Commerce électronique Accords de libre-échange, chapitres sur le numérique et impact sur le travail

Une analyse comparative de textes de traités et de leurs possibles incidences concrètes

ITUC CSI IGB Confédération syndicale internationale

Rédigé à l'intention de la Confédération syndicale internationale (CSI) par Duncan McCann, Chercheur principal, New Economics Foundation

New Economics Foundation

www.neweconomics.org

info@neweconomics.org

+44 (0)20 7820 6300

@NEF

Photo de couverture: Adobe Stock

Organisation caritative enregistrée sous le numéro 1055254

TABLE DES MATIÈRES

AVANT-PROPOS

Les propositions sur le commerce électronique au sein de l'OMC : une recette pour alimenter la cupidité des entreprises

Avant la crise du COVID-19, la confiance dans les gouvernements et même dans la démocratie était en train de s'effondrer dans le monde entier, 60 % des travailleurs de la planète se trouvaient dans des emplois informels qui ne leur conféraient ni droits ni protection, et des centaines de millions de personnes qui avaient pourtant un emploi n'arrivaient pas à joindre les deux bouts. La crise du COVID-19 a des effets catastrophiques à l'échelon mondial, qui s'ajoutent aux faiblesses existantes. L'insistance pour parvenir à un accord au sein de l'OMC sur le « commerce électronique » ne peut qu'exacerber les inégalités et les divisions, alors que le monde aurait besoin de formuler une réponse d'une seule voix. Un tel accord est tout simplement la recette pour alimenter l'insatiable cupidité des entreprises. Les gouvernements font la promotion de nouvelles règles susceptibles de réduire encore davantage leur propre faculté à adopter des réglementations qui défendent les intérêts de leur population ; en ce sens, ils se comportent plus en otages des grands groupes, y compris des gigantesques monopoles de la technologie, qu'en garants de l'intérêt public.

La technologie numérique détient un potentiel immense pour lutter contre les problèmes les plus pressants du monde en matière de climat, de pauvreté, d'inégalité, de santé, d'éducation et bien plus encore. Elle a un rôle considérable à jouer dans la lutte contre la propagation du virus SARS-CoV-2 et ses conséquences. Il est désormais plus important que jamais que les gouvernements concentrent leurs efforts sur l'exploitation de la technologie pour le bien public, plutôt que de la mettre au service d'un ordre du jour rédigé par les entreprises en vue de pérenniser leur propre pouvoir et de renforcer les inégalités et la méfiance.

Le présent rapport, commandité à la New Economics Foundation par la CSI, révèle plusieurs répercussions alarmantes que pourrait avoir un accord sur le commerce électronique, tout en mettant en exergue des éléments profondément préoccupants qui figurent déjà dans certains accords de libre-échange.

Le contrôle des données se trouve au cœur des propositions, et c'est par le biais de ce contrôle que le pouvoir des géants numériques tels qu'Amazon atteindrait de nouveaux sommets. Or leur pouvoir est déjà très étendu, du fait de l'incapacité des gouvernements à appliquer des politiques de concurrence susceptibles d'empêcher que ces entreprises dominent les marchés. Cette domination commerciale est vouée à une plus grande croissance encore, tant que les gouvernements ne parviendront pas à faire en sorte que les sociétés et technologies numériques jouent un rôle dans la lutte contre le COVID-19, en matière de traçage numérique et d'autres domaines, qui aille dans le sens de l'intérêt public, dans le plein respect des droits, au lieu de favoriser les exigences des entreprises.

Le présent rapport souligne de quelle manière un accord aligné sur les propositions actuelles entraînerait une augmentation du travail précaire, avec une « ubérisation » des emplois et une érosion des droits des travailleurs, et rendrait encore plus difficile de réglementer et de faire appliquer les règles face au pouvoir des Big Tech sur les travailleurs.

Compte tenu des préoccupations internationales concernant les incidences que pourraient avoir l'intelligence artificielle et le déploiement sans contrôle d'algorithmes, les dispositions prévues quant à la confidentialité des codes sources permettraient aux sociétés du numérique de maintenir l'opacité la plus complète et de faire disparaître tout recours possible contre la malfaisance d'entreprise, rendant ainsi impossible pour les victimes d'un dommage d'obtenir réparation. De même, l'utilisation de logiciels libres dans la passation de marchés publics pourrait être contestée, voire niée.

Il est important d'observer que les incidences d'un tel accord sur le commerce électronique s'observeraient bien au-delà du simple secteur de la technologie électronique. À mesure que les données et la numérisation se retrouvent au cœur du modèle des affaires dans tous les secteurs, les règles sur les données affectent tous les pans de l'économie et finissent par concerner chaque travailleur, chaque consommateur, chaque citoyen.

Les propositions viendraient entraver, et dans certains cas annihiler, le potentiel de croissance et de prospérité des petites et moyennes entreprises et elles affecteraient même l'agriculture, secteur dans lequel travaille la moitié des travailleurs de la planète. Les services publics, déjà sous-financés et mis à mal par diverses politiques, subiraient une nouvelle érosion due à l'incursion de monopoles numériques dans la prestation de services vitaux, alors que le développement d'industries nationales serait bloqué, en particulier dans des pays n'ayant pas encore un niveau technologique avancé. Des régimes de protection des données tels que le RGPD de l'UE seraient eux aussi mis à mal, et la neutralité d'internet mise en péril.

Les Big Tech cherchent à utiliser un accord sur le commerce électronique au sein de l'OMC pour avoir une meilleure prise sur l'économie mondiale, en opprimant encore plus les consommateurs et la population active. Une grande partie de ce que ces sociétés exigent n'est même pas en rapport avec le commerce ; cependant, l'OMC sous sa forme actuelle est un moyen dérobé de poursuivre les attaques contre le travail, la sphère privée, les droits de propriété et d'autres normes qui sont pourtant cruciales pour la démocratie.

Sachant que près de la moitié de la population mondiale n'a toujours pas pu entrer dans l'ère numérique, la mission de permettre à tout un chacun dans la planète de se connecter doit sans nul doute primer sur la volonté de certaines des sociétés les plus puissantes et les moins responsables du monde d'étendre leur pouvoir et de le graver dans la pierre à tout jamais.

Le mouvement syndical international s'opposera à l'élaboration de tout accord, au sein de l'OMC ou ailleurs, qui chercherait à saper si fondamentalement les intérêts des travailleurs et de la population dans son ensemble.

Sharan Burrow, Secrétaire générale
Confédération syndicale internationale

INTRODUCTION

Lorsque vous surfez sur internet, que vous envoyez des messages ou des courriels et que vous vous déplacez dans une ville en utilisant une application de cartographie en ligne, vous créez des données. Ces données, si elles sont analysées de manière adéquate, peuvent en dire beaucoup sur vos comportements. Les sociétés du Big data s'empressent de collecter vos données en échange d'une service « gratuit », telle une application qui vous aide à compter les calories ingérées, et vous y consentez dès que vous cliquez sur « J'accepte » à la fin d'un long document sur les Conditions générales d'utilisation… que vous ne lisez jamais.

La valeur des données d'une personne à titre individuel est plutôt insignifiante. Cependant, lorsque ces données sont agrégées en des millions de points de données, des algorithmes bien conçus sont en mesure d'en extraire des conclusions précieuses sur la consommation, les moyens de transport, le travail ou autres. Ces conclusions sont ensuite utilisées afin de cibler les bons consommateurs au bon moment ou de proposer des réaménagements sur le lieu de travail susceptibles d'accroître la productivité.

