reposant sur l'IA qui intègrent différentes solutions personnalisées (Lund *et al.*, 2023). Pour faire face à ces problèmes de réglementation, tout en soutenant le déploiement et le commerce de produits reposant sur l'IA dignes de confiance, il a été proposé que les organismes de réglementation réfléchissent à des moyens créatifs de faire en sorte que les prescriptions et spécifications relatives aux produits soient dynamiques et adaptables à la nature comportementale et évolutive de ces technologies, de sorte qu'elles ne deviennent pas obsolètes à mesure que les caractéristiques, les risques et les vulnérabilités de l'IA évoluent tout au long du cycle de vie des produits.[24]

L'évolution constante des produits reposant sur l'IA peut par ailleurs nécessiter de nouvelles approches pour certifier leur conformité avec les prescriptions réglementaires. En effet, si un produit reposant sur l'IA a été soumis avec succès à des procédures d'essai, de vérification ou d'autres procédures de certification avant d'être mis sur le marché, cela ne signifie pas nécessairement qu'il restera certifiable tout au long de son cycle de vie. Les produits reposant sur l'IA, en particulier les produits de l'IdO ou de la robotique connectés à Internet, peuvent générer de nouveaux risques après leur déploiement en raison de facteurs de « mutabilité » tels que de nouvelles mises à jour, de nouvelles données, des modifications imprévues des attributs et fonctions dues à la personnalisation opérée par les utilisateurs, ou des comportements autonomes imprévus (voir l'encadré 3.2).[25] Comme nous l'avons déjà vu, l'évaluation de la conformité de certains produits reposant sur l'IA avec des règlements techniques et des normes sous-jacents peut aussi nécessiter l'accès au code source, ce qui soulève des questions liées à la propriété intellectuelle (voir le chapitre 3 a) iv)). Les organismes de réglementation pourraient aussi faire face à des difficultés pour ce qui est d'évaluer la conformité des produits reposant sur l'IA avec diverses prescriptions réglementaires nouvelles qui visent, par exemple, à évaluer la qualité des données utilisées dans ces produits. Compte tenu de ces multiples difficultés, certains considèrent que les organismes de réglementation devront peut-être réévaluer leurs approches en matière d'évaluation de la conformité et élaborer des méthodes permettant de veiller à ce que les produits de l'IA en constante évolution restent effectivement conformes aux règlements techniques et aux normes sous-jacents (Lund *et al.*, 2023 ; Meltzer, 2023).[26]

L'intégration de l'IA dans les marchandises et les services a en outre élargi la portée, le nombre et la nature des risques et des préoccupations que les règlements et les normes doivent traiter. Comme indiqué plus haut, outre les préoccupations réglementaires « traditionnelles » telles que l'interopérabilité, la sécurité, la sûreté, la qualité et la protection de la santé et de la vie des personnes, l'utilisation et le déploiement de l'IA peuvent créer divers risques « non typiques », que certains qualifient même d'« existentiels » (UNDRR, 2023) et qui peuvent soulever des questions éthiques et sociétales complexes touchant à la moralité publique et à la dignité humaine.[27] Si l'IA est entraînée sur des ensembles de données biaisés et faussés, elle risque de perpétuer ou d'exacerber les biais ou la discrimination à l'égard de groupes minoritaires et de porter atteinte aux droits et libertés individuels (voir le chapitre 2). Les marchandises et les services reposant sur l'IA sont également une source de préoccupation importante en ce qui concerne la confidentialité des données, car ils impliquent la collecte, le traitement et le stockage de grandes quantités de données des utilisateurs (voir le chapitre 3 a)). En outre, comme il est indiqué plus haut, l'IA est une technologie susceptible de double usage, ce qui peut soulever des questions complexes touchant à la géopolitique et à la sécurité nationale et conduire à une fragmentation accrue de la réglementation. Enfin, tant les données d'« entrée » que de « sortie » de l'IA soulèvent des questions nouvelles et complexes concernant la propriété intellectuelle et sa protection (voir le chapitre 3 a) iv)).

Ces préoccupations font qu'il est difficile de concevoir des solutions réglementaires appropriées pour veiller à ce que l'IA et les produits reposant sur l'IA soient dignes de confiance et soutenir leur commerce. Comme nous l'avons déjà mentionné, l'IA soulève des préoccupations sociétales et éthiques (risques « immatériels ») qui, contrairement aux préoccupations « traditionnelles » telles que la santé et la sécurité (risques « matériels »), ne font généralement pas l'objet de règlements techniques ni de normes. Ces préoccupations « non techniques » sont plus difficiles à réglementer, à surveiller et à faire respecter que des objectifs réglementaires plus traditionnels, tels que la sécurité des produits ou la protection de la santé ou de la

vie des personnes, qui peuvent être traités de manière plus « technique » et objective. Il a été fait valoir que les cadres de gouvernance et de réglementation de l'IA pouvaient exiger des règles, des règlements et des normes qu'il convient peut-être mieux de décrire comme des instruments non pas purement « techniques », mais plutôt « sociotechniques », c'est-à-dire combinant des questions techniques avec des considérations sociétales plus larges (Dentons *et al.*, 2023 ; Kerry, 2024 ; Meltzer, 2023). Pouget (2023) fait valoir qu'il est difficile d'élaborer des règlements sociotechniques dans les situations où la technologie et les dommages qu'elle peut causer sont « si complexes qu'il devient difficile de faire la part des jugements de valeur et des détails techniques ». Certains se sont même demandé si cela pourrait un jour être fait dans la pratique.[28]

Ces risques et préoccupations non typiques ou immatériels engendrés par l'IA peuvent aussi être intrinsèquement sujets à une fragmentation réglementaire, ce qui pourrait entraver les échanges. En effet, il pourrait être difficile pour les législateurs de convenir de dénominateurs internationaux communs en ce qui concerne certaines valeurs et préoccupations sociétales liées à l'IA telles que l'éthique, la vie privée ou les droits de l'homme, dont l'importance relative peut varier d'une économie à une autre.[29] Une fragmentation réglementaire non nécessaire ou évitable pourrait à son tour entraver les possibilités et les avantages associés à l'IA (Bello Villarino, 2023 ; OCDE, 2022a). En particulier, elle pourrait entraîner de lourdes charges et des coûts élevés liés au respect de la réglementation et, par conséquent, créer des obstacles non tarifaires au commerce pour les entreprises du domaine de l'IA.

iv) Comment l'IA est façonnée par la propriété intellectuelle et pourrait la transformer

L'IA présente de nouveaux défis conceptuels concernant l'approche traditionnelle, centrée sur l'humain, des droits de propriété intellectuelle. Des droits de propriété intellectuelle équilibrés et les moyens de les faire respecter ont un rôle important à jouer pour assurer à la fois un accès équitable à la technologie de l'IA et une juste répartition des gains économiques résultant de son utilisation. L'IA soulève plusieurs questions importantes à cet égard.

Une première question concerne la forme de protection de la propriété intellectuelle qui est accordée aux algorithmes d'IA. Si la protection de la propriété intellectuelle est fondée sur le fait que ces algorithmes sont des secrets commerciaux – et que le secret est donc une condition essentielle sur laquelle établir la protection de la propriété intellectuelle –, cela soulève des questions concernant un manque de transparence. Des algorithmes nouveaux et inventifs peuvent également être protégés par des brevets dans certaines juridictions, le mécanisme de divulgation obligatoire du système des brevets donnant des renseignements détaillés sur les technologies de l'IA, qui tombent directement dans le domaine public dans de nombreuses économies (OMPI, 2024). Toutefois, la protection conférée par des brevets peut limiter le développement d'algorithmes dans les économies où des brevets ont été délivrés. Le droit d'auteur, un autre type de protection de la propriété intellectuelle, peut être automatiquement accordé à la fois pour le code source et le code objet, ce qui peut limiter l'analyse et l'utilisation des algorithmes. Comme le prévoient les objectifs du système international de propriété intellectuelle, il faut des exceptions et limitations appropriées à la protection des droits de propriété intellectuelle pour équilibrer les différents intérêts et assurer un accès approprié aux technologies de l'IA ainsi qu'une diffusion appropriée de ces technologies. Ces outils réglementaires devront peut-être être adaptés à ce contexte spécifique, et certaines juridictions ont pris des mesures législatives ou ont élaboré des politiques pour encourager le développement de technologies d'IA à source ouverte.[30]

Une deuxième question concerne l'utilisation de données protégées par le droit d'auteur comme données d'entrée pour l'IA. Dans le cadre juridique international actuel de la propriété intellectuelle, des matériels tels que des textes originaux, des images originales et des compilations originales de données peuvent faire l'objet d'une protection par le droit d'auteur. Cela peut soulever la question de savoir si leur utilisation pour l'entraînement de l'IA équivaut à une atteinte au droit d'auteur. Cette question se traduit par la question de savoir si une telle utilisation est actuellement, ou devrait être, automatiquement admissible au titre d'exceptions au droit d'auteur exclusif (par exemple l'utilisation de matériels protégés par le droit d'auteur pour l'enseignement). L'application de ces exceptions limitées à l'IA générative, en particulier, est plus complexe que dans les cas traditionnels, en raison de facteurs tels que le volume des données utilisées et le but de l'utilisation.

Un troisième ensemble de questions concerne le point de savoir si les résultats générés de manière autonome par l'IA peuvent être protégés en tant que propriété intellectuelle. Le résultat produit par une IA est créé sur la base des schémas et des règles appris au cours du processus d'entraînement, au moyen des données d'entrée. Toutefois, ce résultat (qui peut revêtir la forme d'un contenu) n'est pas une simple reproduction ou recombinaison de ces données. De fait, le résultat peut prendre la forme d'éléments nouveaux et créatifs, témoignant de la capacité du système d'IA de comprendre et d'imiter les complexités des contenus générés par des humains. Ainsi, les résultats produits par l'IA peuvent englober un large éventail de créations et d'innovations,[31] dont des œuvres d'art, des œuvres littéraires, de la musique, des dessins, des films, des jeux vidéo et des inventions. L'IA étant de plus en plus capable de produire des résultats de manière autonome, les frontières entre les contributions humaines et de l'IA à la création ou aux inventions deviennent de plus en plus floues, ce qui rend la question de la paternité d'une invention ou d'une œuvre d'autant plus pressante et plus complexe.

Diverses approches ont été adoptées ou proposées pour trouver des réponses équilibrées et équitables à certaines des questions susmentionnées, en ce qui concerne à la fois les données d'entrée et les résultats de l'IA. En ce qui concerne les données d'entrée, les partisans de l'utilisation de matériel protégé par le droit d'auteur pour entraîner l'IA font valoir que cela constitue une utilisation « transformative », car le modèle ne reproduit pas les œuvres protégées par le droit d'auteur, mais crée du nouveau contenu inspiré des schémas appris. Ils font également valoir que cette utilisation n'a pas d'incidence négative sur le marché des œuvres originales et que, dans certains cas, elle pourrait éventuellement compléter ce marché. Le débat se poursuit. Il faut trouver une approche équilibrée tenant compte des intérêts moraux et économiques aussi bien des créateurs d'œuvres originales que des utilisateurs de l'IA, et la communauté juridique continue d'étudier ces questions. Les approches adoptées vis-à-vis de cette question diffèrent considérablement d'une juridiction à une autre (voir le chapitre 3 b)).

La question de la protection et de la propriété des résultats générés par l'IA appelle une réévaluation des cadres juridiques existants en matière de propriété intellectuelle. Comme il est indiqué plus haut, l'IA peut produire des résultats sous la forme d'une œuvre ou d'une invention. Cela soulève à son tour des questions sur le point de savoir si et/ou dans quelles circonstances des droits de propriété intellectuelle peuvent être accordés pour des créations ou des innovations générées par l'IA et, dans l'affirmative, qui, le cas échéant, détient la propriété intellectuelle qui en résulte ou qui est responsable si le résultat viole la propriété intellectuelle d'autrui. Est-ce l'auteur de l'outil d'IA, l'utilisateur dont les requêtes à l'IA ont abouti au résultat en question, ou ni l'un ni l'autre, puisque le créateur ou l'inventeur n'est pas humain ? Les lois actuelles sur la propriété intellectuelle attribuent la paternité des œuvres et des inventions, ainsi que les droits économiques qui en résultent, à des humains. Dans certaines juridictions, l'IA elle-même n'est pas reconnue comme créatrice ou inventrice dans le cadre juridique actuel de la propriété intellectuelle.[32] Dans d'autres, la question est ouverte à l'interprétation jurisprudentielle fondée sur les lois existantes.[33] Avec le déploiement généralisé de l'IA, qui peut désormais être utilisée par des personnes dans le monde entier, la question de la protection et de la propriété des résultats générés par l'IA devient une préoccupation constante et mondiale. Non seulement cette question met à l'épreuve la conception traditionnelle de la créativité et de la propriété, mais elle appelle aussi une réévaluation des cadres juridiques existants de la propriété intellectuelle à l'ère de l'IA (voir aussi le chapitre 4 f)).

b) La course mondiale à la promotion et à la réglementation de l'IA et le risque de fragmentation

L'immense potentiel de l'IA a incité les gouvernements du monde entier à prendre des mesures pour promouvoir son développement et son utilisation tout en atténuant les risques potentiels. Toutefois, le nombre croissant d'initiatives nationales, régionales et internationales et leur conception fragmentent le paysage politique, ce qui est susceptible d'avoir des conséquences négatives sur les entreprises qui font du commerce international. Les coûts économiques de la fragmentation montrent à quel point il est important de réduire l'hétérogénéité des réglementations.

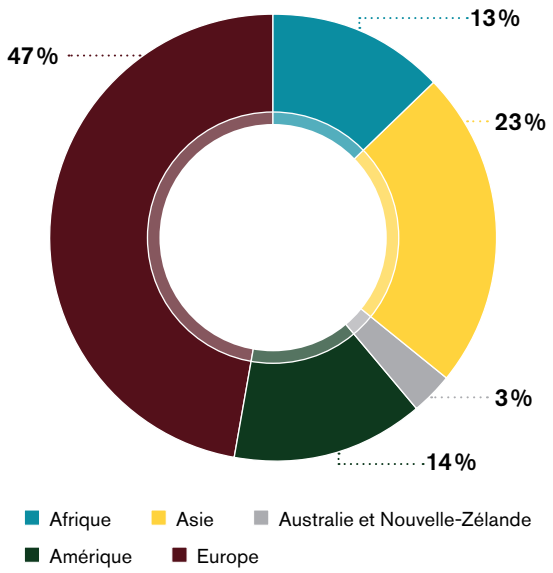
i) Initiatives nationales

Les gouvernements utilisent divers instruments pour promouvoir l'IA ainsi qu'en atténuer les risques et y remédier. Ces instruments vont des stratégies et politiques spécifiques à l'IA à des textes législatifs sectoriels (y compris la réglementation des données) et des mesures de politique commerciale. Toutefois, on remarque déjà des signes indiquant que l'hétérogénéité dans la conception de ces mesures pourrait conduire à une fragmentation réglementaire. Le grand nombre de stratégies et d'initiatives politiques nationales liées à l'IA montre qu'il s'agit d'un domaine prioritaire et l'on peut s'attendre à un niveau d'intervention élevé et soutenu dans un avenir proche, avec un risque potentiel de fragmentation croissante de la réglementation.