Les sociétés du Big data tirent un profit immense de cet avantage conséquent en termes d'information, qu'elles peuvent exploiter pour transformer l'économie mondiale et le monde du travail en fonction de leurs propres besoins. Ces transformations sont déjà en train de survenir et ce, en dehors de tout contrôle exercé par les travailleurs ou de tout contrôle démocratique. Par exemple, les dispositifs portables tels que les montres intelligentes peuvent indiquer à leurs contrôleurs logiciels de quelle manière nous travaillons ; ces derniers pourront utiliser les données que nous produisons pour resserrer la surveillance des travailleurs, accroître les contrôles et éventuellement, dans certains cas, automatiser nos tâches et nous faire perdre notre emploi. Les applications dans le secteur agricole mettent aujourd'hui sous les feux de la rampe des informations jusqu'à présent méconnues au sujet des tâches agricoles, des risques, des entrants et des futures récoltes, ce qui finira par modifier la nature du travail dans ces secteurs. L'analyse des métadonnées (Big data) permet aux entreprises d'utiliser un savoir pour accroître leur captation de valeur dans les chaînes d'approvisionnement et d'avoir la mainmise sur la valeur ajoutée tout en transformant le secteur.

Les nouvelles technologies et la révolution des données sont porteuses d'occasions immenses pour répondre aux défis qui se posent à l'humanité : le réchauffement climatique, les mauvaises conditions de travail, la faim, les maladies. L'histoire a toutefois démontré que toutes les révolutions technologiques n'atteignent pas forcément tout le monde. Près de 1,2 milliard de personnes doivent encore accéder à la deuxième révolution industrielle, tandis que d'autres entrent déjà dans la quatrième.

La révolution technologique ne va pas automatiquement se faire à notre avantage collectif.

En fait, les grandes entreprises et les gouvernements des pays qui les accueillent déploient déjà tous leurs efforts pour faire en sorte de conserver le contrôle sur les nouvelles technologies et dicter les règles de la gouvernance des données. À cette fin, ces entreprises poussent leurs gouvernements à accepter des engagements spécifiques dans les accords de libre-échange. Le premier traité à inclure un chapitre entier sur le commerce électronique était l'accord de libre-échange (ALE) de 2003 entre Singapour et l'Australie[1].

La 11e Conférence ministérielle de l'OMC s'est certes conclue sans l'adoption d'une déclaration finale, mais un certain nombre d'initiatives ont été annoncées à cette occasion. L'une d'entre elles faisait état de l'intention de démarrer des négociations sur le commerce électronique et provenait d'un groupe de 70 Membres, des pays industrialisés pour la plupart. Par la suite six autres pays se sont joints au groupe, et en janvier 2019 ces Membres ont lancé des négociations plurilatérales sur le commerce électronique au sein de l'OMC. Le mandat n'a pas été confié à l'ensemble de l'OMC étant donné qu'un grand groupe de pays en développement avait réussi à bloquer le lancement de nouvelles négociations officielles sur le commerce numérique. La finalité de ces négociations plurilatérales est de convenir de dispositions sur le commerce numérique qui finiraient par asseoir la subordination numérique des petites entreprises, entraîner un grave déséquilibre du pouvoir de négociation entre le capital et le travail et ne donner aux pays en développement qu'une possibilité restreinte de façonner leurs propres stratégies de numérisation.

L'accord sur le commerce électronique constituerait un cadre permettant de discipliner la capacité de nos gouvernements à réglementer et à faire appliquer des lois dans le cyberespace. Uber prétend être une entreprise du numérique et non pas une société de taxis ; Fintech prétend fournir des services numériques et non pas des prêts réels soumis aux règles financières. L'internet leur donne l'excuse de se soustraire à différents aspects du droit national et de ses domaines de compétence, y compris la fiscalité. Et elles veulent que ces privilèges soient gravés dans la pierre.

1 Weber, R. (10 septembre 2015). *The expansion of e-commerce in Asia-Pacific trade agreements (L'expansion du commerce électronique dans les accords de libre-échange en Asie-Pacifique).* Consulté sur : https://www.ictsd.org/opinion/the-expansion-of-e-commerce-in-asia-pacific-trade-agreements

L'importance du commerce électronique va croissant, soutenue par le développement et l'expansion de la vitesse et de la portée des réseaux numériques. Les ventes du commerce électronique au détail avaient atteint 3 530 milliards de dollars en 2019 à l'échelle mondiale et l'on s'attend à une augmentation des recettes du commerce électronique au détail qui atteindraient 6 540 milliards de dollars en 2022[2]. Et tout comme le numérique s'infiltre désormais dans d'autres secteurs toujours plus nombreux, les chapitres sur le numérique dans les accords de libre-échange ont pris de l'ampleur et portent sur des questions qui dépassent, de loin, la portée originelle qui consistait à faciliter les échanges passant par internet.

Par exemple, un des nouveaux domaines les plus importants à avoir été inclus dans les accords de libre-échange est l'exigence d'une libre circulation des données par-delà les frontières. En incluant cette disposition dans les accords de libre-échange, la volonté est de contribuer à faire en sorte que la propriété des données, par défaut, relève du privé, et que les grandes entreprises transnationales aient la faculté de faire circuler librement les données de par le monde avec une réglementation minimale, voire inexistante.

L'élargissement de la portée des chapitres numériques, qui s'ajoute à la centralité des données pour le commerce mondial (on estime qu'en 2020 les flux de données vont représenter plus de 20 % du PIB mondial), a mené aux négociations sur le « commerce électronique » à l'OMC, expression volontairement employée pour camoufler que l'on parle ici de la « gouvernance des données ».

L'on pense communément que l'UE et les États-Unis ont des positions diamétralement opposées sur la manière dont leurs économies numériques respectives devraient fonctionner. Mais en fait, les propositions des deux blocs économiques sont remarquablement proches. À une exception près, d'importance : celle qui concerne la protection des données personnelles, puisque l'UE, en vertu de son Règlement général sur la protection des données (RGPD), s'est propulsée à la tête de la défense mondiale de la législation protégeant la vie privée.

Un élément fondamental de la stratégie a consisté à regrouper certains sujets pour lesquels les négociateurs estiment qu'ils sera possible de parvenir à un accord plus aisément, par exemple les pourriels, l'authentification ou la reconnaissance des contrats électroniques, qui servent ainsi de cheval de Troie permettant d'aboutir à ce que l'on souhaite vraiment avec les chapitres sur le commerce électronique, à savoir la garantie de la libre circulation des données par-delà les frontières et l'élimination des exigences relatives à la localisation des données, tout en interdisant strictement la divulgation des codes sources.

Même si la révolution numérique est de grande ampleur, il est important de se rappeler qu'il s'agit encore d'une innovation très récente : l'internet a célébré récemment son 30e anniversaire. Ce qui signifie que nos institutions et nos cadres politiques sont encore en train de s'adapter aux changements apportés par l'économie numérique dans nos vies, notre travail, nos loisirs.

Ceci est encore plus marqué dans les pays en développement, où quatre milliards de personnes n'ont toujours pas accès à internet. Les pays en développement sont en train de déployer à l'heure actuelle leurs premiers efforts pour lancer un programme d'industrialisation numérique qui vise à créer des activités économiques locales. Nombre de ces pays en sont encore aux premières phases de la mise sur pied d'un cadre juridique prévoyant la protection des données personnelles et garantissant que l'innovation numérique se fasse au bénéfice des travailleurs.

Verrouiller des règles mondiales à une phase aussi précoce du développement d'internet et du commerce numérique reviendrait à pérenniser le statu quo en vertu duquel la propriété et le contrôle des données seraient concentrés dans les mains d'un petit nombre de grandes sociétés, empêchant ainsi aux États de porter à son maximum le bien public qui découle de l'innovation numérique.

2 Statista (2019) *Retail e-commerce sales worldwide from 2014 to 2023 (Les ventes du commerce électronique au détail à l'échelle mondiale de 2014 à 2023)*. Consulté sur : https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

ANALYSE COMPARATIVE DES DISPOSITIONS DES ACCORDS DE LIBRE-ÉCHANGE

Nous allons, dans la présente partie, nous pencher sur quatre textes fondamentaux, à savoir l'Accord de Partenariat transpacifique global et progressiste (PTPGB), l'Accord Canada-États-Unis-Mexique (ACEUM), l'Accord de partenariat économique (APE) UE-Japon, et la Communication présentée par l'Union européenne à l'OMC (mai 2019), en vue d'en effectuer une analyse juridique comparative. Cette partie va couvrir six dispositions distinctes des chapitres sur le commerce électronique :

1. moyens d'authentification et de signature, contrats électroniques ;
2. code source ;
3. flux de données ;
4. emplacement des données ;
5. protection des données ;
6. accès à un internet ouvert.

Nous avançons dans cette partie une série d'arguments généraux concernant les enjeux et impacts potentiels à partir de l'analyse des différentes dispositions concernant le commerce électronique. Ces arguments sont les suivants :

- De manière générale, les sujets couverts par ces dispositions ne relèvent pas spécifiquement du commerce et il est donc inapproprié de les inclure dans des accords de libre-échange. Par conséquent, la position politique par défaut sur ces sujets devrait être de réglementer au moyen de la législation nationale là où cela est possible, en particulier lorsqu'une législation type existe.

- De fait, l'inclusion de chapitres spécifiques sur le numérique dans les accords commerciaux internationaux a pour but de restreindre la capacité des gouvernements nationaux de réglementer des domaines clés émergents de l'économie numérique.

- Les technologies du numérique commencent déjà à avoir des répercussions et à perturber notre économie, indépendamment de leur inclusion ou pas, et si oui dans quelle mesure, dans les accords commerciaux internationaux. Néanmoins, en verrouillant un environnement libéral sous-réglementé, ces chapitres sur le numérique vont à maints égards exacerber les risques existants de répercussions néfastes, économiques et sociales, découlant de la disruption numérique.

- À mesure que les données et les algorithmes deviennent des composantes chaque fois plus centrales de nos vies sociales et économiques, les dispositions sur le commerce numérique dans les accords commerciaux internationaux vont aussi gagner en importance.

MOYENS D'AUTHENTIFICATION, SIGNATURES ÉLECTRONIQUES ET CONTRATS ÉLECTRONIQUES

PTPGB	UE-Japon	ACEUM	Communication de l'UE à l'OMC
Article 14.6 : Authentification électronique et signatures électroniques 1. Sauf dans des circonstances autrement prévues dans son droit, une Partie ne conteste pas la validité juridique d'une signature au seul motif que la signature est sous forme électronique. 2. Aucune Partie n'adopte ni ne maintient des mesures en matière d'authentification électronique qui : (a) interdiraient aux parties à une transaction électronique de déterminer d'un commun accord les méthodes d'authentification appropriées au regard de cette transaction ; ou (b) priveraient les parties à une transaction électronique de la possibilité de démontrer aux autorités judiciaires ou administratives que leur transaction respecte toutes les exigences légales concernant l'authentification. 3. Nonobstant les dispositions du paragraphe 2, une Partie peut exiger, pour une catégorie particulière de transactions, que la méthode d'authentification réponde à certaines normes de performance ou soit certifiée par une autorité accréditée conformément à son droit. 4. Les Parties encouragent l'utilisation de l'authentification électronique interopérable.	Article 8.77 Authentification électronique et signature électronique Sauf dispositions contraires prévues par ses dispositions légales et réglementaires, une partie ne refuse pas de reconnaître la validité juridique d'une signature au seul motif qu'elle se présente sous une forme électronique. 2. Une partie n'adopte ni ne maintient des mesures régissant l'authentification électronique et la signature électronique qui : (a) interdiraient aux parties à une transaction électronique de déterminer d'un commun accord les méthodes d'authentification électroniques appropriées à leur transaction ; ou (b) priveraient les parties à des transactions électroniques de la possibilité d'établir devant des autorités judiciaires ou administratives que leurs transactions électroniques satisfont à toutes les exigences légales en ce qui concerne l'authentification électronique et la signature électronique. 3. Nonobstant le paragraphe 2, chaque partie peut exiger que, pour une catégorie donnée de transactions, la méthode d'authentification réponde à certaines normes de performance ou soit certifiée par une autorité accréditée conformément à ses dispositions légales et réglementaires.	Article 19.6 : Authentification électronique et signatures électroniques 1. Sauf dans des circonstances prévues par son droit, une Partie ne conteste pas la validité juridique d'une signature au seul motif que la signature est sous forme électronique. 2. Aucune Partie n'adopte ni ne maintient des mesures concernant l'authentification électronique et les signatures électroniques qui, selon le cas : (a) interdiraient aux parties à une transaction électronique de déterminer d'un commun accord les méthodes d'authentification ou les signatures électroniques appropriées pour cette transaction ; ou (b) priveraient les parties à une transaction électronique de la possibilité de démontrer aux autorités judiciaires ou administratives que leur transaction respecte toutes les exigences légales concernant l'authentification ou les signatures électroniques. 3. Nonobstant les dispositions du paragraphe 2, une Partie peut exiger, pour une catégorie particulière de transactions, que la signature électronique ou la méthode d'authentification réponde à certaines normes de performance ou soit certifiée par une autorité accréditée conformément à son droit. 4. Chacune des Parties encourage l'utilisation de l'authentification électronique interopérable.	2.2 Authentification électronique et signatures électroniques 1. Les Membres ne contesteront pas, dans une procédure juridique, l'effet juridique et la recevabilité en tant que preuve, d'une signature électronique au seul motif qu'elle est sous forme électronique. 2. Les Membres veilleront à ce que les parties à une transaction électronique ne soient pas empêchés : (a) de déterminer mutuellement les méthodes d'authentification électronique appropriées pour leur transaction ; (b) de pouvoir prouver aux autorités judiciaires et administratives que l'utilisation d'une authentification électronique ou d'une signature électronique dans cette transaction est conforme aux prescriptions juridiques applicables. 3. Nonobstant le paragraphe 2, les prescriptions en matière de certification d'une autorité accréditée conformément à la législation nationale ou à certaines normes de performance pourront s'appliquer à une catégorie particulière de transactions, à la méthode d'authentification ou à la signature électronique. De telles prescriptions ou normes seront objectives, transparentes et non discriminatoires et se rapporteront seulement aux caractéristiques spécifiques de la catégorie de transactions concernée. 4. Dans la mesure prévue par le droit interne, les Membres appliqueront les paragraphes 1 à 3 aux autres procédés ou moyens électroniques qui facilitent ou qui permettent les transactions électroniques, tels que les cachets électroniques, les services d'envoi recommandé électroniques ou l'authentification de sites Web.

Lorsque les personnes et les entreprises font du commerce, il est indispensable de disposer de manières permettant à la fois de valider les détails de la transaction et de s'assurer que les personnes et entreprises effectuant la transaction sont bien qui elles prétendent être. Dans ce processus, il est crucial de disposer de la technologie qui permette une authentification électronique et une signature électronique. Dans ce domaine, la bataille qui se livre oppose les entreprises, qui veulent le moins possible de lois et de réglementations spécifiant, limitant ou restreignant l'utilisation d'une authentification électronique, à l'intérêt public, qui voudrait que l'on garantisse un environnement sûr et sécurisé pour le commerce numérique.

Cette dernière disposition est particulièrement mise en avant par l'UE, qui s'est dotée dès 1999 d'une directive sur la signature électronique, mise à jour récemment par le Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques (plus connu sous le nom de Règlement eIDAS), entré en vigueur en juillet 2016. L'adoption précoce de ces réglementations et les efforts déployés par les entreprises de l'UE pour s'y conformer signifient qu'il s'agit là d'un domaine dans lequel l'UE est pionnière du point de vue technologique, et qu'elle bénéficie par conséquent d'une possibilité directe d'agir en tant que force motrice pour les entreprises en plaçant ces exigences dans les traités.

Bien que des dispositions générales sur l'authentification électronique et sur la signature électronique n'apparaissent que dans la moitié des accords commerciaux[3], chacun des quatre documents sur lesquels nous nous sommes penchés de manière détaillée comportent des clauses précises en la matière.