Stratégies et politiques en matière d'IA

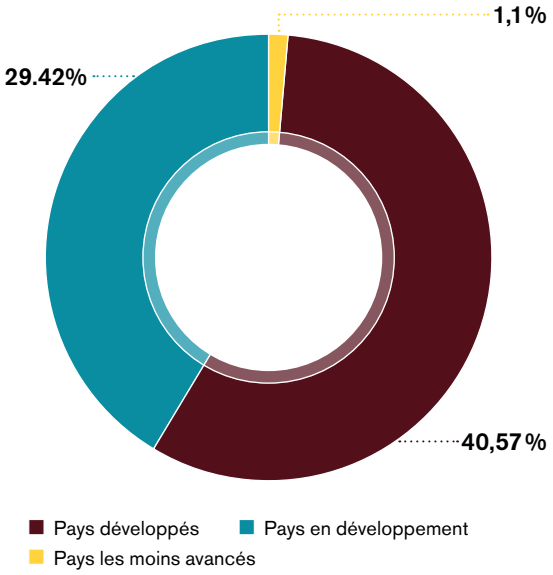
Un nombre croissant de juridictions mettent en place des stratégies et des politiques en matière d'IA au niveau national. Le nombre d'économies ayant mis en œuvre des stratégies en matière d'IA[34] est passé de trois en 2017 (Canada, Chine et Finlande) à 75 en 2023. Le Canada a lancé la première stratégie nationale dans ce domaine en mars 2017. Rien qu'en 2023, huit nouvelles stratégies ont été mises en place par des économies du Moyen-Orient, d'Afrique et des Caraïbes, témoignant de l'expansion mondiale de l'élaboration de politiques en matière d'IA (Maslej *et al.*, 2024). En outre, ou dans le cadre de ces stratégies nationales, les gouvernements du monde entier ont pris plus de 1 000 initiatives en matière d'IA.[35] La majorité de ces initiatives sont concentrées en Europe, suivie par l'Asie, l'Amérique et l'Afrique (voir la figure 3.4). La plupart des textes législatifs relatifs à l'IA adoptés depuis 2016 visent à renforcer les capacités de l'économie dans le domaine de l'IA, par la

Figure 3.4 : Nombre d'initiatives politiques en matière d'IA par région (2024)



Source : Base de données de l'OCDE sur les politiques nationales en matière d'IA (https://oecd.ai).

Figure 3.5 : Nombre d'initiatives politiques en matière d'IA par niveau de développement (2024)



Source : Base de données de l'OCDE sur les politiques nationales en matière d'IA (https://oecd.ai).

mise en place d'un réseau de superordinateurs accessibles au public par exemple, par opposition aux textes restrictifs, qui imposent des conditions ou des limites au déploiement ou à l'utilisation de l'IA (Maslej *et al.*, 2024).

L'Union européenne, Membre à part entière de l'OMC,[36] a été particulièrement active, avec l'adoption d'une série de mesures visant à soutenir le développement d'une IA digne de confiance au niveau de l'UE. Parmi ces mesures figurent le train de mesures sur l'innovation en matière d'IA,[37] le Plan coordonné dans le domaine de l'IA,[38] la « Proposition de clauses contractuelles types pour la passation de marchés par des organisations publiques dans le domaine de l'intelligence artificielle (IA) » et le règlement de l'UE sur l'IA (Union européenne, 2024). Le règlement sur l'IA, officiellement adopté en 2024, est le premier cadre juridique horizontal global au monde relatif à l'IA.[39] Son principal objectif officiel est de veiller à ce que les systèmes d'IA au sein de l'UE soient sûrs et conformes aux lois existantes en matière de droits fondamentaux, de normes et de valeurs.[40] Le règlement adopte une approche fondée sur les risques pour réglementer les systèmes d'IA.[41]

La plupart des initiatives politiques nationales en matière d'IA sont mises en œuvre par des économies développées, témoignant de la fracture croissante dans ce domaine. Si une part raisonnable (environ 30 %) des économies en développement ont mis en place des mesures en matière d'IA, ce n'est le cas que pour un seul PMA, l'Ouganda, avec deux politiques sectorielles et une politique générale concernant la gouvernance de l'IA (voir la figure 3.5). L'attention croissante accordée à l'IA dans l'élaboration des politiques est également visible dans les mentions s'y rapportant dans les procédures législatives, qui ont presque décuplé dans le monde depuis 2016, et quasi doublé entre 2022 et 2023 (Maslej *et al.*, 2024).

Les initiatives politiques nationales en matière d'IA peuvent être classées en quatre grandes catégories : gouvernance, soutien financier, lignes directrices et réglementation, et catalyseurs de l'IA. En mars 2024, plus d'un tiers (36 %) des initiatives politiques en matière d'IA répertoriées par l'Observatoire des politiques de l'IA de l'OCDE[42] concernaient la gouvernance de l'IA. Les aspects liés à la gouvernance se concentrent généralement sur la mise en place de cadres pour le développement et le déploiement de l'IA, y compris la coordination verticale et horizontale, l'intégration de l'IA dans le secteur public, les mécanismes de consultation publique et d'évaluation, et la création d'organismes ou de comités de réglementation chargés de superviser les activités liées à l'IA. Près de 19 % des initiatives politiques nationales en matière d'IA visent à fournir un soutien financier et des incitations en faveur de la recherche, du développement et de l'adoption de l'IA.[43] Environ 18 % de ces initiatives prévoient l'élaboration de lignes directrices et de réglementations (sur des questions telles que la confidentialité des données, la transparence des algorithmes, l'atténuation des biais et les normes de sécurité afin de promouvoir le développement et l'utilisation responsables et éthiques des technologies de l'IA), la création d'organismes de surveillance réglementaire et de conseil éthique afin d'accompagner et de superviser la mise en œuvre effective de ces réglementations, et l'élaboration de normes et de processus de certification pour faciliter le développement et l'adoption des technologies de l'IA conformément aux prescriptions réglementaires et aux principes éthiques. Enfin, un grand nombre d'initiatives politiques nationales en matière d'IA (environ 27 %) se concentrent sur la promotion d'un environnement propice à

Encadré 3.3 : Normes nationales en matière d'IA[44]

Les normes jouent un rôle important dans les approches politiques nationales en matière d'IA et plusieurs économies élaborent des stratégies ou mettent en place des initiatives spécifiques en vue de l'élaboration de normes dans le domaine de l'IA.[45] Certaines économies reconnaissent même ce domaine comme l'un des domaines prioritaires de leurs stratégies générales de normalisation.[46]

En juillet 2024, près de 170 normes étaient en cours d'élaboration ou avaient déjà été publiées par divers organismes nationaux de normalisation (tels que le BSI, le CEN, le CENELEC ou le NIST).[47] La plupart de ces normes nationales semblent être d'application horizontale, tandis que d'autres semblent être sectorielles, c'est-à-dire qu'elles concernent uniquement des branches de production et des secteurs spécifiques tels que les transports, les soins de santé ou l'énergie. Les normes relatives à l'IA couvrent divers grands domaines, le plus souvent liés à la gestion, la qualité, le traitement et la protection des données, ainsi qu'à la gestion des risques, à la sûreté et la sécurité, à l'interopérabilité et à la gouvernance organisationnelle. Ces normes portent sur des exigences techniques spécifiques telles que les processus, la gestion et la gouvernance, les méthodes de mesure et d'essai, la terminologie, les spécifications relatives à l'interface et à l'architecture, et les exigences relatives aux produits et aux résultats.[48]

Les diverses approches nationales en matière de normalisation ont en commun la reconnaissance de l'importance de l'engagement et de la coopération en matière de normalisation de l'IA au niveau international (Kerry, 2024).[49] Par exemple, le Plan d'action de l'Australie concernant l'IA reflète l'intention du pays de participer aux processus internationaux de normalisation,[50] tandis que l'Initiative mondiale sur la gouvernance de l'IA de la Chine encourage la coopération internationale en vue de l'élaboration de normes en matière d'IA sur la base d'un large consensus.[51] Dans le même ordre d'idées, l'Ordonnance exécutive des États-Unis sur le développement et l'utilisation sûrs, sécurisés et fiables de l'intelligence artificielle charge les organismes compétents de coopérer avec les organismes de normalisation afin de favoriser l'élaboration de normes consensuelles relatives à l'IA.[52]

À cet égard, comme dans d'autres domaines réglementaires, les efforts nationaux de normalisation en matière d'IA tendront au fil à temps à s'appuyer sur les travaux de normalisation internationaux.[53]

l'innovation dans ce domaine et à l'adoption de l'IA (c'est-à-dire les catalyseurs de l'IA). Il s'agit notamment d'initiatives visant à améliorer les compétences et l'enseignement dans le domaine de l'IA afin d'attirer les talents, de campagnes de sensibilisation du public destinées à mieux faire connaître l'IA, de la mise en place de plates-formes collaboratives, afin de réunir les parties prenantes au sein de l'écosystème de l'innovation, et de services de conseil aux entreprises, afin de soutenir l'innovation et l'entrepreneuriat (Maslej *et al.*, 2024). Certaines de ces initiatives, comme l'Ordonnance exécutive des États-Unis de 2023 sur le développement et l'utilisation sûrs, sécurisés et fiables de l'intelligence artificielle, contiennent des mesures visant à fournir un soutien en relation avec le matériel lié à l'IA, comme l'infrastructure informatique, ainsi qu'en faveur de la concurrence et de l'innovation dans le secteur des semi-conducteurs.

Les gouvernements semblent élaborer ou adopter un nombre croissant de règles et de règlements détaillés concernant la mise en œuvre et l'application de la législation relative à l'IA. Selon l'indice IA de 2024 de l'Université de Stanford, le nombre de mesures réglementaires liées à l'IA a considérablement augmenté aux États-Unis et dans l'Union européenne au cours des dernières années. En 2023, 25 mesures réglementaires en la matière ont été adoptées aux États-Unis, dont trois concernaient spécifiquement le commerce international et le financement international, contre une seule en 2016. Le nombre total de mesures réglementaires liées à l'IA a augmenté de 56,3 % rien qu'en 2023, pour atteindre 83. S'agissant de l'Union européenne, celle-ci a adopté près de 130 mesures réglementaires liées à l'IA depuis 2017, dont 13 pilotées par la Direction générale du commerce et la Direction générale de la concurrence (Maslej *et al.*, 2024). Plusieurs économies élaborent également des stratégies ou mettent en place des initiatives spécifiques en vue de l'élaboration de normes en matière d'IA (voir l'encadré 3.3.).

Les préoccupations environnementales figurent au premier rang des priorités politiques. Ainsi, les gouvernements commencent à élaborer des cadres réglementaires afin de remédier aux éventuels effets négatifs de l'IA sur l'environnement et de tirer parti de ses nombreux avantages. Par exemple, l'un des objectifs du règlement de l'UE sur l'IA est de garantir la « protection de l'environnement […] contre les effets néfastes des systèmes d'IA dans l'Union […] et […] [de] souten[ir] l'innovation ».[54] Voir aussi l'encadré 2.1 sur l'impact de l'IA sur l'environnement.

Un nombre croissant de juridictions mettent également en place des « bacs à sable » en matière d'IA L'objectif de ces initiatives est de tester de nouvelles approches économiques, institutionnelles et technologiques

ainsi que des dispositions juridiques sous la supervision d'un organisme de réglementation pendant une période limitée.[55] Une douzaine de juridictions, parmi lesquelles l'Allemagne, la Colombie, l'Estonie, la France, la Lituanie, Malte, la Norvège, le Royaume-Uni, Singapour et l'Union européenne, ont mis en place de telles structures (OCDE, 2023).

Certaines juridictions développent également des outils « GovTech » (outils numériques servant à optimiser les services publics) afin de répondre aux nouvelles difficultés en matière de réglementation posées par l'IA et de promouvoir une IA digne de confiance. Un exemple notable à cet égard est l'outil « AI Verify » de Singapour, développé par l'Autorité pour le développement de l'information, de la communication et des médias et la Commission de protection des données à caractère personnel.[56] Il s'agit d'un logiciel en source ouverte permettant d'évaluer la fiabilité des systèmes d'IA en fonction d'un ensemble de critères et de facteurs. Cet outil, qui en est au stade de produit minimum viable,[57] vise à automatiser l'évaluation de la transparence des systèmes d'IA, ce qui permettrait aux entreprises de savoir si les nouveaux systèmes d'IA sont conformes aux normes et réglementations internationales pertinentes (voir l'étude de cas sur l'approche de Singapour en matière d'IA dans l'encadré 3.4).

L'hétérogénéité des initiatives nationales est susceptible d'entraîner une fragmentation involontaire. Sur la base de l'analyse de onze recueils de règles sur l'IA de sept juridictions (Argentine, Brésil, Canada, Chine, États-Unis, République de Corée et Union européenne), Fritz *et al.* (2024) constatent que les gouvernements donnent la priorité à des objectifs différents dans leur réglementation relative à l'IA, utilisent des prescriptions réglementaires sensiblement différentes pour répondre à des priorités identiques et choisissent des formulations et des champs d'application différents pour atteindre la même exigence réglementaire pour une priorité donnée, ce qui entraîne une fragmentation involontaire au niveau des priorités, des exigences et des champs d'application.

La fragmentation involontaire s'étend à la législation sectorielle non spécifique à l'IA, telle que la réglementation relative à la propriété intellectuelle et aux données qui présente un intérêt pour l'IA. Les approches relatives à l'« utilisation équitable » du droit d'auteur, par exemple, diffèrent considérablement d'une juridiction à l'autre (voir le chapitre 3 a) iv)). Alors que le Japon a modifié sa loi sur le droit d'auteur en 2018 afin de permettre aux modèles d'apprentissage machine d'utiliser les œuvres protégées par le droit d'auteur à toutes fins, y compris commerciales, sans avoir besoin de l'autorisation expresse des détenteurs du droit d'auteur,[58] le règlement de l'UE sur l'IA est beaucoup moins permissif. Conformément à ce dernier, le fournisseur d'un modèle d'IA générative, qu'il soit en source ouverte ou fermée, doit établir une politique de respect du droit d'auteur de l'UE, y compris sa Directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique. En vertu de cette directive, les organismes de recherche sont autorisés à reproduire et à extraire des œuvres protégées par le droit d'auteur à des fins d'extraction de textes et de données sans avoir à demander l'autorisation du titulaire du droit d'auteur, à condition que ces organismes de recherche aient un accès légal aux œuvres et que l'utilisation soit destinée à la recherche scientifique. L'utilisation de matériels protégés par le droit d'auteur à des fins d'extraction de textes et de données pour quelque raison que ce soit est également autorisée au-delà de la recherche scientifique, mais dans ce cas, les titulaires du droit d'auteur ont la possibilité de réserver explicitement leurs droits et d'empêcher ainsi l'utilisation de leurs œuvres à ces fins sans leur accord (Parlement européen, 2024). De même, le projet de loi sur l'IA en cours d'adoption au Congrès brésilien prévoit, par exemple, une exception limitée au droit d'auteur lorsque l'extraction, la reproduction, le stockage et la transformation dans le cadre de processus d'extraction de textes et de données sont effectués par des organisations et institutions de recherche et journalistiques, des musées, des archives et des bibliothèques. Aux États-Unis, bien qu'il n'y ait toujours pas de législation ou de réglementation sur cette question, le New York Times a intenté une action en justice très médiatisée en décembre 2023 contre OpenAI pour utilisation non autorisée de son contenu. Un autre exemple est celui des approches divergentes pour les œuvres créées par des algorithmes (voir le chapitre 3 a) iv)). Alors que le Royaume-Uni protège les créations algorithmiques, sans toutefois reconnaître l'IA elle-même comme auteur,[59] l'Australie et les États-Unis précisent qu'un auteur humain est nécessaire (Liu et Lin, 2020). Enfin, certaines juridictions accordent une protection étendue aux secrets commerciaux, appliquant une protection exclusive au code source, aux algorithmes, au matériel de formation et aux ensembles de données utilisés pour entraîner les modèles d'IA, tandis que d'autres ne leur accordent pas de protection exclusive au titre de la propriété intellectuelle (Kilic, 2024). Au-delà de la propriété intellectuelle, la réglementation des données est également marquée par un niveau élevé de fragmentation.