Dans la présente section, la profonde similitude entre les textes apparaît clairement. Ils renforcent tous un aspect central : « une Partie ne conteste pas la validité juridique d'une signature au seul motif que la signature est sous forme électronique ». Ce qui doit être lu conjointement au texte interdisant aux gouvernements d'adopter ou de maintenir des exigences qui « interdiraient aux parties à une transaction électronique de déterminer d'un commun accord les méthodes d'authentification électroniques appropriées à leur transaction » et, en cas de contestation, qui empêcheraient que ces parties puissent saisir un tribunal pour statuer sur la validité d'une signature. L'aspect primordial qui a voulu être renforcé est qu'il ne doit pas incomber au gouvernement de dire aux deux (ou plus) parties à une transaction quelle technologie, système ou modèle de mise en œuvre elles devraient utiliser. Au contraire, les accords de libre-échange stipulent qu'il revient aux parties à la transaction de déterminer quelle est la meilleure technologie d'authentification.

Le PTPGB, l'ACEUM et le texte de l'accord UE-Japon commencent tous trois avec la même précision selon laquelle leurs dispositions s'appliquent « Sauf dans des circonstances autrement prévues dans son droit ». Il est intéressant que la communication de l'UE à l'OMC ne contienne pas la même phrase, puisqu'il s'agirait vraisemblablement d'une dérogation importante qui a de toute évidence un ample soutien parmi d'autres pays, y compris de l'UE, puisqu'il fait partie du texte UE-Japon. Enfin, les quatre textes autorisent l'établissement par les gouvernements de normes de performance « pour une catégorie particulière de transactions », sans définir de quelque manière que ce soit quelles pourraient être ces catégories. La formulation de ces pouvoirs, en conjonction avec le fait qu'il n'y ait pas d'obligation de garantir un objectif légitime de politique publique, pourrait signifier que ces pouvoirs fourniraient aux gouvernements l'espace suffisant pour faire en sorte que les transactions requérant de hauts niveaux de sécurité, concernant la finance ou l'identité par exemple, seraient susceptibles de faire l'objet d'une législation. Une fois encore, le PTPGB, l'ACEUM et le texte UE-Japon prévoient spécifiquement que les gouvernements aient la possibilité d'exiger que les protocoles d'authentification soient « certifiés par une autorité accréditée conformément à son droit ». La communication de l'UE à l'OMC, quant à elle, donne beaucoup de détails sur les limites des actions du gouvernement à cet égard. Elle vise à exiger que les prescriptions soient toutes « objectives, transparentes et non discriminatoires et se rapportent seulement aux caractéristiques spécifiques de la catégorie de transactions concernée ».

Une partie du défi qui se pose au décryptage des impacts réels de ces diverses dispositions réside dans l'absence de définition de deux termes pourtant fondamentaux, à savoir « parties » et « transaction électronique ». Ainsi, bien que les parties aux accords sachent certainement de quelle manière s'appliquent ces dispositions, il est très difficile pour quiconque ne dispose pas des définitions de parvenir à un jugement définitif.

Nous pouvons, en revanche, mettre en avant quelques problèmes qui peuvent éventuellement se poser du fait que les parties ont la possibilité de décider d'un commun accord de la technologie d'authentification devant être utilisée.

- Premièrement, il existe une entente en matière d'efficacité qui veut que dans un monde où coexistent de multiples normes privées d'authentification, le manque d'interopérabilité entre les multiples systèmes et la nécessité de gérer ces multiples systèmes entraînerait un coût supplémentaire.
- Deuxièmement, les entreprises dominantes pourraient être en mesure de fixer des normes qui sont souvent trop onéreuses pour que tout le monde les observe, et ensuite pénaliser ceux

3 Wu, M. (2017). *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for Multilateral Trade System (Dispositions relatives au commerce numérique : modèles existants et enseignements à tirer pour le système commercial multilatéral).* RTA Exchange. Consulté sur : http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf

qui ne le font pas. Dans un exemple récent, Visa et Mastercard ont fait appliquer un logiciel anti-fraude à leurs réseaux de commerçants, dans le but déclaré de veiller à sécuriser le système de paiement. Cependant, la Fédération nationale des détaillants aux États-Unis a déclaré que ce système constituait une « quasi-escroquerie » et dans un recours juridique il a été affirmé que « le système est mis en place moins pour sécuriser les données liées à la carte des consommateurs que pour permettre aux sociétés émettrices des cartes de crédit d'engranger des bénéfices par le biais d'amendes et de pénalités »[4].

- Troisièmement, il existe un grave risque que la norme prônée par les entreprises ne soit pas suffisamment sûre. Comme le constate Richard Hill, il arrive souvent que les pouvoirs publics se voient obligés d'intervenir en raison d'une défaillance du marché provoqué par des « externalités associées à une sécurité insuffisante ; les coûts d'une infraction à la sécurité sont en grande mesure portés par des entités autres que la société qui a été victime de l'infraction du fait d'une sécurité inadéquate »[5].
- Quatrièmement, la protection des consommateurs fournit également de bons arguments en faveur d'une fixation des normes par les pouvoirs publics, faute de quoi les consommateurs pourraient avoir du mal à comprendre si la myriade de technologies d'authentification est réellement sécurisée.

Enfin, les accords de libre-échange ne sont pas les plus adéquats pour résoudre cette problématique. La loi type[6] proposée par la CNUDCI est une manière nettement plus efficace d'incorporer ces prescriptions au sein des cadres juridiques nationaux parce qu'elle donne aux pays la possibilité d'adapter leur législation aux nécessités et exigences locales.

4 Zetter, K. (1er novembre 2012). *Rare legal fight takes on credit card company security standard and fines* (*Rare bataille juridique contre les normes de sécurité et les amendes imposées par les sociétés émettrices de cartes de crédit*). Consulté sur : https://www.wired.com/2012/01/pci-lawsuit/

5 Hill, R. (2017). *Notes on & E-signatures and Trade (Notes sur la signature électronique et le commerce).* Our World is Not for Sale. Consulté sur : https://ourworldisnotforsale.net/2017/Hill_E-signatures.pdf

6 CNUDCI (2001) *Loi type sur les signatures électroniques et guide pour son incorporation.* Consultée sur : https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/ml-elecsign-f.pdf

CODE SOURCE

PTPGB	UE-Japon	ACEUM	Communication de l'UE à l'OMC
Article 14.17 : Code source 1. Une Partie n'exige pas le transfert de codes sources de logiciel appartenant à une personne d'une autre Partie ou l'accès à ce code, comme condition à l'importation, à la distribution, à la vente ou à l'utilisation sur son territoire de ce logiciel ou de produits dans lesquels ce logiciel est incorporé. 2. Aux fins du présent article, les logiciels visés par le paragraphe 1 sont exclusivement des logiciels de grande consommation ou des produits dans lesquels ces logiciels sont incorporés, et ne comprennent pas les logiciels associés aux infrastructures essentielles. 3. Aucune disposition du présent article n'empêche : (a) l'inclusion ou l'application de modalités se rapportant à la fourniture de codes sources dans des contrats négociés sur le plan commercial ; ou (b) une Partie d'exiger que soient effectuées sur des codes sources de logiciels certaines modifications qui sont nécessaires pour permettre à ces logiciels de se conformer à des lois ou des règlements qui ne sont pas incompatibles avec le présent accord. 4. Le présent article n'est pas interprété de manière à avoir une incidence sur les exigences se rapportant aux demandes d'enregistrement de brevets ou aux brevets délivrés, y compris sur les ordonnances prononcées par une autorité judiciaire dans le cadre de litiges en matière de brevet, sous réserve des protections contre la divulgation non autorisée prévues par le droit ou la pratique d'une Partie.	Article 8.73 : Code source 1. Une partie ne peut exiger le transfert du code source, ou l'accès à celui-ci, d'un logiciel appartenant à une personne de l'autre partie. Rien dans le présent paragraphe n'empêche l'inscription ou la mise en œuvre de modalités et conditions relatives au transfert du code source ou à l'octroi de l'accès à celui-ci dans les contrats négociés sur une base commerciale, ou le transfert volontaire du code source ou l'octroi volontaire de l'accès à celui-ci, par exemple dans le cadre de marchés publics. 2. Aucune disposition du présent article ne porte atteinte : (a) aux dispositions d'un tribunal judiciaire ou administratif ou d'une autorité en matière de concurrence visant à remédier à une violation du droit de la concurrence ; (b) aux dispositions d'un tribunal judiciaire ou administratif ou d'une autorité administrative en ce qui concerne la protection et l'application des droits de propriété intellectuelle, dans la mesure où les codes sources sont protégés par ces droits ; et (c) au droit d'une partie de prendre des mesures conformément à l'article III de l'accord sur les marchés publics. 3. Il est entendu qu'aucune disposition du présent article n'empêche une partie d'adopter ou de maintenir des mesures qui sont incompatibles avec le paragraphe 1, conformément aux articles 1.5, 8.3 et 8.65.	Article 19.16 : Code source 1. Une Partie n'exige pas le transfert du code source d'un logiciel appartenant à une personne d'une autre Partie ou d'un algorithme exprimé dans ce code source, ni l'accès à ce code ou algorithme, comme condition à l'importation, à la distribution, à la vente ou à l'utilisation sur son territoire de ce logiciel ou de produits dans lesquels ce logiciel est incorporé. 2. Ce présent article n'empêche pas un organisme de réglementation ou l'autorité judiciaire d'une Partie d'ordonner à une personne d'une autre partie de conserver le code source d'un logiciel ou un algorithme exprimé dans ce code source, et de donner accès à ce code ou algorithme à cet organisme de réglementation en vue d'une enquête, d'une inspection, d'un examen, d'une action coercitive ou d'une procédure judiciaire spécifique, sous réserve des protection contre la divulgation non autorisée.	2.6 Transfert du code source ou accès au code source 1. Les Membres n'exigeront pas le transfert du code source du logiciel appartenant à une personne physique ou morale d'autres Membres ni l'accès à ce code source. 2. Il est entendu que : (a) les exceptions générales, les exceptions concernant la sécurité ainsi que les exceptions prévues au paragraphe 2 de l'Annexe sur les services financiers de l'AGCS s'appliquent aux mesures adoptées ou maintenues dans le cadre d'une procédure de certification ; (b) le paragraphe 1 ne s'applique pas au transfert volontaire du code source ou à l'octroi de l'accès au code source sur une base commerciale par une personne physique ou morale, par exemple dans le cadre d'une transaction concernant les marchés publics ou d'un contrat librement négocié. 3. Le paragraphe 1 est sans préjudice : (a) des prescriptions imposées par un tribunal judiciaire ou administratif ou par une autorité de surveillance de la concurrence en vue de remédier à une violation des lois sur la concurrence ; (b) de la protection et du respect des droits de propriété intellectuelle ; (c) du droit de prendre des mesures ou de ne pas divulguer des renseignements considérés comme étant nécessaires à la protection des intérêts essentiels de sécurité relatifs aux achats d'armes, de munitions ou de matériel de guerre, ou aux achats indispensables à la sécurité nationale ou aux fins de la défense nationale.

Le code source est l'ensemble d'instructions ou de règles suivies par un programme informatique, écrit de manière à être compris par les êtres humains. Il est utilisé pour tout, à commencer par les logiciels de nos téléphones, les appareils intelligents et les voitures, et bien sûr les algorithmes qui sont utilisés pour faire le tri des informations que nous recherchons sur internet, par exemple les moteurs de recherche de Google ou le fil d'actualité de Facebook, ainsi que les protocoles qui gèrent nos feux tricolores et les infrastructures nationales d'électricité.

Le code source est déjà inclus, partout dans le monde, dans les protections relatives à la propriété intellectuelle et aux secrets commerciaux. Lorsqu'il relève de la protection d'un brevet, il est déjà illégal pour une per-

sonne, une entreprise ou un gouvernement d'accéder à un code source, de le partager ou de le copier, sans motivation juridique. La protection du brevet exige souvent à la partie demandant la protection de communiquer le code au bureau des brevets. Ceux qui ne souhaitent pas le faire peuvent toutefois recourir à la protection des secrets commerciaux pour faire en sorte que leurs codes ne fassent pas indûment l'objet d'un accès ou d'un partage. Les secrets commerciaux sont protégés par l'article 39 de l'accord de l'OMC sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC). Par conséquent, la disposition qui nous occupe dans les chapitres sur le commerce numérique s'attache uniquement à la faculté des gouvernements et de leurs agents, tribunaux ou entités de réglementation, de prendre des mesures qui exigeraient le transfert du code source ou l'accès à celui-ci comme condition pour être autorisé à avoir des activités commerciales dans un pays donné.

Il est important de souligner qu'il existe de nombreuses raisons légitimes pour lesquelles un gouvernement peut exiger d'une entreprise qu'elle partage son code source. Des exemples contemporains portent sur des gouvernements qui l'exigent dans le cadre d'une affaire judiciaire spécifique, tel un différend concernant la propriété intellectuelle. Mais il peut s'agir aussi de motifs plus généraux, par exemple la nécessité d'assurer la stabilité économique, ou la tenue d'enquêtes sur de possibles erreurs. Voici quelques exemples de cas dans lesquels les gouvernements demandent les codes sources légalement, mais qui pourraient ne pas être autorisés dans le cadre des accords de libre-échange convenus ou proposés[7].

- Certains régulateurs financiers, tels que les États-Unis, exigent que les sociétés qui utilisent des algorithmes aux fins d'arbitrages de haute fréquence communiquent leur code source de manière à ce que les régulateurs soient en mesure de « réviser le code, les données de formation et les formules propriétaires » afin de comprendre ce qui aurait provoqué des krach éclair[8] en bourse et de les prévenir à l'avenir[9].
- Une grande partie des jeux d'argent et de hasard passe désormais par le biais de machines électroniques, d'applications et de sites Web où les probabilités de gains sont déterminées par voie logicielle. Les organismes régulateurs des jeux contrôlent par conséquent le code source qui gère les machines électroniques de jeux d'argent et de hasard pour vérifier que la programmation des probabilités de gains est juste[10].
- Un grand nombre de véhicules du constructeur Toyota ont été impliqués dans des accidents suspects ayant entraîné la mort. Toyota s'est vue obligée de remettre son code source aux organismes de régulation, qui ont recruté la NASA pour effectuer l'analyse des données. Celle-ci n'a pas trouvé de preuve tangible, mais suffisamment d'éléments pour obliger l'entreprise à donner son code source aux consultants informatiques des victimes qui, eux, ont pu déterminer l'origine du problème[11].

Le recours au transfert de technologie pour aider à combler le fossé numérique a été une attente légitime de certains secteurs dans nombre de pays[12], même si les États-Unis le voient comme une entrave au commerce[13]. À mesure qu'augmente le nombre de produits et de services gérés par un code source, l'interdiction de l'obligation de partager le code source, comme condition pour accéder à un marché en vertu de l'accord de commerce, rendrait illégal tout transfert de technologie impliquant un code source.

Bien qu'il existe des divergences prononcées entre les quatre textes de traités que nous avons analysés, l'on s'entend généralement sur l'essence de ce qui doit être couvert, à savoir : « Une Partie n'exige pas le transfert de codes sources de logiciel appartenant à une personne d'une autre Partie ». Seul l'ACEUM ajoute à cela en incluant « un algorithme exprimé dans ce code source » dans ce qui est couvert par ladite disposition. Le PTPGB et l'ACEUM stipulent explicitement ce que les autres textes semblent présupposer, à savoir qu'une partie ne peut exiger le partage du code source ou l'accès à celui-ci « comme condition à l'importation, à la distribution, à la vente ou à l'utilisation sur son territoire de ce logiciel ou de produits dans lesquels ce logiciel est incorporé ».