La conception de certaines mesures peut affecter les concurrents sur le marché dans d'autres économies et avoir des effets de distorsion des échanges, entraînant une plus grande fragmentation. Le potentiel économique important de l'IA amène les autorités politiques de diverses juridictions à mettre en place des mesures visant à promouvoir son développement. Il peut s'agir de la création d'« usines d'IA », pour permettre aux jeunes entreprises et aux petites entreprises d'avoir accès à des superordinateurs avec lesquels elles peuvent concevoir leurs propres modèles, d'initiatives de recherche destinés à connecter des chercheurs et des éducateurs à des ressources informatiques, des données et des ressources pédagogiques afin de faire progresser la recherche sur l'IA et la recherche employant l'IA, et de subventions en faveur des entreprises qui achètent des puces destinées à l'IA produites dans le pays. Certaines de ces mesures semblent limiter les possibilités aux entités nationales ou accorder des incitations sous réserve que des produits nationaux soient utilisés (Aaronson, 2024b).

Les coûts économiques de la fragmentation réglementaire montrent à quel point il est important de réduire l'hétérogénéité des réglementations. L'incidence de la fragmentation peut être ressentie à différents niveaux, y compris dans la perte de possibilités

Encadré 3.4 : Étude de cas : l'approche de Singapour en matière d'IA

Pour Singapour, l'IA est un moyen nécessaire pour surmonter les contraintes naturelles, telles qu'une main-d'œuvre réduite sur une petite superficie, et pour accroître la productivité et renforcer la compétitivité de ses branches de production, tant dans les secteurs ouverts aux échanges internationaux, tels que le commerce et les finances, que dans les secteurs nationaux, tels que le commerce de détail et les produits alimentaires et les boissons.

Par exemple, Singapour s'appuie sur l'IA pour continuer à agir en tant que plaque tournante mondiale facilitant le commerce et la connectivité. L'aéroport de Changi, qui a accueilli plus de 59 millions de voyageurs l'année dernière, se sert de l'IA pour contrôler et trier les bagages, ainsi que pour alimenter la technologie de reconnaissance faciale permettant de simplifier les vérifications en matière d'immigration. Le port de Singapour, qui a traité un volume de fret de 39 millions d'équivalents vingt pieds (EVP) en 2023, utilise l'IA pour, entre autres, diriger le trafic maritime, cartographier les points d'amarrage, coordonner la livraison en flux tendu de marchandises et traiter les documents d'enregistrement. Afin de faciliter les communications et les échanges commerciaux dans une région hétérogène sur le plan linguistique comptant 680 millions de personnes parlant plus de 1 200 langues différentes, Singapour a également investi dans le développement du premier grand modèle de langage au monde adapté aux langues et aux cultures de l'Asie du Sud-Est ; ce modèle à source ouverte est dénommé SEA-LION, abréviation de Southeast Asian Languages in One Network (Un réseau pour les langues de l'Asie du Sud-Est).

En 2019, Singapour a publié un cadre pour une utilisation responsable de l'IA. Le Cadre type de gouvernance de l'IA fournit des orientations détaillées et pratiques pour aborder les principales questions d'éthique et de gouvernance dans le cadre du déploiement de solutions fondées sur l'IA. En 2024, Singapour a élargi le cadre type au-delà de l'IA traditionnelle pour prendre en compte l'IA générative et les nouveaux risques qu'elle pose. Au sein de l'Association des nations de l'Asie du Sud-Est (ASEAN), Singapour a dirigé l'élaboration d'un Guide de l'ASEAN sur la gouvernance et l'éthique de l'IA. Dans le cadre des Nations Unies, Singapour participe au Forum des petits États, un regroupement de 108 petites économies ; elle a introduit un pilier numérique en 2022, qui offre un renforcement des capacités de base sur des questions telles que l'IA, y compris plus récemment par le biais du Manuel de l'IA pour les petits États, qui a été élaboré conjointement avec le Rwanda et lancé au Sommet de l'avenir des Nations Unies en septembre 2024.

Singapour travaille en étroite collaboration avec divers partenaires, sur le plan bilatéral et dans le cadre de différents groupes, sur des lignes directrices relatives au développement et à l'innovation dans le domaine de l'IA. Avec les États-Unis, elle a approfondi le partage de renseignements et les consultations sur la sécurité, la sûreté, la confiance et l'élaboration de normes en matière d'IA au niveau international par le biais de collaborations dans le domaine de l'IA, y compris le Dialogue États-Unis-Singapour sur les technologies essentielles et émergentes.

Avec la Chine, Singapour améliore la compréhension mutuelle des approches relatives à la gouvernance de l'IA, par exemple dans le cadre du Dialogue inaugural Singapour-Chine sur la politique numérique. Elle participe également au processus d'Hiroshima du G-7, à la série de sommets sur la sécurité de l'IA, aux Principes de l'OCDE sur l'IA, au Partenariat mondial sur l'IA (PMIA) et à l'Alliance pour la gouvernance de l'IA du Forum économique mondial.

En 2022, Singapour a lancé IA Verify, un cadre de test de la gouvernance de l'IA et ensemble d'outils logiciels, qui contient des tests normalisés de base, couvrant les principes fondamentaux d'équité, d'explicabilité et de robustesse. En 2024, Singapour a lancé le projet Moonshot dans le cadre d'AI Verify, qui élargit l'ensemble d'outils initial pour couvrir l'IA générative et fournir des résultats intuitifs sur la qualité et la sécurité des grands modèles de langage. Compte tenu du fait que la science des tests et de la gouvernance de l'IA n'en est qu'à ses débuts, Singapour a également créé la Fondation AI Verify afin d'exploiter la puissance collective et les contributions de la communauté mondiale des logiciels à source ouverte pour développer conjointement les outils de test d'AI Verify. La Fondation compte aujourd'hui plus de 110 membres, dont des entreprises telles que Google, IBM, Microsoft, Red Hat, Meta et Salesforce.

Source : Sur la base des contributions du Ministère du développement numérique et de l'information de Singapour.

Encadré 3.5: Les difficultés liées à la complexité de la réglementation sur l'IA : l'exemple de Canvass AI

Invitée à prendre la parole à l'occasion d'un atelier de l'OMC sur la coopération dans le domaine de la réglementation des produits numériques, Humera Malik, PDG de Canvass AI, une jeune entreprise qui fournit des solutions industrielles en matière d'IA pour améliorer l'efficacité opérationnelle, la rentabilité et la durabilité, a expliqué qu'en raison de la diversité des approches en matière de réglementation de l'IA il était difficile d'avoir un rayonnement mondial. La divergence des réglementations pèse sur les ressources, rend difficile de s'y retrouver dans toutes les règles en l'absence de connaissances spécialisées et a une incidence sur l'entrée sur le marché. En outre, la réglementation relative à la protection des données impose des restrictions additionnelles qui affectent le développement de l'IA et l'entrée transfrontières sur le marché. L'intervenante a ajouté que « la réduction au minimum de la complexité et la promotion de la convergence faciliteraient grandement les efforts de mise en conformité ».

Source : https://www.wto.org/french/tratop_f/tbt_f/tbt_2006202310_f/tbt_2006202310_f.htm.

commerciales, une diminution des gains de productivité et un étouffement de l'innovation, avec des conséquences économiques potentiellement importantes pour les vendeurs de produits et de services reposant sur l'IA (Fritz et Giardini, 2024). Étant donné que les technologies de l'IA sont de plus en plus intégrées dans les produits et les services d'un grand nombre de secteurs, en l'absence d'efforts pour atténuer l'hétérogénéité réglementaire, les coûts et autres conséquences négatives qui en résultent sont susceptibles de croître de manière significative. L'incidence risque d'être particulièrement importante pour les petites entreprises, qui ont déjà du mal à s'y retrouver dans les différentes approches réglementaires en matière d'IA (voir l'encadré 3.5).

Réglementation des données

La réglementation des données fait partie des principales préoccupations politiques. Avec l'essor des technologies numériques, y compris de l'IA, les initiatives visant à promouvoir l'accès aux données pour favoriser l'innovation et la concurrence au niveau national, la protection de la vie privée et le contrôle des flux de données transfrontières figurent parmi les principales préoccupations politiques. Toutefois, on voit émerger un ensemble de mesures qui sont non seulement fragmentées, mais aussi susceptibles d'avoir des effets de distorsion sur le commerce.

Initiatives de données publiques ouvertes et de partage des données pour favoriser l'innovation et la concurrence

Un nombre croissant de juridictions prennent des initiatives pour promouvoir l'ouverture des données publiques afin de favoriser la création d'entreprises et l'innovation et d'accroître la concurrence sur les marchés intérieurs. Reconnaissant la valeur des données en tant que bien public, certaines juridictions, tant dans les économies développées que dans les économies en développement,[60] lancent des initiatives de données publiques ouvertes afin de promouvoir la création d'entreprises et l'innovation et de stimuler l'économie numérique et l'économie de l'IA au niveau national en encourageant l'utilisation, la réutilisation et la distribution gratuite d'ensembles de données publiques dans le cadre de licences de données ouvertes. On peut citer par exemple la Directive de l'UE sur les données ouvertes, la plate-forme de données publiques ouvertes de l'Inde[61] et l'initiative « Smart Nation » de Singapour.[62] Ces initiatives viennent s'ajouter aux réglementations *ex ante* de la concurrence mises en place sur certains marchés pour mieux répondre aux questions de concurrence soulevées par l'économie numérique.[63] L'ouverture des données publiques est un objectif qui est également poursuivi aux niveaux régional et international dans le contexte de l'Initiative liée à la Déclaration conjointe sur le commerce électronique de l'OMC (voir le chapitre 4 a) v)).

D'autres approches visent à promouvoir le partage des données entre les secteurs pour favoriser l'innovation ou à l'imposer pour contrebalancer la dynamique du « gagnant rafle tout » dans l'économie numérique. Le règlement de l'UE sur la gouvernance des données, par exemple, vise à renforcer la confiance dans le partage des données et la mise à disposition des données. Il est entré en vigueur en 2023 et soutient la mise en place de systèmes de partage de données fiables – appelés espaces européens communs de données – dans des domaines stratégiques, impliquant des acteurs privés comme publics. L'entraînement de systèmes d'IA figure parmi les principaux avantages de l'initiative (Commission européenne, 2024b). Le règlement de l'UE sur les données, qui est entré en vigueur en janvier 2024, vient compléter le règlement sur la gouvernance des données et crée les processus et les structures nécessaires pour faciliter le partage de données par les entreprises, les particuliers et le secteur public (Commission européenne, 2024a). Il protège les entreprises de l'UE dans le cadre

des contrats de partage de données contre les clauses contractuelles abusives qu'une partie contractante pourrait imposer à l'autre partie ; l'objectif est de permettre aux petites entreprises, en particulier, de participer plus activement au marché des données. D'autres économies ont mis en place des initiatives de partage de données, parmi lesquelles la Colombie, le Japon et la République de Corée. Certaines juridictions, comme l'Australie et l'Union européenne, expérimentent également l'obligation légale de partage de données afin de favoriser un environnement concurrentiel dans lequel les jeunes entreprises de l'IA ont également accès à de grands ensembles de données (Mayer-Schönberger et Ramge, 2018 ; Prüfer, 2020).

La mesure dans laquelle les initiatives de données publiques ouvertes et de partage de données soutiennent l'innovation et instaurent des conditions égales tant à l'intérieur des économies qu'entre elles reste difficile à déterminer. D'aucuns craignent que ces initiatives ne profitent en fait de manière disproportionnée aux grandes entreprises d'IA, car celles-ci ont la capacité de collecter des données ouvertes et de les mettre en corrélation avec les « données fermées » qu'elles possèdent et qu'elles contrôlent pour générer de nouvelles données. Ainsi, les grandes entreprises d'IA ont davantage à gagner que celles qui n'ont pas ces capacités et doivent s'en remettre entièrement aux données ouvertes, ce qui pourrait amplifier la fracture croissante entre les entreprises dans le domaine de l'IA (voir le chapitre 3 a)). Ces politiques pourraient également avoir des incidences géopolitiques, dans la mesure où les entreprises qui opèrent dans des économies numériques relativement grandes et fermées sont en mesure de capter des données ouvertes ailleurs dans le monde en plus des données qu'elles recueillent sur le marché intérieur sans trop de concurrence extérieure, ce qui pourrait entraîner de nouveaux déséquilibres entre les économies (Streinz, 2021).

En outre, si certaines initiatives de partage des données sont clairement ouvertes aux étrangers, cela reste incertain concernant d'autres. Cela pourrait soulever d'éventuelles questions concernant le traitement de la nation la plus favorisée (NPF) et entraîner des effets de distorsion des échanges. Le Japon, par exemple, a annoncé en 2024 que ses espaces de données seraient ouverts aux étrangers, mais les programmes de certaines autres juridictions semblent destinés à soutenir le partage de données au sein de la juridiction concernée, ce qui pourrait avoir un effet de distorsion des échanges (Aaronson, 2024).

Protection des données et de la vie privée

Au cours des dernières décennies, de nombreux gouvernements ont adopté des réglementations concernant la protection des données personnelles afin de répondre aux préoccupations croissantes concernant la protection de la vie privée. D'après ONU commerce et développement (CNUCED), plus de 70 % des juridictions – 137 sur 194 – avaient adopté une législation visant à garantir la protection des données et de la vie privée en 2021, avec des différences significatives selon le niveau de développement (CNUCED, 2021a). La proportion de juridictions ayant adopté une législation de ce type est la plus faible dans les PMA (48 %). Le Règlement général de l'UE sur la protection des données, qui est entré en vigueur en mai 2018, est l'exemple le plus connu dans ce domaine.

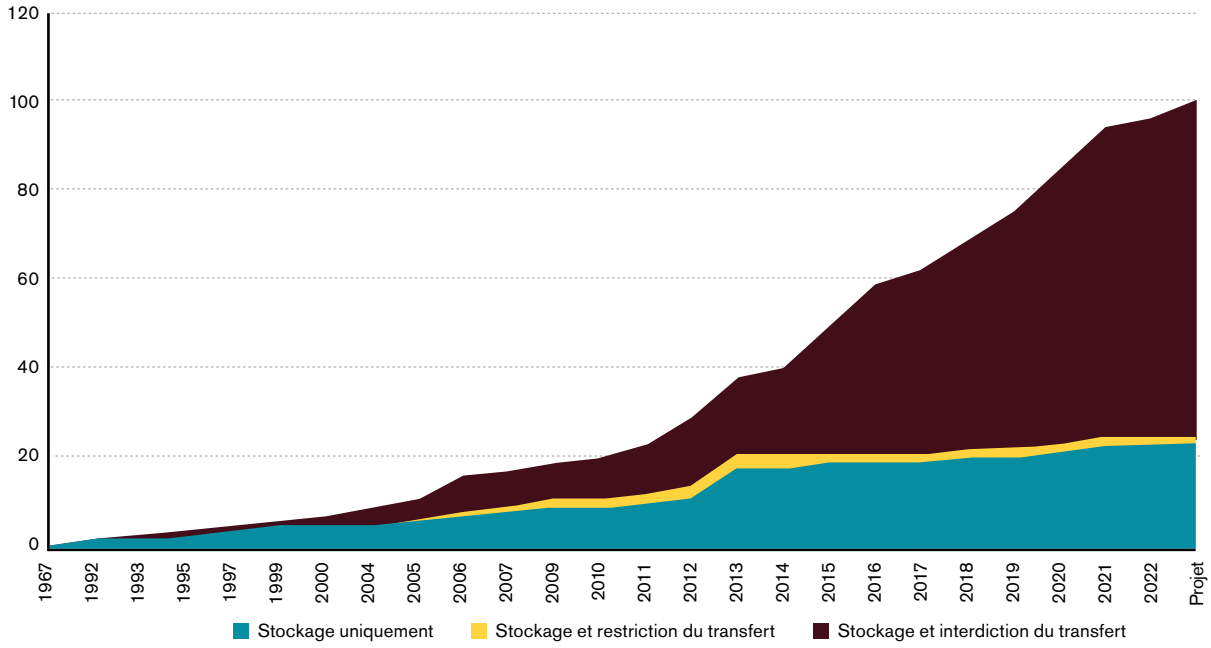
L'IA suscite de nouvelles préoccupations en matière de protection de la vie privée chez les particuliers et les consommateurs. Cet état de fait amène à devoir procéder à des compromis de plus en plus complexes entre la nécessité d'accéder à de grandes quantités de données pour entraîner des modèles d'IA et les préoccupations en matière de protection de la vie privée. Comme indiqué dans le chapitre 2, le fait que l'IA s'appuie sur de grandes quantités de données, y compris des données à caractère personnel, et sa capacité à traiter et à analyser de vastes ensembles de données et à établir des corrélations entre les données peuvent entraîner des atteintes à la vie privée et la diffusion d'informations, ce qui pose de nouveaux défis en matière de protection de la vie privée.