L'extension de l'exclusion aux algorithmes dans l'ACEUM pose un nouveau défi, plus grave si on le compare aux dispositions déjà problématiques en soi concernant le code source. Un algorithme diffère du code source dans le sens où il décrit le fondement logique que doit

7 Smith, SR. (10 décembre 2017) *Some preliminary implications of WTO source code proposal (Aperçu des premières implications de la proposition sur le code source à l'OMC*). Third World Network Briefings. Consulté sur : https://www.twn.my/MC11/briefings/BP4.pdf

8 Un krach éclair est un événement survenant dans les marchés de titres électroniques, lorsque le retrait d'ordres de bourse amplifie rapidement une chute des cours. Il en résulte apparemment des cessions rapides d'actifs, survenant en l'espace de quelques minutes et se traduisant par des cours qui chutent de manière spectaculaire.

9 *Rieke, A. Bogen, M. & Robinson, D. (2018) Public Scrutiny of Automated Decisions: Early lesson and Emerging Methods (Examen public de décisions automatisées : un premier enseignement et des méthodes émergentes). Upturn and Omidyar Network.* Consulté sur : https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf

10 *Gambling Commission (2018). Testing strategy for compliance with remote gambling and software technical standards* (Essais de stratégie de conformité pour les normes techniques de logiciels et les jeux de hasard et d'argent à distance). Consulté sur : http://www.gamblingcommission.gov.uk/pdf/Testing-strategy-for-compliance-with-remote-gambling-and-software-technical-standards.pdf

11 Safety Research & Strategies Inc. (7 novembre 2013) *Toyota Unintended Acceleration and the big bowl of Spaghetti code* (*L'accélération non intentionnelle chez Toyota et la platée de nouilles des codes sources*). Consulté sur : http://www.safetyresearch.net/blog/articles/toyota-unintended-acceleration-and-big-bowl-%E2%80%9Cspaghetti%E2%80%9D-code

12 Smith, SR. (10 décembre 2017) S*ome preliminary implications of WTO source code proposal* (*Aperçu des premières implications de la proposition sur le code source à l'OMC*). Third World Network Briefings. Consulté sur : https://www.twn.my/MC11/briefings/BP4.pdf p.4

13 Fefer, R. (29 mars 2019) *Digital Trade (Commerce numérique).* Congressional Research Service. Consulté sur : https://fas.org/sgp/crs/misc/IF10770.pdf

suivre un programme informatique. Un algorithme peut être compris comme une recette qui fait intervenir une série d'étapes séquentielles comportant des options et des points de décision, alors que le code source est le langage et la forme dans lesquels ces instructions sont rédigées par des personnes pour être ensuite interprétées par des ordinateurs. Mais au cœur de l'algorithme, en dernière instance, se trouve une idée, laquelle n'est pas protégée en tant que telle de manière spécifique par les régimes existants de propriété intellectuelle. L'ADPIC avait déjà permis aux entreprises de commencer à utiliser la protection des secrets commerciaux pour leurs algorithmes. La proposition des États-Unis va bien au-delà puisqu'elle étend les protections déjà problématiques du code source aux algorithmes eux-mêmes.

L'essentiel des sections sur le code source concernent les situations dans lesquelles il est possible de contourner la prohibition convenue du partage du code source. L'évolution des exceptions est un parfait exemple des défis que comporte le fait de convenir d'un texte sur des questions qui continuent d'évoluer rapidement et pour lesquelles certains signataires pourraient ne pas prévoir toutes les répercussions possibles. L'accord entre le Japon et la Mongolie, le premier à s'être doté d'une telle disposition, n'avait une exception que pour des infrastructures essentielles. Lors de la conclusion du PTPGB les parties se sont rendu compte que ne déterminer qu'une liste si étroite reviendrait à saper le fonctionnement même du droit des brevets de manière générale, puisque celui-ci exige que le code soit remis pour obtenir le statut de monopole protégé.

C'est pourquoi les rédacteurs du PTPGB ont étendu les dérogations pour y inclure le droit des brevets. L'ACS à son tour a étendu l'exception pour y inclure les objectifs légitimes de politique publique (y compris le droit de la concurrence) tout en sachant que les Parties, au long de l'histoire, ont trouvé que la dérogation était difficile à appliquer en raison de l'étroite interprétation en jurisprudence de ce qu'est un objectif légitime de politique publique[14]. On trouve dans la Communication de l'UE à l'OMC une liste de dérogations encore plus spécifique, qui inclut le droit de la concurrence, la propriété intellectuelle et des considérations de sécurité nationale. Enfin, l'ACEUM a quant à lui opté pour une tout autre voie en ne tentant plus de dresser une liste exhaustive de domaines dans lesquels il serait possible d'exiger l'accès à un code source, choisissant plutôt de se concentrer sur les entités qui peuvent légitimement demander ces données, et dans quelles circonstances. Dans le libellé choisi par l'ACEUM, l'exigence de partager un code source peut être permise tant qu'elle est émise par « un organisme de réglementation ou une autorité judiciaire » en vue « d'une enquête, d'une inspection, d'un examen, d'une action coercitive ou d'une procédure judiciaire ». L'ajout du mot « spécifique » peut être vu comme une protection contre des exigences génériques imposées par des parties, dans le sens où l'on ne peut accéder au code source que dans des cas spécifiques, une fois que l'État a entamé une forme de procédure officielle.

Un autre problème grave identifié dans l'ALE UE-Japon ainsi que dans la Communication de l'UE à l'OMC est que même si ces textes permettent aux gouvernements d'exiger la communication des codes sources en vue de remédier à une infraction au droit de la concurrence, on peut se demander si le libellé inclurait la communication du code en vue de prouver qu'une infraction a eu lieu. Il s'agit pourtant pratiquement d'une condition préalable pour établir la nécessité d'un recours. L'on peut trouver un exemple récent dans l'industrie automobile, lorsque le logiciel frauduleux de contrôle des émissions chez Volkswagen n'a été confirmé que lorsque des chercheurs non étatiques furent en mesure d'analyser le code source – ce qui pourrait ne plus être possible à l'avenir.

Il est normal que les dérogations prévues aux accords évoluent, ce qui montre bien le problème que pose la volonté de verrouiller des règles spécifiques dans le détail avant de comprendre pleinement ce dont on a besoin et quelle pourrait être l'envergure du champ dérogatoire au final. Bien qu'il apparaisse clairement que les dérogations sont mieux rédigées dans les accords ratifiés plus récemment et dans ceux qui sont proposés à l'heure actuelle, tels que l'ACEUM ou la Communication de l'UE à l'OMC, elles n'évoquent malgré tout pas certains cas importants dans lesquels il conviendrait de procéder au partage du code source. Comme illustré par les exemples cités plus haut, le fait de ne pas divulguer un code source pose des problèmes qui vont au-delà des champs étroits de la concurrence, de la propriété intellectuelle et de la sécurité nationale. L'ACEUM reconnaît cet état de fait, mais le fait qu'il soit axé sur « l'organisme de réglementation » signifie que dans des cas importants il pourrait ne pas être possible de partager le code source avec des avocats spécialisés ou des experts technologiques qui sont pourtant souvent essentiels pour déterminer s'il y a lieu de poursuivre et de demander réparation. Permettre que la non-divulgation à ce type d'acteurs devienne la norme rendrait bien plus difficile de surveiller la performance et de faire en sorte que le code source des entreprises soit en conformité. Même si les libellés finissaient par devenir parfaits, le problème demeurerait pour les accords déjà conclus puisque les textes ne prévoient pas de mise à jour automatique à mesure que des problèmes sont identifiés et que la rédaction s'améliore.