Les réglementations en matière de protection de la vie privée et des données personnelles diffèrent considérablement d'un pays à l'autre, ce qui affecte la circulation des données. La plupart des gouvernements ont adopté des lois sur la protection des données, mais celles-ci varient considérablement d'une juridiction à l'autre. Alors que certaines économies, comme les États-Unis, s'appuient principalement sur l'autoréglementation par la branche de production de la protection des données personnelles, d'autres suivent des approches différentes qui se concentrent sur l'intervention des pouvoirs publics pour défendre la souveraineté de l'État, les droits des citoyens, la sécurité ou le développement national (Bradford, 2023 ; Jones, 2023 ; Mitchell et Mishra, 2018 ; CNUCED, 2021b). Celles-ci prévoient notamment des limitations concernant le transfert international de données personnelles, qui visent à maintenir un contrôle juridictionnel. Ces différentes approches en matière de gouvernance des données créent des « courants » distincts qui favorisent une nouvelle fracture numérique entre ces juridictions et d'autres qui seront contraintes d'accepter ces règles, créant une incertitude réglementaire et des obstacles au transfert de données à travers les frontières (Aaronson et Leblond, 2018 ; Jones, 2023). La divergence des approches réglementaires entre l'Union européenne et les États-Unis illustre bien ce point, deux accords sur la confidentialité des données ayant été invalidés par la Cour de justice de l'Union européenne.[64]

Restrictions au transfert de données transfrontières et prescriptions concernant la localisation des données

Les restrictions au transfert de données transfrontières visent à limiter la circulation des données et le nombre de mesures visant à contrôler le lieu de stockage ou de traitement des données est en hausse. Les motivations à l'origine des restrictions au transfert de données transfrontières et des prescriptions concernant la localisation des données (c'est-à-dire l'obligation explicite de stockage et de traitement des données sur le territoire national) varient, allant des préoccupations concernant

Figure 3.6 : La localisation des données se développe et devient plus restrictive (Nombre de mesures)



Source : Del Giovane *et al.* (2023).

les données sensibles, liées à la sécurité nationale, à des considérations relatives à la protection de la vie privée. Ces mesures sont parfois considérées comme une incitation visant à stimuler la compétitivité au niveau local (Aaronson, 2024b ; McKinsey, 2022). Début 2023, on dénombrait 96 mesures de localisation des données en vigueur dans 40 économies, près de la moitié des mesures identifiées ayant vu le jour après 2015 (voir la figure 3.6). Non seulement le nombre de ces mesures a augmenté, mais celles-ci deviennent elles-mêmes plus restrictives, plus des deux tiers des mesures identifiées prévoyant non seulement une prescription relative au stockage, mais aussi une interdiction de transfert des données d'une économie à l'autre (Del Giovane *et al.*, 2023). Ces réglementations s'appliquent à différents types de données, y compris les données à caractère personnel, et à différents secteurs. Comme indiqué au chapitre 3 a), il est essentiel de trouver un juste équilibre entre la promotion de l'innovation en matière d'IA grâce à l'accès aux données et la protection de la vie privée afin de maximiser les avantages de l'IA pour le commerce international.

La fragmentation mondiale des réglementations relatives au transfert des données souligne la nécessité d'une coopération internationale accrue. Bien qu'il y ait des raisons légitimes pour cette diversité en matière de réglementation, le paysage actuel est de plus en plus complexe et fragmenté, imposant des coûts supplémentaires pour les entreprises, en particulier celles situées sur de petits marchés, créant de l'incertitude et entravant les flux transfrontières de données qui jouent un rôle essentiel dans le développement de l'IA et de l'innovation, en particulier pour les petites économies. Les coûts économiques de la fragmentation des réglementations en matière de flux de données par blocs géoéconomiques pourraient être importants, équivalant à une perte de plus de 1 % du PIB réel selon une étude de l'OCDE-OMC (OCDE et OMC, 2024). Une approche mondiale conciliant la nécessité d'une surveillance solide des données et la protection de la vie privée, tout en veillant à ce que les données soient accessibles et puissent circuler librement à travers les frontières, est nécessaire (Jones, 2023).

Mesures à la frontière

Bon nombre des composants matériels et des matières premières indispensables aux systèmes d'IA font l'objet de restrictions croissantes à l'exportation. Le nombre de restrictions à l'exportation visant les matières premières industrielles, dont beaucoup jouent un rôle essentiel dans la fabrication de puces de pointe nécessaires au fonctionnement des systèmes d'IA et dans les équipements de communication, a plus que quintuplé entre 2009 et 2020 (OCDE, 2023b). Plus récemment, la course à la domination dans le développement de l'IA, à laquelle viennent s'ajouter des considérations économiques, géopolitiques et de sécurité plus larges liées à la dualité d'usage des systèmes d'IA, a conduit un nombre croissant d'économies avancées à imposer des restrictions à l'exportation de puces de pointe essentielles aux systèmes d'IA et d'outils servant à leur fabrication.[65] En réaction, la Chine, qui est l'une des principales cibles de ces mesures, a demandé des consultations au titre du Mémorandum d'accord de l'OMC sur le règlement des différends (Mémorandum d'accord) en décembre 2022[66] et a imposé des restrictions à l'exportation de deux métaux utilisés dans la fabrication de puces et d'équipements de communication en juillet 2023.

Ces restrictions risquent d'affecter le développement et le déploiement des technologies de l'IA au niveau mondial et d'accroître la fragmentation économique et, éventuellement, technique. À court terme ou lorsqu'il existe peu de solutions de remplacement, les restrictions peuvent avoir une incidence sur l'accès à la technologie pour les économies importatrices. À plus long terme, les nouveaux développements technologiques pourraient être reportés en raison d'un manque d'accès aux technologies de pointe, ce qui aggraverait les risques de fragmentation économique et technique.

ii) Initiatives de coopération bilatérale et régionale concernant l'IA

Le nombre croissant d'initiatives de coopération bilatérale et régionale en matière de gouvernance de l'IA, axées sur des priorités différentes, ajoute au risque de créer de multiples approches fragmentées.

Les initiatives de coopération bilatérale portant sur des questions relatives à l'IA et au commerce donnent la priorité à des questions différentes. La coopération entre les États-Unis et l'Union européenne dans le cadre du Conseil du commerce et des technologies (CCT), qui a été créé dans le but de promouvoir cette coopération, se concentre principalement sur l'alignement de la terminologie et de la taxonomie et sur le suivi et la mesure des risques liés à l'IA (NIST, 2021). Le premier résultat auquel est parvenu le CCT en matière d'IA a été le lancement, en décembre 2022, d'une feuille de route conjointe sur les outils d'évaluation et de mesure pour une IA digne de confiance et la gestion des risques. Celle-ci vise à orienter la mise au point d'outils, de méthodes et d'approches dans le domaine de la gestion des risques liés à l'IA et de l'IA digne de confiance, à développer une interprétation commune des termes clés, à soutenir et piloter l'élaboration de normes internationales, et à surveiller et mesurer les risques existants et émergents liés à l'IA. En mai 2023, le CCT a adopté la « Terminologie et taxonomie UE-États-Unis pour l'intelligence artificielle – Première édition », qui s'appuie sur les normes existantes, telles que celles de l'Organisation internationale de normalisation (ISO), pour définir les termes clés liés à l'IA, mais ne définit pas l'IA.[67] En avril 2024, l'Union européenne et les États-Unis ont lancé une Alliance de recherche sur l'IA pour le bien public. Celle-ci vise à encourager la coopération scientifique afin de mieux exploiter l'IA au profit de l'environnement, de l'optimisation de l'énergie, de la réduction des catastrophes et des réponses aux situations d'urgence.[68]

D'autres initiatives bilatérales auxquelles les États-Unis participent se concentrent davantage sur la collaboration pour promouvoir l'alignement en termes généraux. En octobre 2023, les États-Unis et Singapour ont lancé un dialogue sur les technologies essentielles et émergentes,[69] qui établit un groupe de travail bilatéral sur la gouvernance de l'IA axé sur la promotion de principes communs pour une innovation sûre, digne de confiance et responsable en matière d'IA, et appelle à renforcer la collaboration par le biais d'un financement conjoint de la recherche et de l'enseignement et à envisager des programmes de certification réciproque pour les professionnels américains et singapouriens de l'IA sur la base de normes, d'essais et de critères de référence communs. Le dialogue prévoit une coopération en matière d'élaboration de normes et un exercice de cartographie entre les organismes nationaux de normalisation afin d'harmoniser les approches. En avril 2024, les États-Unis et l'Uruguay ont signé un mémorandum d'accord visant à encourager la coopération dans le domaine des technologies essentielles et émergentes, telles que les semi-conducteurs, l'IA, les flux de données, les télécommunications et la cybersécurité, y compris en identifiant les possibilités de soutenir l'élaboration et l'utilisation de normes internationales pertinentes et en encourageant l'interopérabilité et la compatibilité à l'échelle mondiale, ainsi qu'une plus grande coopération au sein des organisations multilatérales et internationales.

Les initiatives bilatérales de la Chine donnent la priorité à la sécurité et à la gouvernance de l'IA, ainsi qu'aux questions de développement. Le dialogue entre la Chine et les États-Unis se concentre principalement sur la sécurité et la gouvernance de l'IA. Annoncé en novembre 2023, le premier dialogue s'est tenu en mai 2024 (Maison Blanche, 2023b ; Murgia, 2024). La gouvernance mondiale de l'IA occupe également une place de choix dans les discussions de la Chine avec les dirigeants africains dans le cadre du Forum Chine-Afrique sur le développement d'Internet et la coopération dans ce domaine. Le dernier forum, qui s'est tenu en avril 2024, a appelé à une plus grande représentation des économies en développement dans la réglementation de l'IA. Outre les exemples susmentionnés, des dispositions visant à maintenir des dialogues bilatéraux sur l'IA figurent également dans certains accords commerciaux régionaux (ACR) et accords sur l'économie numérique (voir le chapitre 3 b) iii)).

Les approches en matière de gouvernance de l'IA lancées au niveau régional prennent différentes formes. Diverses initiatives régionales ont vu le jour en Afrique, en Asie et en Amérique latine. Certaines d'entre elles prennent la forme de déclarations ministérielles, telles que la Déclaration ministérielle du Marché commun du Sud (MERCOSUR) de novembre 2023 sur les principes des droits de l'homme dans le domaine de l'intelligence artificielle,[70] la Déclaration de Santiago d'octobre 2023 sur la promotion d'une intelligence artificielle éthique en Amérique latine et dans les Caraïbes,[71] et la Déclaration du Conseil des ministres des pays nordiques de mai 2018 sur l'IA dans la région des pays nordiques et baltes.[72] D'autres prennent la forme de guides, tels que le guide de l'Association des nations de l'Asie du Sud-Est (ASEAN) de février 2024 sur la gouvernance et l'éthique de l'IA (ASEAN, 2024), ou de documents de stratégie, tels que le Livre blanc de 2024 de l'Agence de développement de l'Union africaine – Nouveau partenariat pour le développement de l'Afrique (AUDA-NEPAD),[73] qui a conduit à l'adoption, le 17 juin 2024, de la Stratégie continentale de l'Union africaine sur l'intelligence artificielle.[74]

Certaines initiatives régionales mettent l'accent sur les droits de l'homme et l'éthique, tandis que d'autres se concentrent sur le développement économique et la croissance. La Déclaration du MERCOSUR met fortement l'accent sur les droits de l'homme et la transparence, soulignant l'importance d'éviter toute discrimination et de protéger la vie privée et l'intégrité des informations aux fins de la démocratie et de la préservation de la culture, tandis que la Déclaration de Santiago met l'accent sur les droits de l'homme et l'éthique. Le guide de l'ASEAN encourage l'alignement des normes de gouvernance et d'éthique de l'IA sur la base de sept principes directeurs,[75] mais ne cite pas la croissance inclusive, le développement durable et le bien-être – qui correspondent au premier des Principes de l'OCDE sur l'IA[76] – comme principes essentiels. Il contient des recommandations concernant les initiatives nationales et régionales[77] que les gouvernements de la région de l'ASEAN peuvent prendre pour assurer la conception, le développement et le déploiement responsables des systèmes d'IA. Pour leur part, le Livre blanc de l'AUDA-NEPAD et la Stratégie continentale de l'Union africaine sur l'intelligence artificielle se concentrent principalement sur l'exploitation du potentiel de l'IA en matière de développement et de croissance économiques, tout en encourageant son utilisation éthique, en minimisant les risques potentiels et en tirant parti des possibilités qu'elle offre. Le Livre blanc souligne l'importance de promouvoir l'innovation et de créer des outils multilingues africains grâce à l'IA afin de soutenir une « renaissance panafricaine au moyen de l'IA » et énumère cinq piliers d'action : le développement du capital humain dans le domaine de l'IA, l'infrastructure et les données, un environnement favorable au développement et au déploiement de l'IA, l'économie de l'IA et la promotion de l'investissement dans l'IA, et la mise en place de partenariats durables. La Stratégie continentale, adoptée en juin 2024, identifie quatre secteurs prioritaires : l'agriculture, les soins de santé, l'éducation et l'adaptation aux changements climatiques. De même, le Groupe de travail arabe sur l'IA se concentre principalement sur la coopération en vue de réduire la fracture numérique et d'encourager le renforcement des capacités.

iii) Accords commerciaux régionaux et accords sur l'économie numérique

Des dispositions spécifiques relatives à l'IA ont commencé à être intégrées dans les accords commerciaux régionaux (ACR) et les accords sur l'économie numérique,[78] mais prennent principalement la forme de dispositions non contraignantes. Bien que leur intégration dans ces accords constitue un fait positif, ces dispositions ne suffiront pas à empêcher la fragmentation réglementaire. Six accords contiennent des dispositions spécifiques concernant l'IA. Il s'agit de l'accord de libre-échange entre le Royaume-Uni et l'Australie, de l'accord de libre-échange entre le Royaume-Uni et la Nouvelle-Zélande et des accords sur l'économie numérique récemment signés entre l'Australie et Singapour (SADEA), entre le Chili, la Nouvelle-Zélande et Singapour (DEPA), entre Singapour et le Royaume-Uni (UKSDEA) et entre la République de Corée et Singapour (KSDPA), ainsi que d'un accord de libre-échange récemment signé entre l'Ukraine et le Royaume-Uni, qui n'est pas encore entré en vigueur.

Les dispositions relatives à l'IA prennent essentiellement la forme de clauses d'effort maximal (c'est-à-dire qui exigent des parties qu'elles fassent tout leur possible pour parvenir au résultat escompté). Les dispositions spécifiques relatives à l'IA reconnaissent généralement l'importance croissante de l'IA dans l'économie mondiale et comprennent des clauses d'effort maximal pour « collaborer et promouvoir »[79] l'élaboration de cadres de gouvernance afin de promouvoir une utilisation fiable, sûre et responsable de l'IA ou pour « élaborer »[80] de tels cadres en tenant compte des lignes directrices internationales ; les accords entre le Royaume-Uni et l'Australie et entre le Royaume-Uni et la Nouvelle-Zélande font spécifiquement référence aux Principes de l'OCDE de 2019 (OCDE, 2019a) (voir le chapitre 3 b) iv)). Certains accords, en particulier ceux signés par le Royaume-Uni, reconnaissent également l'importance d'une approche fondée sur les risques et axée sur les résultats et des principes de l'interopérabilité technologique et de la neutralité technologique,[81] et comprennent diverses dispositions relatives à la coopération concernant l'échange de renseignements et le partage de données d'expérience et de bonnes pratiques en matière de lois, de réglementations, de politiques, d'application et de respect des règles ;[82] à l'utilisation éthique, à la diversité humaine et aux biais involontaires, aux normes techniques émanant de l'industrie et la transparence des algorithmes ;[83] à la recherche ;[84] et à la participation active aux instances internationales ;[85] les accords entre le Royaume-Uni et l'Australie et entre le Royaume-Uni et l'Ukraine font explicitement référence à la coopération dans l'élaboration de normes, de réglementations et de procédures d'évaluation de la conformité au niveau international.

Plusieurs dispositions spécifiques à l'IA font explicitement référence au commerce. Trois accords – entre le Royaume-Uni et l'Ukraine,[86] entre le Royaume-Uni et Singapour[87] et entre le Royaume-Uni et l'Australie[88] – reconnaissent explicitement le rôle de l'IA dans la promotion de la compétitivité et la facilitation du commerce international. L'accord entre le Royaume-Uni et l'Australie encourage également les activités visant à faciliter et à promouvoir le commerce des technologies émergentes, et les accords entre le Royaume-Uni et l'Ukraine et entre le Royaume-Uni et Singapour encouragent la participation active aux instances internationales « sur les questions relatives à l'interaction du commerce et des technologies émergentes ».

Les dispositions relatives au commerce numérique figurant dans les ACR sont également importantes pour le développement et l'utilisation de l'IA. Le nombre d'ACR contenant des dispositions relatives au commerce numérique n'a cessé d'augmenter depuis le début des années 2000. La première disposition relative au commerce numérique se trouve dans l'Accord de libre-échange de 2000 entre la Jordanie et les États-Unis. Fin 2022, 116 ACR – représentant 33 % de tous les ACR existants – comportaient des dispositions relatives au commerce numérique (López-

González *et al.*, 2023). Ces dispositions portent généralement sur les flux de données, la localisation des données, la protection des données personnelles et l'accès aux données publiques, qui, comme indiqué dans les sections précédentes, jouent un rôle important dans la détermination de l'accès aux données nécessaires pour entraîner les modèles d'IA. Des dispositions interdisant les mesures imposant la divulgation du code source, des logiciels et des algorithmes ont également été incluses dans un certain nombre d'accords commerciaux, notamment ceux conclus par les États-Unis. Ces dispositions visent généralement à protéger les entreprises technologiques contre les mesures gouvernementales exigeant la divulgation de secrets commerciaux comme condition préalable à l'exercice d'activités dans certains secteurs (Jones *et al.*, 2024). L'accès au code source peut toutefois être important pour évaluer la fiabilité des systèmes d'IA (voir le chapitre 3 a) iii)). En outre, les interdictions de divulgation du code source peuvent avoir une incidence sur l'accès aux technologies et la concurrence sur le marché, et limiter la disponibilité de logiciels à source ouverte (Jones *et al.*, 2024). Les dispositions relatives au code source peuvent par conséquent avoir une incidence significative sur le développement et l'utilisation de l'IA et sur la promotion de la fiabilité de l'IA. D'autres dispositions relatives à l'adoption de normes et à l'évaluation de la conformité peuvent également jouer un rôle essentiel dans la promotion d'une l'IA digne de confiance (voir le chapitre 3 a) iii)), tandis que les dispositions relatives à la concurrence sur le marché numérique sont importantes pour lutter contre le pouvoir de concentration du marché de l'IA (voir le chapitre 3 a) i)). Enfin, les dispositions relatives aux droits de douane sur les transmissions électroniques ont joué un rôle important dans la promotion d'un environnement propice au commerce numérique (Groupe de la Banque mondiale, FMI, OCDE, OMC, ONU, 2023).

L'étendue des dispositions relatives au commerce numérique figurant dans les ACR varie considérablement, reflétant des approches divergentes. Sur la base de l'analyse des dispositions relatives au commerce numérique de 12 accords conclus entre mars 2018 et janvier 2023, Jones *et al.* (2024) constatent un degré élevé d'hétérogénéité entre les accords (voir la figure 3.7). Par exemple, si la plupart des accords contiennent des obligations contraignantes concernant la libre circulation des données, l'ACR entre le Royaume-Uni et l'Union européenne ne contient aucune disposition sur les flux de données non financières. S'agissant de la protection des données personnelles, les accords conclus par les États-Unis considèrent que les engagements volontaires pris par les entreprises privées constituent une protection suffisante, ce qui contraste avec l'approche globale de l'Union européenne en matière de protection des données dans le cadre du Règlement général sur la protection des données. Les dispositions sur l'ouverture des données publiques prennent la forme d'une clause d'effort maximal dans les accords conclus par les États-Unis et les accords sur l'économie numérique, tandis que l'Accord de libre-échange entre le Royaume-Uni et la Nouvelle-Zélande comporte des dispositions contraignantes mais non spécifiques. S'agissant de la divulgation du code source, les accords conclus par les États-Unis et les accords sur l'économie numérique prévoient une protection étendue et contraignante du code source, bien que les accords sur l'économie numérique ne mentionnent pas les algorithmes. En revanche, les accords signés par la Nouvelle-Zélande et le Partenariat économique régional global (RCEP) ne comportent aucune disposition de ce type.[89]

Peu d'économies en développement et de PMA ont négocié des dispositions relatives au commerce numérique. L'inclusion de dispositions détaillées relatives au commerce numérique tend à être plus fréquente dans les ACR négociés par les économies à revenu élevé et certaines économies à revenu intermédiaire et à revenu intermédiaire de la tranche supérieure. Seuls quelques PMA sont parties à des ACR contenant des dispositions relatives au commerce numérique (Groupe de la Banque mondiale, FMI, OCDE, OMC, ONU, 2023).

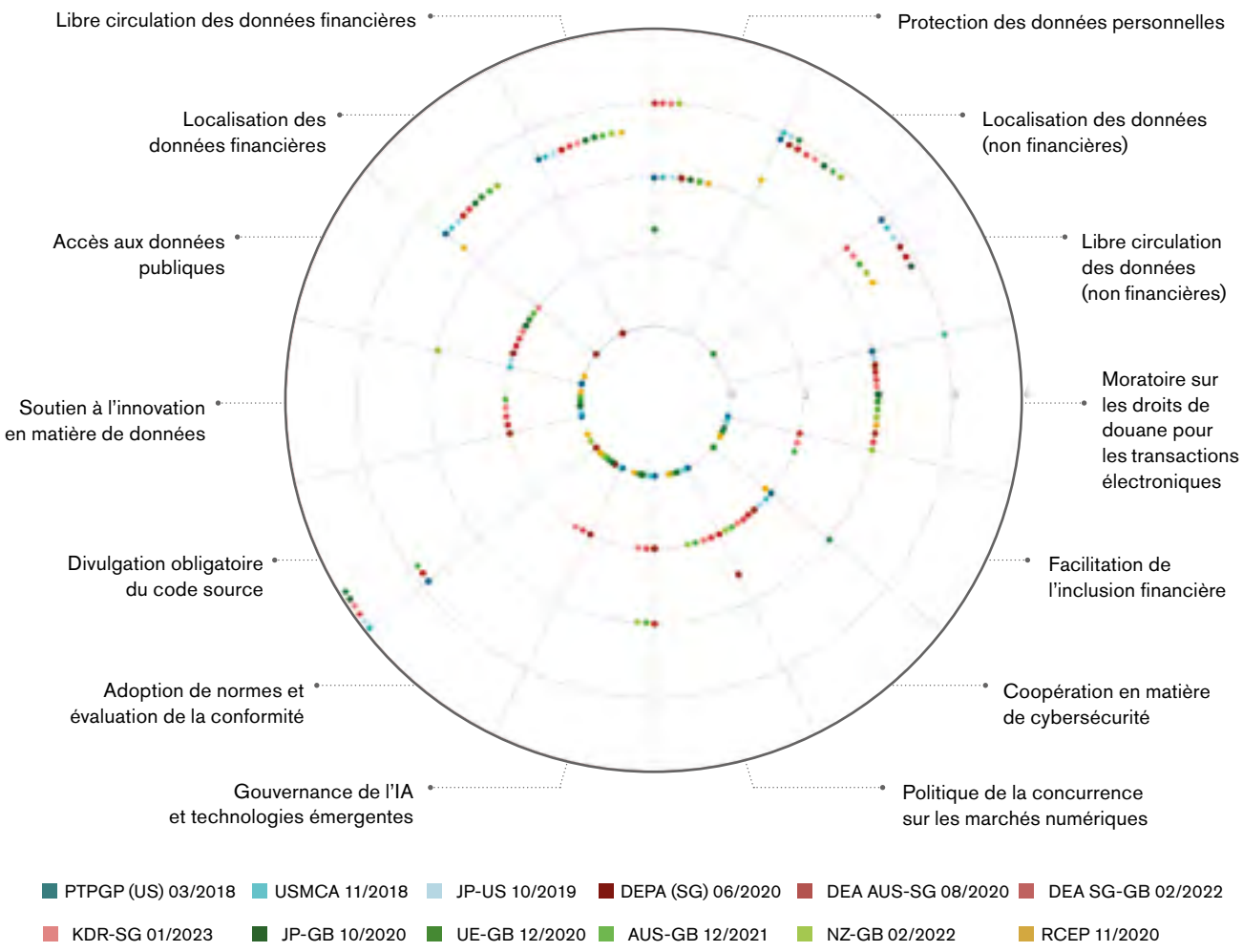
Les disciplines sur le commerce des services figurant dans les ACR sont également une voie importante par laquelle les politiques commerciales et les obligations commerciales des gouvernements peuvent affecter l'environnement politique de l'IA. Toutefois, le niveau des engagements pris varie considérablement d'une économie à l'autre. Les ACR sur les services prévoient des niveaux beaucoup plus élevés d'engagements en matière d'accès aux marchés et de traitement national que dans le cadre de l'Accord général sur le commerce des services (AGCS) de l'OMC pour différents modes de fourniture et secteurs de services, y compris pour les services numériques et les services liés à l'IA. Par exemple, dans le cadre des services informatiques, tous les Membres de l'OMC d'Europe, du Moyen-Orient et d'Amérique du Nord ont pris des engagements en matière d'accès aux marchés pour les services de traitement des données au titre de l'AGCS et/ou d'ACR, et il en va de même de la plupart des Membres d'Amérique latine et des Caraïbes (88 %), et d'Asie (91 %). Toutefois, en Afrique, seuls 26 % des Membres ont pris des engagements en matière d'accès aux marchés pour les services de traitement des données, que ce soit au titre de l'AGCS ou d'ACR, bien que cette proportion devrait augmenter une fois les engagements concernant les services pris au titre de l'Accord portant création de la zone de libre-échange continentale africaine (ZLECAf) seront entrés en vigueur et auront été notifiés à l'OMC (Roy et Sauvé, à paraître).[90]

iv) Initiatives internationales visant à relever les défis posés par l'IA

Initiatives politiques

Ces dernières années ont été marquées par une vague d'initiatives diverses liées à l'IA. Cette dynamique s'explique par la prise de conscience du fait que le caractère intrinsèquement international des risques et des avantages liés à l'IA rend nécessaires des discussions, une coopération et des solutions elles aussi internationales (voir la figure 3.8).[91]

Figure 3.7 : L'étendue des dispositions relatives au commerce numérique figurant dans les ACR varie considérablement



Source : Visualisation des auteurs sur la base de Jones *et al.* (2024).

Note : La valeur « 0 » (cercle intérieur) signifie que l'accord ne contient aucune disposition sur une question donnée. La valeur « 1 » signifie que l'accord contient une disposition rédigée en termes purement incitatifs. La valeur « 2 » signifie que l'engagement pris est contraignant mais non spécifique. La valeur « 3 » signifie que les engagements sont contraignants et spécifiques, les mesures à prendre (ou à ne pas prendre) étant décrites dans des termes clairs et précis. La valeur « 4 » signifie que les engagements sont contraignants et spécifiques, avec des obligations plus étendues et très détaillées. Les points situés entre deux lignes correspondent à la valeur plus élevée en termes d'engagements, mais avec des flexibilités. Plus les flexibilités sont importantes, plus le point est proche du cercle intérieur de la valeur inférieure.

Ces initiatives impliquent différentes parties prenantes et prennent différentes formes. Les initiatives internationales font intervenir un large éventail de parties prenantes, y compris des gouvernements, des organisations intergouvernementales, des organismes internationaux de normalisation et des entreprises. La plupart de ces initiatives prennent la forme de principes de haut niveau, d'orientations, de recommandations volontaires, de rapports scientifiques, de codes de conduite ou de listes d'exemples de politiques, tandis que d'autres prennent la forme de normes internationales. En mai 2024, le premier traité contraignant sur l'IA – la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit[92] – a été adopté.

Il y a des éléments de complémentarité entre ces initiatives et un alignement sur les principes fondamentaux, mais différentes initiatives donnent la priorité à différents aspects de la gouvernance de l'IA. Parmi les thèmes communs aux diverses initiatives internationales figurent, par exemple, la promotion d'une IA sûre, sécurisée, fiable, « centrée sur l'homme », éthique, transparente, responsable et interopérable, ainsi que l'identification et l'atténuation des risques liés à l'IA au moyen de diverses actions, de politiques nationales et de la coopération internationale.[93] Toutefois, dans certains cas, les initiatives internationales semblent définir des priorités différentes pour ces thèmes. Certaines initiatives, comme la Recommandation de l'Organisation des Nations Unies

Figure 3.8 : Principales initiatives politiques internationales dans le domaine de l'IA



* Parmi les signataires figurent l'Allemagne, l'Australie, le Canada, les États-Unis, la France, l'Italie, le Japon, la République de Corée, Singapour, le Royaume-Uni et l'Union européenne.

pour l'éducation, la science et la culture (UNESCO) sur l'éthique de l'IA, se concentrent sur des questions comme les droits de l'homme et l'éthique de l'IA, tandis que d'autres, comme la *Déclaration de Bletchley* sur la sécurité de l'IA, se concentrent sur la sûreté, la sécurité et la fiabilité de l'IA ou son interopérabilité.

Un certain nombre d'initiatives contiennent également divers éléments communs ayant une dimension commerciale et un lien avec l'OMC importants. Ces éléments comprennent :

- la reconnaissance du rôle de la réglementation et des normes (y compris les procédures de certification) dans l'encadrement de l'IA et l'importance de l'interopérabilité entre ces outils ;
- la nécessité d'éviter la fragmentation réglementaire en utilisant des normes internationales pour régir l'IA ;
- l'importance d'une approche appropriée et équilibrée de la protection et de l'application des droits de propriété intellectuelle ;
- l'importance de la vie privée, de la protection des données personnelles et de la gouvernance des données ; et
- l'importance de la coopération, de la coordination et du dialogue au niveau international.

Il est important de noter que des références explicites à l'OMC ont été incluses dans le rapport final de l'Organe consultatif de l'ONU sur l'IA. Celui-ci souligne la nécessité d'une « stratégie adaptée » et d'une coordination entre les nombreux processus et organisations internationaux produisant des documents clés relatifs à la gouvernance de l'IA, afin de fournir une « base normative commune pour tous les travaux liés à l'IA », et fait expressément référence à divers Accords de l'OMC, comme l'Accord général sur les tarifs douaniers et le commerce (GATT), l'Accord général sur le commerce des services (AGCS), l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC), l'Accord sur les obstacles techniques au commerce (OTC), l'Accord sur les technologies de l'information (ATI) et l'Accord sur la facilitation des échanges (AFE) (paragraphe 76 et figure 9 du rapport final). Le rapport souligne également le rôle central des normes internationales et de la coopération en matière de réglementation et reconnaît le rôle clé de l'OMC dans ce domaine (paragraphe 121).[94] Enfin, il recommande la création d'un « cadre mondial de données sur l'IA » auquel participeraient divers acteurs clés, y compris les économies et les organisations internationales pertinentes, dont l'OMC (paragraphe 170). Pour en savoir plus, se reporter à l'annexe 3.