La proposition centrée sur le code source va dans le sens de la stratégie entrepreneuriale en vertu de laquelle chaque entreprise s'efforce de garder son code source secret afin de maximiser son bénéfice. Ce n'est en revanche pas forcément la meilleure manière d'assurer notre sécurité à tous. Le Département de la défense des États-Unis préfère travailler avec des logiciels libres parce que « le fait que les codes sources soient dis-

14 Organisation mondiale du commerce. *Renseignements techniques sur les obstacles techniques au commerce.* Consulté sur : https://www.wto.org/french/tratop_f/tbt_f/tbt_info_f.htm

ponibles au public aide considérablement les avocats de la défense … et améliore la fiabilité et la sécurité ». Ce raisonnement montre à quel point nous devons être prudents avant d'accepter la notion que le code source, et l'algorithme qui lui est relié, devraient rester secrets – en particulier parce que les domaines qui seront régis par de tels codes sont en expansion constante en raison de la numérisation et de l'automation. En fin de compte, comme l'a bien indiqué l'Open Rights Group, « ces clauses pourraient être utilisées pour contester tout marché public dont on suspecterait qu'il avantage les logiciels libres »[15].

Le fait d'étendre l'interdiction de demander le code source au-delà de ce qui est déjà prévu dans les protections des brevets et du secret commercial représente une attaque éhontée à la capacité des pouvoirs publics de veiller à ce que les logiciels, et la pléthore d'applications en découlant, nous gardent ainsi que nos données en sécurité, protégeant sûreté et vie privée[16]. C'est en outre une attaque malavisée qui ne tient pas compte des intérêts géopolitiques occidentaux sur le long terme. En effet, si la première intention du rédacteur était d'empêcher un pays de demander à voir un code propriétaire d'un des géants du numérique qui se trouvent être aux États-Unis à l'heure actuelle, la disposition empêchera également les gouvernements des États-Unis ou de l'UE de demander à voir un code chinois ou russe.

FLUX DE DONNÉES TRANSFRONTIÈRES

PTPGB	UE-Japon	ACEUM	Communication de l'UE à l'OMC
Article 14.11 : Transfert transfrontières de renseignements par voie électronique 1. Les Parties reconnaissent que chacune des Parties peut avoir ses propres exigences réglementaires concernant le transfert de renseignements par voie électronique. 2. Chacune des Parties autorise le transfert transfrontières de renseignements par voie électronique, y compris les renseignements personnels, lorsque cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée. 3. Aucune disposition du présent article n'empêche une Partie d'adopter ou de maintenir, en vue de réaliser un objectif légitime de politique publique, des mesures qui sont incompatibles avec le paragraphe 2, à condition que ces mesures : (a) d'une part, ne soient pas appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable, soit une restriction déguisée au commerce ; et (b) d'autre part, n'imposent pas de restrictions sur les transferts de renseignements qui soient plus importantes que celles qui sont nécessaires pour atteindre cet objectif.	Article 8.81 Libre circulation des données Les parties réexaminent, dans un délai de trois ans à compter de la date d'entrée en vigueur du présent accord, la nécessité d'incorporer des dispositions concernant la libre circulation des données dans le présent accord.	Article 19.11 : Transfert transfrontières de renseignements par voie électronique 1. Aucune Partie n'interdit ni ne limite le transfert transfrontières de renseignements, y compris de renseignements personnels, par voie électronique si cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée. 2. Le présent article n'empêche pas une Partie d'adopter ou de maintenir, en vue de réaliser un objectif légitime de politique publique, une mesure qui est incompatible avec le paragraphe 1, à condition que cette mesure : (a) d'une part, ne soit pas appliquée de façon à constituer un moyen de discrimination arbitraire ou injustifiable ou une restriction déguisée au commerce ; (b) d'autre part, n'impose pas de restrictions sur les transferts de renseignements qui soient plus importantes que celles qui sont nécessaires pour atteindre cet objectif.	2.7 Flux de données transfrontières 1. Les Membres s'engagent à assurer le flux de données transfrontières afin de faciliter le commerce dans l'économie numérique.

15 Ruiz, J. (14 mars 2019) US red lines for digital trade with the UK cause alarm (Les limites infranchissables pour les États-Unis en matière de commerce numérique, alarmantes pour le Royaume-Uni). Consulté sur : https://www.openrightsgroup.org/blog/2019/us-red-lines-for-digital-trade-with-the-uk-cause-alarm
16 Knowledge Ecology International. (29 décembre 2015) KEI statement on TPP for the January 12, 2016 hearing of the United States International Trade Commission (Déclaration de KEI pour l'audition du 12 janvier 2016 de la Commission du commerce international des États-Unis). Consulté sur : https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf

Avec la croissance de l'économie numérique et la dépendance accrue des secteurs envers les données en tant qu'intrant essentiel, pratiquement toutes les entreprises, en particulier les grandes sociétés multinationales, ont besoin de faire circuler aisément les données par-delà les frontières nationales, ce qui devient une exigence de base de l'industrie[17]. La concentration d'ensembles volumineux de données provenant de multiples pays a le potentiel d'aider à relever certains des principaux défis qui se posent au monde, ainsi que de stimuler les échanges internationaux et d'améliorer notre santé. Un cadre de l'OCDE soulignait que les flux de données transfrontières « jouent un rôle déterminant dans les échanges aujourd'hui, à tel point qu'il est difficile de se représenter clairement leur omniprésence »[18]. Si ceci est probablement vrai, et que les flux de données devraient être permis dès que possible, cela n'est pas la même chose que d'exiger que toutes les formes de données, en particulier les données personnelles et les plus sensibles, puissent librement traverser les frontières sans la moindre restriction ni contrôle ou surveillance.

Un aspect particulièrement intéressant des dispositions sur les flux de données transfrontières est l'absence de clauses communes à l'ensemble des quatre textes que nous analysons ici, ce qui traduit bien les profonds désaccords en la matière entre les parties principales. Il existe en revanche quelques traits communs dans les deux textes en rapport avec les États-Unis et d'autres part dans les deux textes en rapport avec l'UE. C'est là le reflet des différents points de vue existant aux États-Unis et dans l'UE au sujet des flux de données transfrontières.

Dans l'accord entre l'UE et le Japon, aucune disposition ne porte sur la libre circulation des flux de données ; seul un engagement apparaît, celui de se repencher sur la question au bout de trois ans.

Tant le PTPGB que l'ACEUM s'attachent à faire de la libre circulation des données la position par défaut puisque tous deux exigent de chacune des parties qu'elle « autorise le transfert transfrontières de renseignements par voie électronique, y compris les renseignements personnels, lorsque cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée ». Un point intéressant est que le PTPGB encadre cette obligation par une affirmation positive, que « chacune des parties autorise » alors que l'ACEUM dit « aucune partie n'interdit ». Bien que tant le PTPGB que l'ACEUM autorisent aux parties d'adopter des mesures pour restreindre la libre circulation des données lorsque cette restriction permet de « réaliser un objectif légitime de politique publique », cette disposition a rarement donné aux pays la liberté politique qu'un profane pourrait induire de la formulation. En effet, l'adjectif « légitime » a été interprété, dans un différend au sein de l'OMC, comme signifiant une solution politique communément admise[19], tout en considérant que seuls sont acceptables à cet effet les politiques de la santé, de l'environnement et de la vie privée. Ce qui signifie que les approches novatrices dans certains secteurs, notamment ceux qui traversent une transformation numérique, pourraient être jugées illégitimes même si elles concernent la santé, l'environnement ou la vie privée qui sont pourtant des objectifs politiques valables. Ceci est particulièrement vrai en combinaison avec le test de nécessité sur les politiques qui « n'imposent pas de restrictions sur les transferts de renseignements qui soient plus importantes que celles qui sont nécessaires pour atteindre cet objectif ». Ainsi, sur 44 tentatives d'utiliser cette méthode pour déroger à une disposition particulière, une seulement a abouti.