Plusieurs de ces initiatives portent également sur l'impact environnemental de l'IA. C'est le cas, par exemple, des Principes de l'OCDE sur l'IA, des Principes du G-20 sur l'IA, de la Déclaration des chefs d'État et de gouvernement de New Delhi,[95] de la Recommandation de l'UNESCO sur l'IA, des Principes directeurs de l'IA et du Code de conduite de l'IA du G-7, de la Déclaration de Bletchley sur la sécurité de l'IA et du rapport de l'Organe consultatif de l'ONU sur l'IA. En outre, le comité technique mixte (JTC) 1 et le sous-comité 42 (SC) de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI) (ISO/CEI JTC 1/SC 42) élaborent actuellement une norme internationale portant spécifiquement sur les « aspects liés à la durabilité environnementale des systèmes d'IA ». La politique en matière d'IA a constitué une question clé lors du Sommet du G-20 tenu à Rio de Janeiro en novembre 2024, l'accent ayant été mis sur l'utilisation de l'IA au service du développement durable ; dans la Déclaration ministérielle de Trieste du G-7 adoptée en 2024, les économies du G-7 ont également exprimé leur désir de participer aux discussions du G-20 sur l'IA et la durabilité.

Cependant, il n'y a toujours pas d'harmonisation mondiale de la terminologie de l'IA. Un accord mondial sur la terminologie et les définitions clés de l'IA pourrait constituer un élément particulièrement important d'un point de vue commercial, car il serait susceptible de contribuer à garantir la cohérence et l'interopérabilité, et à éviter la fragmentation entre les différents régimes réglementaires nationaux en matière d'IA (Meltzer, 2023). Comme expliqué dans le présent rapport, la fragmentation réglementaire représente en elle-même un important obstacle au commerce, en particulier pour les économies en développement et les micro, petites et moyennes entreprises (MPME). À cet égard, les Principes de l'OCDE sur l'IA[96] contiennent diverses définitions relatives à l'IA, dont celles d'un « système d'IA »[97] et d'un « cycle de vie d'un système d'IA »,[98] qui sont essentielles à la mise en œuvre de toute stratégie ou politique nationale dans ce domaine, notamment aux fins de la réglementation. La Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit[99] contient également une définition d'un « système d'IA » qui est pratiquement identique à celle des Principes de l'OCDE.[100] L'ISO/CEI JTC 1/SG 42, qui se consacre à l'établissement de normes relatives l'IA, a adopté en 2022 un document[101] contenant un grand nombre de définitions et de termes détaillés dans le domaine de l'IA. Celui-ci comprend une définition d'un « système d'IA », qui présente des similitudes, mais aussi des différences, avec la définition figurant dans les Principes de l'OCDE. Enfin, si les Principes du G-20 sur l'IA[102] intègrent plus ou moins l'ensemble des principes de l'OCDE, ils n'en approuvent pas expressément les définitions, y compris celle d'un « système d'IA ». Contrairement à l'OCDE et à l'ISO/CEI, la Recommandation de l'UNESCO sur l'éthique de l'IA ne définit pas l'IA.[103]

Certaines initiatives semblent aller au-delà des principes ou orientations d'ordre général pour mettre en œuvre des actions plus ciblées ou plus spécifiques. Par exemple, afin de promouvoir les connaissances relatives aux approches et pratiques existantes, le G-20 a publié des exemples de politiques nationales visant à faire appliquer les Principes du G-20 sur l'intelligence artificielle[104] et des exemples de mesures pour une adoption accrue de l'IA par les MPME et les jeunes entreprises.[105] En 2024, le G-7 a annoncé son intention de faire progresser son processus d'Hiroshima sur l'IA de 2023. Les actions prévues comprennent l'élargissement des communications avec les gouvernements partenaires pour élargir le soutien en faveur des Principes directeurs et du Code de conduite de l'IA du G-7, l'intensification des efforts visant à encourager l'adhésion à ces deux instruments et le renforcement de la coopération

avec les instances multilatérales afin de promouvoir la vision du G-7 concernant les systèmes d'IA avancés.[106] En outre, dans le prolongement de la Déclaration de Bletchley de 2023 sur la sécurité de l'IA, les gouvernements sont convenus de charger un groupe d'experts de produire un rapport sur l'état des connaissances scientifiques semblable à celui du Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC),[107] qui aura pour but de passer en revue les travaux de recherche de pointe les plus récents sur les capacités des modèles d'IA exploratoires et les risques qu'ils posent. Le *Rapport scientifique international intérimaire sur la sécurité de l'IA avancée* a été publié en mai 2024[108] et résume le meilleur de la recherche existante, tout en identifiant les domaines de recherche prioritaires. Il ne formule pas de recommandations en matière de politique ou de réglementation, mais vise plutôt à éclairer l'élaboration des politiques nationales et internationales. Le rapport final devrait être publié avant le prochain sommet sur l'IA, qui devrait se tenir en février 2025 en France (voir aussi l'annexe 3).

Le chevauchement important des initiatives, les priorités divergentes et l'absence d'accord sur la terminologie essentielle risquent de poser des problèmes de mise en œuvre. Ces éléments sont susceptibles de limiter les efforts visant à prévenir la fragmentation. L'alignement sur des principes fondamentaux ne garantit pas l'alignement sur la manière dont ces principes peuvent être mis en œuvre dans la pratique. En l'absence d'une coordination solide, les initiatives internationales actuelles pourraient ne pas suffire à prévenir la fragmentation réglementaire au niveau mondial. La nécessité d'améliorer la coordination a été reconnue dans le rapport final (2024) de l'Organe consultatif de l'ONU sur l'IA publié en septembre 2024 et le dans le Pacte numérique mondial adopté par l'Assemblée générale des Nations Unies en septembre 2024. Le rapport final identifie trois « lacunes dans la gouvernance mondiale de l'IA » à combler : des problèmes de représentation, de coordination et de mise en œuvre. L'OMC a un rôle à jouer dans ces trois domaines et, comme indiqué plus haut, des références spécifiques à l'OMC figurent dans différentes parties du rapport final. S'agissant du Pacte numérique mondial, celui-ci comprend un engagement des Membres de l'ONU à lancer un dialogue mondial sur la gouvernance de l'IA auquel prendraient part les gouvernements et toutes les parties prenantes concernées (paragraphe 56).

Initiatives internationales visant à combler la fracture en matière d'IA

De plus en plus, les organisations internationales élaborent des cours sur l'IA et intègrent cette dernière dans leurs activités d'assistance technique, qui comportent pour certaines une composante commerciale. L'Union internationale des télécommunications (UIT), par exemple, propose un cours en ligne intitulé « La gouvernance de l'intelligence artificielle » et, en partenariat avec 40 autres organismes des Nations Unies, elle a lancé « AI for Good », une plate-forme mondiale sur l'IA axée sur l'action destinée à identifier les applications pratiques de l'IA en vue de faire progresser les Objectifs de développement durable (ODD) de l'ONU.[109] Cette initiative comprend un programme de webinaires en ligne qui se déroulent tout au long de l'année, ainsi qu'un sommet mondial annuel en présentiel. D'autres institutions spécialisées des Nations Unies ont élaboré des projets axés sur leurs propres domaines d'expertise. L'UNESCO, par exemple, a mis au point une méthode d'évaluation de l'état de préparation pour aider ses membres à mettre en œuvre sa Recommandation sur l'éthique de l'IA, et fournit une assistance technique ciblée dans ce cadre par le biais de projets tels que son programme d'évaluation des besoins en IA dans les pays africains.[110] Parallèlement, l'Organisation des Nations Unies pour le développement industriel (ONUDI) a organisé des dialogues sur le thème de l'autonomisation des PME des pays en développement grâce à l'intelligence artificielle[111] afin de promouvoir l'adoption de l'IA par les MPME des économies en développement, dans le but d'améliorer leur compétitivité et leur durabilité par le biais de conversations partagées. Une publication connexe de l'ONUDI contient des recommandations et des outils pratiques destinés à aider les MPME à faire face aux difficultés et à tirer parti de l'IA pour diverses fonctions commerciales et zones de production. S'agissant de la Banque mondiale, on relèvera deux projets notables ayant une dimension liée à l'AI : le projet « L'apprentissage machine en Algérie », qui vise à améliorer l'efficacité et l'intégrité des opérations douanières grâce à l'apprentissage machine et le projet « Analyse des fraudes au Kenya à l'aide d'applications d'IA », qui vise à améliorer le recouvrement des recettes grâce à des mesures de lutte contre la fraude.[112] Enfin, l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI) a élaboré un cours destiné aux organismes chargés de l'application des lois afin de les doter des ressources nécessaires pour institutionnaliser l'IA responsable, en veillant à sa conformité avec les droits de l'homme et l'éthique.[113]

L'Organe consultatif de l'ONU sur l'IA a appelé à la création d'un fonds mondial pour l'IA. Publié en septembre 2024, le rapport final de l'Organe consultatif de l'ONU sur l'IA recommande la création d'un fonds mondial pour l'IA afin « de réduire la fracture en la matière ». Géré par une structure de gouvernance indépendante, le fonds recevrait des contributions financières et des ressources en nature de sources publiques et privées, qui seraient allouées pour faciliter l'accès aux outils de l'IA, tels que des ressources de calcul mises en commun pour l'entraînement de modèles, des dispositifs expérimentaux et des ensembles de données conservés, « en vue de favoriser la réalisation des objectifs de développement durable au niveau local ».[114] Le Pacte numérique mondial,[115] qui a été adopté par l'Assemblée générale des Nations Unies en septembre 2024 après la publication du rapport de l'Organe consultatif de l'ONU sur l'IA, préconise « des formules novatrices de financement aux fins du renforcement des capacités d'intelligence artificielle, basées sur des contributions volontaires, tenant compte des recommandations formulées par l'Organe consultatif de haut niveau sur l'intelligence artificielle au sujet d'un fonds mondial pour l'IA ».

Notes

1. Voir https://eto.tech/.

2. Voir https://eto.tech/.

3. Voir https://oecd.ai/fr/data.

4. Voir https://ourworldindata.org/extreme-poverty-in-brief.

5. Voir https://stackoverflow.com/.

6. Voir https://ourworldindata.org/grapher/share-new-artificial-intelligence-cs-phds-female.

7. Dans le même temps, l'IA peut également favoriser la concurrence. Par exemple, elle donne aux consommateurs la possibilité d'utiliser de grands volumes de données pour personnaliser leurs recherches de produits et leurs transactions, et les aide à se repérer sur des marchés complexes ou incertains pour sélectionner les meilleures offres en fonction de leurs préférences. Cela pourrait conduire à l'émergence de « consommateurs algorithmiques », dont la prise de décisions serait partiellement automatisée par des algorithmes (Gal et Elkin-Koren, 2017).

8. Plusieurs affaires concernant le respect des règles en matière de concurrence ont récemment été engagées à l'encontre d'entreprises spécialisées dans l'IA. Par exemple, la Commission fédérale du commerce des États-Unis (FTC) a intenté une action en justice pour bloquer l'acquisition d'Arm Ltd. projetée par Nvidia, l'un des principaux producteurs de puces de pointe faisant fonctionner l'IA, qui a fini par renoncer à la transaction (voir https://www.ftc.gov/news-events/news/press-releases/2022/02/statement-regarding-termination-nvidia-corps-attempted-acquisition-arm-ltd). La Commission européenne, comme l'Autorité de la concurrence et des marchés du Royaume-Uni et la FTC, a également commencé à examiner si l'investissement de Microsoft dans OpenAI constituait une fusion (Commission européenne, 2024a). Conscientes des risques que l'IA pose pour la concurrence, les autorités de la concurrence de l'Union européenne, du Royaume-Uni et des États-Unis d'Amérique ont publié en juillet 2024 une déclaration conjointe sur la concurrence concernant les modèles de fondation d'IA générative et les produits de l'IA, qui énonce divers principes relatifs à la protection de la concurrence dans l'écosystème de l'IA (voir https://www.gov.uk/government/publications/joint-statement-on-competition-in-generative-ai-foundation-models-and-ai-products/joint-statement-on-competition-in-generative-ai-foundation-models-and-ai-products).

9. On peut citer comme exemple le fait que le moteur de recherche de Google peut donner de meilleurs résultats que celui de Microsoft parce qu'il dispose d'un accès plus large à des demandes plus rares. Le fait qu'il dispose de données diverses et, en particulier, sa capacité de prendre en compte des événements plus rares sont également importants pour la formulation de meilleures prédictions (Goldfarb et Trefler, 2018).

10. Toutefois, des avancées telles que l'apprentissage fédéré, qui permet à des entités situées en différents lieux de construire des modèles d'apprentissage machine en collaboration et sans échanger de données (c'est l'algorithme qui est transféré, et non les données elles-mêmes), et les fiducies de données (« data trusts »), un système et une entité juridique qui gère les données de quelqu'un en son nom, pourraient atténuer les difficultés liées aux flux de données transfrontières (Bonawitz et al., 2019; Forum économique mondial, 2020a).

11. Avec l'IA, même des données d'entreprises et des données opérationnelles non personnelles telles que des inventaires peuvent présenter des risques pour la protection de la vie privée. Ces données, stockées dans les réseaux d'entreprises, peuvent révéler par inadvertance des renseignements sur le personnel participant à la collecte ou à l'analyse des données. En outre, les métadonnées des communications en ligne, telles que les numéros de téléphone, les courriels ou les adresses IP, peuvent rendre les utilisateurs identifiables même si les données ne révèlent pas directement les identités personnelles (Lee-Makiyama, 2018).

12. Voir https://www.consilium.europa.eu/fr/press/press-releases/2024/10/10/eu-brings-product-liability-rules-in-line-with-digital-age-and-circular-economy/#:~:text=The%20EU's%20product%20liability%20regime,caused%20the%20injury%20or%20damage et https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52022PC0496.

13. La confiance est mentionnée dans les principes et déclarations internationaux concernant l'IA comme étant un attribut essentiel qu'un système d'IA devrait posséder. Voir, par exemple, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf, Organisation de coopération et de développement économiques (2019a) et Organisation des Nations Unies pour l'éducation, la science et la culture (2021). Dans la terminologie relative à l'IA, le terme « crédibilité » (ou le fait d'être digne de confiance) s'entend de la « capacité à satisfaire aux attentes d'une ou de plusieurs parties prenantes … de manière vérifiable » (par exemple, au moyen d'une certification par rapport à une spécification technique énoncée dans un règlement ou une norme). Plus précisément, la crédibilité d'un système d'IA a trait à sa capacité de satisfaire à diverses attentes, par exemple en termes de « fiabilité », de « disponibilité », de « résilience », de « sécurité », de « protection de la vie privée », de « sûreté », de « redevabilité », de « transparence », d'« intégrité », d'« authenticité », de « qualité » et d'« utilisabilité ». Voir la norme ISO/IEC 22989:2022, paragraphes 3.5.16 (crédibilité – définition) et 5.15 (crédibilité – concept). Voir aussi la norme ISO/IEC 24028:2020. Bien que l'expression IA « sûre et digne de confiance » soit fréquemment employée, étant donné que la « sûreté » est comprise dans la définition de la crédibilité reproduite plus haut, pour plus de simplicité, nous nous référerons uniquement à une IA digne de confiance dans le présent rapport.

14. Par exemple, les véhicules autonomes à intelligence artificielle peuvent présenter certains risques qui ne sont pas liés à leurs composants physiques. De fait, l'algorithme d'IA (et la façon dont il a été entraîné) peut amener le véhicule à se « comporter » de manière risquée, causant non seulement des dommages matériels (par exemple des blessures corporelles au conducteur, aux passagers ou à des piétons), mais aussi, fait unique, des préjudices immatériels (par exemple des atteintes à la vie privée ou à la cybersécurité, etc.). Voir le rapport de la Chambre des communes du Parlement britannique sur les véhicules autonomes (HC 519, 15 septembre 2023), paragraphe 66 (mentionnant des études qui mettent en garde quant au fait que « les flottes ou modèles de véhicules autonomes pourraient être la cible d'un "piratage systémique malveillant, possiblement terroriste" »). Les solutions réglementaires à ces risques non matériels peuvent aussi soulever des questions éthiques complexes, par exemple le fameux « problème du chariot », dans lequel un véhicule autonome doit « choisir », par exemple, entre heurter une personne âgée et heurter une mère et son enfant en bas âge (par exemple Wells (2023); Lin (2021)).

15. « Les blessures causées à des piétons en raison du dysfonctionnement du système d'IA d'un véhicule autonome serait un dommage physique tangible. En revanche, certains dommages, tels que les dommages psychologiques, peuvent ne pas être aussi tangibles ou quantifiables. D'autres aspects du

préjudice qui peuvent être immatériels ou difficiles à observer directement sont des biais ou une discrimination qui peuvent avoir une incidence disproportionnée et négative sur des communautés particulières, mais qui peuvent être difficiles à observer à l'échelle d'une personne. Les violations du droit fondamental à la vie privée peuvent aussi être immatérielles, telles que l'utilisation non transparente d'un système de surveillance des employés reposant sur l'IA ». Groupe de travail de l'OCDE sur la gouvernance de l'intelligence artificielle: Stocktaking for the development of an AI incident definition, document EP/AIGO(2022)11/FINAL (21 octobre 2023).

16. Voir, par exemple, Rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, COM(2020) 64 final (19 février 2020), pages 9 et 10. Voir https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0064.

17. Voir https://www.iso.org/fr/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0.

18. L'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC) traite, entre autres choses, de la protection des secrets commerciaux, y compris l'imposition de certaines conditions lorsque les pouvoirs publics accèdent à des renseignements exclusifs (« données non divulguées résultant d'essais ou d'autres données non divulguées ») et les utilisent à des fins de réglementation, quoiqu'uniquement dans le contexte de l'« approbation de la commercialisation » (par exemple, les procédures d'évaluation de la conformité telles que la certification et l'homologation) de produits pharmaceutiques et de produits chimiques pour l'agriculture (article 39:3). De même, l'Accord sur les obstacles techniques au commerce (OTC) exige que les Membres de l'OMC veillent à ce que le caractère confidentiel des renseignements dans le contexte des procédures d'évaluation de la conformité (par exemple la certification et l'approbation des produits) soit i) respecté « de la même façon » pour les produits importés et les produits nationaux et ii) respecté « de manière à ce que les intérêts commerciaux légitimes soient protégés. » (Article 5.2.4).

19. Mitchell et al. (2023) contient une analyse détaillée des circonstances dans lesquelles la réglementation de l'IA peut être effectuée sans qu'il soit nécessaire d'accéder au code source (essais de la « catégorie blanche » pour les systèmes d'IA à faible risque) et des circonstances dans lesquelles une compréhension et une explication plus approfondies des décisions et recommandations du système d'IA est nécessaire (systèmes d'IA à haut risque) et il est justifié d'exiger l'accès au code (essais de la « catégorie noire »).

20. RDC n° 657/2022 – Anvisa 26 https://antigo.anvisa.gov.br/documents/10181/5141677/RDC_657_2022_.pdf/f1c32f0e-21c7-415b-8b5d-06f4c539bbc3.

21. Telles qu'Israël, le Japon, la République de Corée, Singapour, le Royaume-Uni et les États-Unis. L'Indice mondial de l'IA (Global AI Index) 2024 publié par Tortoise Media classe les économies en fonction de leur capacité en matière d'IA au niveau international: https://www.tortoisemedia.com/intelligence/global-ai/.

22. « Évolution » en ce sens que certains systèmes d'IA permettent au produit de mieux remplir ses fonctions, de s'adapter et de s'ajuster au fil du temps pour une circonstance donnée ou pour un utilisateur donné, à mesure qu'il fonctionne dans la pratique et reçoit et traite davantage de données; une sorte de « produit de l'IA personnalisé » semblable à l'idée de « médecine personnalisée » (par exemple en utilisant la connaissance du profil génétique d'un patient pour sélectionner « le médicament ou la thérapie qui convient et l'administrer selon la dose ou la posologie qui convient » – voir https://www.genome.gov/genetics-glossary/Personalized-Medicine). En fait, l'IA peut être un moteur et un catalyseur pour faire progresser la médecine personnalisée dans le domaine de la médecine génomique. Voir Cesario et al. (2023); Organisation mondiale de la santé (2021).

23. À cet égard, le règlement de l'UE sur l'IA (2024a), par exemple, indique dans son préambule (considérant 5) que « l'IA peut générer des risques et causer des dommages aux intérêts publics et aux droits fondamentaux » et que « [c]es dommages peuvent être matériels ou immatériels, y compris physiques, psychologiques, sociétaux ou économiques » (pas d'italique dans l'original).

24. Lund et al. (2023) présentent un exemple utile de cette tension en ce qui concerne les dispositifs médicaux, expliquant que l'un des « principaux obstacles à l'utilisation de l'IA dans le domaine des soins de santé et donc de logiciels médicaux reposant sur l'IA » est le fait que la question de savoir « comment faire face au changement continu, c'est-à-dire les systèmes autonomes non verrouillés par opposition aux algorithmes verrouillés, constitue un défi. La force et les avantages de l'IA/l'apprentissage machine sont la capacité d'entraîner et d'améliorer le système sur la base de nouvelles données du monde réel. Toutefois, le système doit aussi rester continuellement sans danger pour les patients et les autres utilisateurs, et respecter les règlements applicables en ce qui concerne, par exemple, la validation ».

25. Par exemple, « [l]a personnalisation rend plus difficiles la traçabilité et l'application des prescriptions en matière de sécurité des produits et de cybersécurité – de nombreux produits (ou de nombreuses propriétés) changent constamment » (Lund et al. 2023).

26. Le règlement de l'UE sur l'IA (2024a), par exemple, semble contenir certaines dispositions sur cette question, car il exige que les systèmes d'IA soient certifiés à nouveau si, après avoir été déployés, ils présentent des « modifications substantielles » imprévues (telles qu'elles sont définies à l'article 1.5 23)), c'est-à-dire « … chaque fois que survient une modification susceptible d'avoir une incidence sur la conformité d'un système d'IA à haut risque avec le présent règlement (par exemple, un changement de système d'exploitation ou d'architecture logicielle) ou que la destination du système change, il convient de considérer ledit système d'IA comme un nouveau système d'IA devant être soumis à nouvelle procédure d'évaluation de la conformité ». Cependant, « les changements intervenant sur l'algorithme et la performance de systèmes d'IA qui continuent à « apprendre » après avoir été mis sur le marché ou mis en service, à savoir l'adaptation automatique de la façon dont les fonctions sont exécutées, ne devraient pas constituer une modification substantielle, à condition que ces changements aient été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité ». Le règlement de l'UE sur l'IA prévoit en outre qu'une surveillance après commercialisation des produits de l'IA pourrait « garantir que les risques potentiels découlant des systèmes d'IA qui continuent à « apprendre » après avoir été mis sur le marché ou mis en service puissent être traités plus efficacement et en temps utile ».

27. La norme ISO/IEC TR 24368 (2022) donne des exemples de domaines dans lesquels il existe un « risque croissant de résultats et de dommages indésirables sur les plans éthique et sociétal », par exemple d'ordre « financier » ou « psychologique »; pour la « santé ou la sécurité physique »; pour les « biens incorporels (par exemple vol de propriété intellectuelle, atteinte à la réputation d'une entreprise) »; pour les « systèmes sociaux ou politiques (par exemple, ingérence dans des élections, perte de confiance dans les autorités »; et pour les « libertés publiques (par exemple, emprisonnement ou autre punition non justifié, censure, violations de la vie privée) ».

28. Commentant le fait que la mise en œuvre du règlement sur l'IA pourrait impliquer l'adoption de normes techniques pour traiter les risques à la fois matériels (par exemple pour la santé) et immatériels (par exemple pour les droits fondamentaux), Smuha et Yeung (2024) font observer que, « … contrairement aux risques pour la sécurité générés par les produits chimiques, les machines

ou les déchets industriels, qui peuvent tous être observés et mesurés sur le plan matériel, les droits fondamentaux sont, en fait, des concepts politiques. Ces droits se voient accorder une protection juridique spéciale, de sorte que, pour évaluer une allégation d'ingérence, il faut porter une attention particulière à la nature et à la portée du droit pertinent et au contexte spécifique et localisé dans lequel il est allégué qu'un droit particulier est violé. Nous doutons donc sérieusement que les droits fondamentaux puissent un jour se traduire par des normes techniques généralisées qui puissent être mesurées précisément en termes quantitatifs, et d'une manière qui reflète fidèlement ce qu'ils sont et comment ils ont été interprétés dans le cadre de la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme».

29. Voir aussi le document officiel de l'OMC G/TBT/GEN/356, disponible à l'adresse https://docs.wto.org/.

30. Voir, par exemple, le règlement de l'Union européenne sur l'IA (https://artificialintelligenceact.eu/fr/), en vertu duquel tous les fournisseurs de «modèles d'IA à usage général» sont tenus de créer une documentation technique sur le processus d'entraînement et d'essai, d'établir une politique en matière de droit d'auteur et de fournir un résumé suffisamment détaillé du contenu utilisé pour l'entraînement. Les fournisseurs de modèles d'IA libres et ouverts, en revanche, sont seulement tenus d'établir une politique en matière de droit d'auteur et de présenter un résumé du contenu utilisé pour l'entraînement.

31. Si le droit d'auteur protège la création de l'esprit (humain), la protection par brevet est disponible pour les innovations techniques (par des humains).

32. US Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, disponible à l'adresse https://copyright.gov/ai/ai_policy_guidance.pdf; US Court of Appeals for the 9th Circuit, Naruto v. Slater, https://cdn.ca9.uscourts.gov/datastore/opinions/2018/04/23/16-15469.pdf; US District Court for the District of Columbia, Thaler v. Perlmutter, https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2022cv1564-24.

33. CJUE, Infopaq International A/S contre Danske Dagblades Forening, Affaire C-5/08 (Centre d'information sur la propriété intellectuelle, 2023; Zhou, 2019).

34. Les stratégies expriment la vision du gouvernement en ce qui concerne la contribution de la science, de la technologie et de l'innovation au développement social et économique d'une économie. Elles fixent les priorités concernant l'investissement public en matière de science, de technologie et d'innovation, et identifient l'orientation des réformes gouvernementales, par exemple dans des domaines tels que le financement de la recherche publique et la promotion de l'innovation dans les entreprises (OCDE, 2016b).

35. Voir la base de données de l'OCDE sur l'IA: https://oecd.ai/en/dashboards/overview.

36. Bien qu'elle ne soit pas un pays, l'Union européenne est habilitée à adopter une législation relative au commerce à l'échelle de l'UE dans les limites fixées par ses traités fondateurs.

37. Voir https://ec.europa.eu/commission/presscorner/detail/fr/ip_24_383.

38. Voir https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

39. Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les Règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) n° 2018/858, (UE) n° 2018/1139 et (UE) n° 2019/2144 et les Directives n° 2014/90/UE, (UE) n° 2016/797 et (UE) n° 2020/1828 (règlement sur l'intelligence artificielle). Le règlement a été publié au Journal officiel de l'UE le 12 juillet 2024 et est entré en vigueur 20 jours plus tard. Toutefois, la plupart de ses règles ne sont applicables que 24 mois après son entrée en vigueur, bien qu'il prévoit des périodes d'application plus courtes pour certaines règles (par exemple, les interdictions de «pratiques prohibées» qui sont répertoriées comme présentant des «risques inacceptables» s'appliqueront dès 6 mois après l'entrée en vigueur), ainsi que des périodes plus longues pour d'autres (par exemple 36 mois pour certains «systèmes à haut risque» visés par la législation d'harmonisation existante de l'UE et pour les systèmes d'IA à usage général sur le marché de l'UE).

40. Dans la notification en 2021 d'un projet de règlement sur l'IA (document G/TBT/N/EU/850), l'Union européenne a expliqué que cette proposition visait à fournir: «… un ensemble de recommandations destinées à aider l'organisation à développer, fournir ou utiliser des systèmes d'IA de manière responsable dans la poursuite de ses objectifs et à répondre aux exigences applicables, aux obligations liées aux parties intéressées et aux attentes de ces dernières. Il comprend les éléments suivants: les approches visant à établir la confiance dans les systèmes d'IA par la transparence, l'explicabilité, la contrôlabilité, etc.; les pièges techniques et les menaces et risques typiques associés aux systèmes d'IA, ainsi que les techniques et méthodes d'atténuation possibles; et les approches permettant d'évaluer et d'atteindre la disponibilité, la résilience, la fiabilité, la précision, la sûreté, la sécurité et la confidentialité des systèmes d'IA. Le document notifié s'applique à toute organisation, quels que soient sa taille, son type et sa nature, qui fournit ou utilise des produits ou des services recourant à des systèmes d'IA.»

41. Toutefois, certains experts estiment que certaines dispositions importantes du règlement sur l'IA ne suivent pas une approche purement fondée sur les risques (Ebers, 2024).

42. Voir https://oecd.ai/fr/.

43. Par exemple, le Royaume-Uni a engagé 100 millions de livres sterling dans la création d'un «modèle de fondation publique» pour soutenir les applications dans les universités, les petites entreprises et le secteur public (voir https://www.gov.uk/government/news/initial-100-million-for-expert-taskforce-to-help-uk-build-and-adopt-next-generation-of-safe-ai) et l'initiative de ressources nationales pour la recherche dans l'intelligence artificielle aux États-Unis travaille dans le même sens (voir https://new.nsf.gov/focus-areas/artificial-intelligence/nairr).

44. Les normes sont l'un des trois types d'obstacles techniques au commerce (OTC) établissant des spécifications de produits. Elles diffèrent toutefois des règlements techniques en ce qu'elles sont des documents d'application volontaire. Il n'est pas rare non plus que des normes adoptées par les gouvernements soient rendues obligatoires par la suite, devenant ainsi des règlements techniques. Les normes peuvent être élaborées par différentes entités au sein des Membres de l'OMC, y compris des organismes gouvernementaux et non gouvernementaux (OMC, 2021).

45. Voir, par exemple, Kerry (2024). Par exemple, en 2024, la Chine a publié un projet de lignes directrices concernant la normalisation de l'IA proposant l'élaboration de plus d'une cinquantaine de normes nationales et sectorielles et de plus d'une vingtaine de normes internationales en matière d'IA d'ici à 2026 (voir https://www.reuters.com/technology/china-issues-draft-guidelines-standardising-ai-industry-2024-01-17/ et https://mmlcgroup.com/miit-ai/). La Commission européenne a chargé les organismes européens de normalisation d'élaborer des normes relatives à l'IA eu égard au fait que les normes joueront un rôle important dans l'application des prescriptions du règlement de l'UE sur l'IA (https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=fr).

46. Par exemple, la stratégie chinoise de normalisation de 2021 a identifié l'IA comme l'un des domaines clés. Voir Kerry (2024).

47. Ce chiffre est fondé sur les données de l'AI Standard Hub et n'est donné qu'à titre d'illustration. Ces données sont présentées

sans préjudice et ne devraient pas être interprétées comme une prise de position sur la question de savoir si ces documents sont des « normes » au sens de la définition de l'Annexe 1 de l'Accord OTC. Voir https://aistandardshub.org/ai-standards-search/.

48. Voir l'AI Standards Hub à l'adresse suivante: https://aistandardshub.org.

49. Par exemple, l'Accord de l'OMC sur les obstacles techniques au commerce (OTC) exige que les Membres de l'OMC utilisent les normes internationales pertinentes comme base de leurs normes, règlements techniques et procédures de certification nationales (voir le chapitre 4).

50. Voir https://webarchive.nla.gov.au/awa/20220816053410/https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan.

51. Voir http://gd.china-embassy.gov.cn/eng/zxhd_1/202310/t20231024_11167412.htm.

52. Voir https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/. Voir également NIST « A Plan for Global Engagement on AI Standards » (version finale, juillet 2024 – disponible à l'adresse suivante: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-5.pdf) et la Stratégie de normalisation des États-Unis pour les technologies essentielles émergentes présentée à la réunion du Comité OTC des 21-23 juin 2023 (https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=r:/G/TBT/M90.pdf&Open=True, paragraphe 6.32).

53. Par exemple, l'Australie a participé activement aux travaux de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (CEI) (ISO/CEI JTC1/SC42) et, en 2024, elle a annoncé l'adoption de l'une des normes ISO/CEI JTC1/SC42 (voir https://www.standards.org.au/news/standards-australia-adopts-the-international-standard-for-ai-management-system-as-iso-iec-42001-2023).

54. Considérant 176 du préambule du règlement de l'UE sur l'IA.

55. Bien qu'il n'existe pas de définition convenue au niveau mondial, le Service de recherche du Parlement européen note dans son document intitulé « Artificial Intelligence Act and Regulatory Sandboxes » (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf) que « les bacs à sable réglementaires font généralement référence à des outils réglementaires permettant aux entreprises de tester et d'expérimenter des produits, services ou activités nouveaux et innovants sous la supervision d'un organisme de réglementation pendant une période de temps limitée. À cet effet, les bacs à sable réglementaires ont un double rôle: 1) ils favorisent l'apprentissage des entreprises, c'est-à-dire le développement et l'essai d'innovations dans un environnement réel; et 2) ils soutiennent l'apprentissage réglementaire, c'est-à-dire la formulation de régimes juridiques expérimentaux pour guider et soutenir les entreprises dans leurs activités d'innovation sous la supervision d'une autorité de réglementation ».

56. Voir https://aiverifyfoundation.sg.

57. C'est-à-dire la version initiale d'un produit qui ne comprend que les caractéristiques essentielles nécessaires pour répondre aux besoins de base des utilisateurs et recueillir des commentaires en vue d'améliorations futures.

58. Documents officiels de l'OMC IP/N/1/JPN/36, IP/N/1/JPN/C/6 et IP/C/M/92/Add.1, disponibles à l'adresse suivante: https://docs.wto.org/.

59. La Loi sur le droit d'auteur, les dessins et modèles et les brevets de 1988 du Royaume-Uni prévoit que la paternité est attribuée à « la personne ayant pris les arrangements nécessaires pour la réalisation de l'œuvre » (paragraphe 9 3)). D'autres juridictions de common law, telles que l'Inde (Loi de 1957 sur le droit d'auteur, paragraphe 2 d)), l'Irlande (Loi de 2000 sur le droit d'auteur et les droits connexes, paragraphe 21), la Nouvelle-Zélande (Loi de 1994 sur le droit d'auteur, paragraphe 5 1)) et l'Afrique du Sud (Loi de 1978 sur le droit d'auteur, paragraphe 1 iv)), suivent l'approche du Royaume-Uni.

60. Pour de plus amples renseignements sur les économies en développement qui mettent en œuvre des politiques d'ouverture des données publiques, voir Verhulst et Young (2017).

61. Voir https://data.gov.in/.

62. Voir https://perma.cc/JAX3-55U8. L'OCDE a récemment lancé un projet sur les données publiques ouvertes pour cartographier les pratiques des différentes économies et évaluer l'incidence de l'ouverture des données publiques (OCDE, 2019b).

63. Contrairement aux politiques antitrust, les réglementations ex ante s'appliquent au niveau d'une branche de production ou d'un secteur et visent à définir les conditions de concurrence des grandes entreprises sur le marché. C'est le cas du règlement de l'Union européenne sur les marchés numériques, qui est entré en vigueur en novembre 2022 et est devenu applicable, pour l'essentiel, le 2 mai 2023. Ce règlement vise à lutter contre le pouvoir de marché des grandes plates-formes numériques, appelées « gardiens ». Il vise à garantir une concurrence loyale et l'innovation sur le marché numérique en empêchant les gardiens d'imposer des conditions déloyales aux entreprises et aux consommateurs (Commission européenne, 2022). Le règlement prévoit des obligations spécifiques pour ces gardiens, comme le fait de permettre à des tiers d'interopérer avec leurs services et l'interdiction de favoriser leurs propres services. Le projet de loi du Royaume-Uni sur les marchés numériques, la concurrence et les consommateurs constitue un autre exemple de nouvelle approche ex ante des marchés numériques. Celui-ci encourage les entreprises les plus puissantes sur les marchés numériques dynamiques à collaborer avec les organismes de réglementation pour veiller au maintien de la concurrence sur une base continue. Voir https://www.gov.uk/government/news/changes-to-digital-markets-bill-introduced-to-ensure-fairer-competition-in-tech-industry#:~:text=The%20Digital%20Markets%2C%20Competition%20and,in%20and%20innovate%20new%20technology.

64. Les principes de la sphère de sécurité relatifs à la protection de la vie privée, qui ont été élaborés entre 1998 et 2000 pour empêcher la divulgation accidentelle ou la perte d'informations personnelles par les organisations privées de l'Union européenne ou des États-Unis qui stockent des données des clients, ont été invalidés par la Cour de justice de l'UE (CJUE) en 2020 suite à une plainte déposée par Max Schrems, un militant, avocat et auteur autrichien, contre Facebook pour violation de la vie privée, y compris la violation des lois européennes sur la protection de la vie privée et le transfert allégué de données personnelles à l'Agence nationale de la sécurité des États-Unis (NSA) dans le cadre du programme d'extraction de données PRISM de cette dernière. Ces principes ont été remplacés par le Bouclier de protection des données jusqu'en 2020, date à laquelle celui-ci a lui aussi été invalidé par la CJUE. Un nouvel accord a été conclu en juillet 2023 pour autoriser les transferts de données sur la base du mécanisme de « décision d'adéquation » du Règlement général de l'UE sur la protection des données.

65. Les États-Unis ont imposé des contrôles à l'exportation des semi-conducteurs en 2022, et ces restrictions ont été élargies au fil du temps. En 2023, les Pays-Bas ont imposé des restrictions sur la fabrication de puces de pointe. Le Royaume-Uni, le Canada et le Japon ont eux aussi imposé des restrictions par la suite. Voir Financial Times (2022) et Wolff (2022).

66. Voir https://www.wto.org/french/tratop_f/dispu_f/cases_f/ds615_f.htm.

67. Voir https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence.

68. Voir https://digital-strategy.ec.europa.eu/en/library/ai-public-good-eu-us-research-alliance-ai-public-good.

69. Voir https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/12/u-s-singapore-critical-and-emerging-technology-dialogue-joint-vision-statement/.

70. Voir https://www.raadh.mercosur.int/wp-content/uploads/2024/04/DECLARACION-SOBRE-LOS-PRINCIPIOS-DE-DERECHOS-HUMANOS-EN-EL-AMBITO-DE-LA-INTELIGENCIA-ARTIFICIAL.pdf.

71. Voir https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf.

72. Voir https://www.stjornarradid.is/library/04-Raduneytin/ForsAetisraduneytid/Framtidarnefnd/AI%20in%20the%20Nordic-Baltic%20region.pdf.

73. Voir https://dig.watch/resource/auda-nepad-white-paper-regulation-and-responsible-adoption-of-ai-in-africa-towards-achievement-of-au-agenda-2063.

74. Voir https://au.int/en/pressreleases/20240617/african-ministers-adopt-landmark-continental-artificial-intelligence-strategy#:~:text=The%20Continental%20AI%20Strategy%20provides,potential%20risks%2C%20and%20leveraging%20opportunities.

75. Ces sept principes directeurs sont la transparence et l'explicabilité, la justice et l'équité, la sécurité et la sûreté, la solidité et la fiabilité, le centrage sur l'humain, la protection de la vie privée et la gouvernance des données, et la responsabilité et l'intégrité.

76. Voir https://www.oecd.org/fr/themes/principes-de-l-ia.html.

77. Les recommandations nationales comprennent la valorisation des talents en matière d'IA et l'amélioration des compétences de la main-d'œuvre, le soutien de l'écosystème de l'innovation et la promotion de l'investissement dans les jeunes entreprises dans le domaine de l'IA, l'investissement dans la recherche-développement en matière d'IA, la promotion de l'adoption d'outils utiles par les entreprises pour mettre en œuvre le guide de l'ASEAN sur la gouvernance et l'éthique de l'IA et la sensibilisation des citoyens aux effets de l'IA dans la société. Les recommandations régionales sont les suivantes: établir un groupe de travail de l'ASEAN sur la gouvernance de l'IA composé de représentants des États membres pour piloter et superviser les initiatives en matière de gouvernance de l'IA dans la région; adapter le guide de l'IA pour traiter la gouvernance de l'IA générative; et établir un recueil de cas d'utilisation illustrant la mise en œuvre pratique du guide de l'IA par des organisations opérant au sein de l'ASEAN.

78. Les accords sur l'économie numérique constituent un nouveau type d'accord. Ils visent à réglementer le commerce numérique, les flux de données et les technologies émergentes comme l'IA. Ces accords constituent la réponse des gouvernements au besoin de cadres réglementaires adaptés aux complexités du commerce et de l'économie numériques. À ce jour, quatre accords sur l'économie numérique ont été signés et sont entrés en vigueur: l'Accord sur l'économie numérique entre Singapour et l'Australie (SADEA), signé en 2020; l'Accord de partenariat pour l'économie numérique (DEPA) entre le Chili, la Nouvelle-Zélande et Singapour, signé en 2020; l'Accord sur l'économie numérique entre le Royaume-Uni et Singapour (UKSDEA), signé en 2022; et l'Accord de partenariat numérique entre la République de Corée et Singapour (KSDPA), signé en 2022. D'autres sont en cours de négociation, parmi lesquels l'Accord-cadre sur l'économie numérique de l'ASEAN (DEFA) et l'Accord sur l'économie numérique entre l'AELE et Singapour.

79. KSDPA, DEPA et Royaume-Uni-Australie.

80. Royaume-Uni-Australie, Royaume-Uni-Nouvelle-Zélande et Royaume-Uni-Singapour (ce dernier précise «le cas échéant»).

81. Royaume-Uni-Ukraine, Royaume-Uni-Singapour et Royaume-Uni-Nouvelle-Zélande.

82. Royaume-Uni-Ukraine, KSDPA, Royaume-Uni-Singapour et Royaume-Uni-Nouvelle-Zélande.

83. Royaume-Uni-Ukraine, Royaume-Uni-Singapour et Royaume-Uni-Nouvelle-Zélande.

84. Royaume-Uni-Ukraine, Royaume-Uni-Singapour, SADEA et Royaume-Uni-Australie.

85. Royaume-Uni-Ukraine et Royaume-Uni-Nouvelle-Zélande.

86. Article 132-V.

87. Article 8.61-R.

88. Article 20.4.

89. La Nouvelle-Zélande a décidé d'exclure les dispositions relatives au code source de ses accords à la suite d'une décision rendue en novembre 2021 par le Tribunal de Waitangi, qui a estimé que la disposition relative au code source de l'Accord de partenariat transpacifique global et progressiste (PTPGP) était contraire au Traité de Waitangi après que des experts en technologie maoris ont fait valoir qu'il existait un risque d'hypothèses biaisées dans la conception algorithmique ou les données d'entraînement. Voir Jones (2024).

90. L'analyse de Roy et Sauvé (à paraître) est basée sur 142 ACR notifiés au titre de l'article V de l'AGCS.

91. Voir, par exemple, la Déclaration de Bletchley (2023b), qui dispose que «[b]on nombre des risques découlant de l'IA sont internationaux par nature et seront donc traités plus efficacement au moyen de la coopération internationale».

92. Voir https://www.coe.int/fr/web/artificial-intelligence/la-convention-cadre-sur-l-intelligence-artificielle.

93. Si, jusqu'à présent, les initiatives en matière de gouvernance mondiale de l'IA ont pour leur part «débouché sur des similitudes de langage, telles que l'importance de l'équité, de la responsabilité et de la transparence», les approches en matière de définition de l'IA sont quant à elles moins coordonnées et cohérentes (https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_interim_report_fr.pdf).

94. En appelant à l'organisation d'un «sommet sur les normes en matière d'IA» auquel participeraient les principaux organismes internationaux de normalisation (par exemple, l'Union internationale des télécommunications (UIT), l'Organisation internationale de normalisation (ISO)/la Commission électrotechnique internationale (CEI) et l'Institute of Electrical and Electronics Engineers (IEEE)) et en indiquant expressément que l'OMC devrait prendre part à ces discussions.

95. Voir https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf.

96. Voir https://www.oecd.org/fr/themes/principes-de-l-ia.html.

97. Voir la définition révisée d'un «système d'IA» donnée par l'OCDE: un «système d'IA» est «un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement».

98. Un «cycle de vie d'un système d'IA» implique: i) la conception, les données et les modèles; un enchaînement qui dépend du contexte et englobe la planification et la conception, la collecte et le traitement de données, ainsi que la construction des modèles; ii) la vérification et la validation; iii) le déploiement; et iv) l'exploitation et le suivi. Ces phases présentent souvent un caractère itératif et ne suivent pas nécessairement un ordre séquentiel. La décision

de mettre un terme à l'utilisation d'un système d'IA peut intervenir à n'importe quel stade de la phase d'exploitation et de suivi » – voir les Principes de l'OCDE sur l'IA (2019), section 1.I.

99. Voir https://www.coe.int/fr/web/artificial-intelligence/la-convention-cadre-sur-l-intelligence-artificielle.

100. Jusqu'à présent, certaines réglementations intérieures en matière d'IA, telles que le règlement de l'UE sur l'AI et le projet de loi n° 2338/2023 du Sénat brésilien, semblent avoir adopté, presque mot pour mot, les définitions des Principes de l'OCDE, y compris celle d'un « système d'IA ».

101. Voir ISO/CEI 22989:2022 (disponible à l'adresse suivante: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html).

102. Voir https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf.

103. Il est précisé à cet égard qu'elle « ne cherche pas à donner de définition unique de l'IA, celle-ci étant appelée à évoluer en fonction des progrès technologiques. Son objectif est plutôt de traiter des caractéristiques des systèmes d'IA qui revêtent une importance majeure sur le plan éthique ». Toutefois, la recommandation donne une idée générale de ce qu'il faut entendre par « systèmes d'IA », à savoir des « systèmes capables de traiter les données et l'information par un processus s'apparentant à un comportement intelligent, et comportant généralement des fonctions de raisonnement, d'apprentissage, de perception, d'anticipation, de planification ou de contrôle » (paragraphe 2). Pour l'UNESCO, cette conception large est « crucial[e] car le rythme rapide de l'évolution technologique rendrait rapidement obsolète toute définition fixe et étroite, et rendrait irréalisables des politiques évolutives » (UNESCO, 2023).

104. Voir https://g20.utoronto.ca/2020/2020-g20-digital-0722.html.

105. Voir http://www.g20italy.org/wp-content/uploads/2021/11/Annex1_DECLARATION-OF-G20-DIGITAL-MINISTERS-2021_FINAL.pdf.

106. Voir https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/390de76d-d4f5-4f45-a7b4-f6879c30c389/0fbffe8a/20231201_en_news_g7_result_00.pdf.

107. Voir https://www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-state-of-the-science-2-november/state-of-the-science-report-to-understand-capabilities-and-risks-of-frontier-ai-statement-by-the-chair-2-november-2023.

108. Voir https://assets.publishing.service.gov.uk/media/66f5311f080bdf716392e922/international_scientific_report_on_the_safety_of_advanced_ai_interim_report.pdf.

109. Voir https://aiforgood.itu.int/.

110. Voir https://unesdoc.unesco.org/ark:/48223/pf0000375321/PDF/375321fre.pdf.multi

111. Voir https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/unido/.

112. Voir https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/wbg/.

113. Voir https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/.

114. Voir https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_fr.pdf.

115. Voir https://www.un.org/techenvoy/fr/global-digital-compact.