Probablement plus intéressant encore, le fait que la Communication de l'UE à l'OMC comporte un engagement nettement plus faible envers les flux de données transfrontières : elle déclare que les « Membres s'engagent à assurer le flux de données transfrontières afin de faciliter le commerce dans l'économie numérique ». Le critère de « s'engager à assurer » les flux transfrontières confère aux parties une bien plus grande liberté de restreindre les flux transfrontières que le texte de l'ACEUM qui dit « Aucune Partie n'interdit ni ne limite le transfert transfrontières de renseignements ». Puisque le libellé de l'UE accorde une plus grande flexibilité aux parties, il n'est pas nécessaire d'équilibrer une interdiction stricte par une série de dérogations complexes.

Il est intéressant que l'UE considère, de toute évidence, que ceci est compatible avec le Règlement général sur la protection des données (RGPD), qui est le régime de protection des données le plus sévère au monde, bien qu'il soit loin d'atteindre la perfection. Ainsi, Wilbur Ross, Secrétaire au commerce des États-Unis, a ouvertement décrit le RGPD comme un obstacle non nécessaire au commerce[20].

En vertu du RGPD, les entreprises et le secteur public se trouvant dans l'UE (ainsi que ceux situés en dehors de l'UE mais traitant des données de ressortissants de l'UE) doivent prendre des mesures en vue de protéger les données personnelles, ce qui enfreint presque certainement les dispositions du PTPGB et de l'ACEUM, puisque cela représente une restriction, à tout le moins, du transfert transfrontières de renseignements, même si ces renseignements sont à caractère personnel et trop sensibles. Ce qui revient à dire que l'UE ne serait jamais en mesure de souscrire à des dispositions telles que celles de l'ACEUM ou du PTPGB.

17 The Software Alliance (2017) *Cross-Border Data Flows (Flux transfrontières de données).* Consulté sur : https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

18 Gonzalez, JL. (3 juin 2019) *Pas de panique ! Le guide du voyageur à la découverte des flux transfrontières de données.* OCDE. Consulté sur : https://www.oecd.org/fr/echanges/guide-flux-transfrontieres-donnees/

19 Organisation mondiale du commerce. *Canada –Protection conférée par un brevet pour les produits pharmaceutiques.* Consulté sur : https://www.wto.org/french/tratop_f/dispu_f/cases_f/ds114_f.htm

20 Ross, W. (18 mai 2018) *EU data privacy laws are likely to create barriers to trade (Législation de l'UE sur les données personnelles susceptible de créer des entraves au commerce).* Consulté sur : https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c

Il sera intéressant de voir de quelle manière le Royaume-Uni entend négocier ses nouveaux accords de commerce compte tenu de la pression qui s'exercera pour qu'il accepte les conditions des États-Unis afin qu'un accord commercial soit rapidement conclu, tout en ayant intégré dans son corpus le RGPD de l'UE.

EMPLACEMENT DES DONNÉES

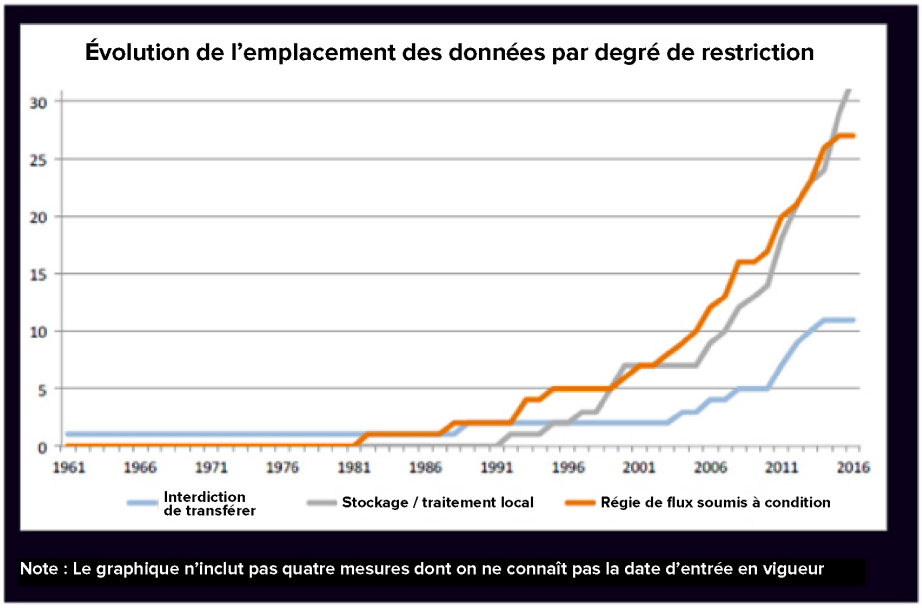
PTPGB	UE-Japon	ACEUM	Communication de l'UE à l'OMC
Article 14.13 : Emplacement des installations informatiques 1. Les Parties reconnaissent que chacune des Parties peut avoir ses propres exigences réglementaires concernant l'utilisation des installations informatiques, y compris des exigences qui visent à garantir la sécurité et le caractère confidentiel des communications. 2. Une Partie n'exige pas d'une personne visée qu'elle utilise ou situe des installations informatiques sur son territoire comme condition à l'exercice des activités commerciales sur ce territoire. 3. Aucune disposition du présent article n'empêche une Partie d'adopter ou de maintenir, en vue de réaliser un objectif légitime de politique publique, des mesures qui sont incompatibles avec le paragraphe 2, à condition que ces mesures : (a) d'une part, ne soient pas appliquées de façon à constituer soit un moyen de discrimination arbitraire ou injustifiable, soit une restriction déguisée au commerce ; et (b) d'autre part, n'imposent pas de restrictions sur l'utilisation ou l'emplacement des installations informatiques qui soient plus importantes que celles qui sont nécessaires pour atteindre cet objectif.		Article 19.12 : Emplacement des installations informatiques Une Partie n'exige pas d'une personne visée qu'elle utilise ou situe des installations informatiques sur le territoire de cette Partie comme condition à l'exercice des activités commerciales sur ce territoire.	2.7 Flux de données transfrontières 1. Les Membres s'engagent à assurer les flux de données transfrontières afin de faciliter le commerce dans l'économie numérique. À cette fin, les flux de données transfrontières ne seront pas limités par : (a) l'obligation d'utiliser des installations informatiques ou des éléments de réseau se trouvant sur le territoire du Membre aux fins du traitement des données, y compris en imposant l'utilisation d'installations informatiques ou d'éléments de réseau qui sont certifiés ou approuvés sur le territoire dudit Membre ; (b) l'obligation de localiser les données sur le territoire du Membre aux fins de leur stockage ou de leur traitement ; (c) l'interdiction de stocker ou de traiter les données sur le territoire d'autres Membres ; (d) l'obligation de subordonner le transfert transfrontières de données à l'utilisation d'installations informatiques ou d'éléments de réseau se trouvant sur le territoire du Membre ou aux prescriptions en matière de localisation sur le territoire dudit Membre.

Les obligations en matière d'emplacement des données, c'est-à-dire du lieu où les entreprises doivent situer, dans un pays donné, une partie ou la totalité de leur équipement chargé de la collecte, des analyses et des transferts de données à l'international, font désormais l'objet d'un important débat géopolitique. À un des extrêmes se trouve la Russie, qui stipule que toutes les données personnelles recueillies de tous les ressortissants russes doivent être stockées et traitées au niveau national[21]. D'autres pays adoptent une approche plus ciblée qui se concentre sur certaines catégories de données ayant une importance stratégique ou particulièrement sensibles, comme le Nigéria, qui exige que les données gouvernementales soient stockées au niveau du pays, et l'Australie, qui permet uniquement que les données relatives à la santé quittent le pays, et seulement dans certaines circonstances très précises (ce qui de fait impose le stockage local des données). À l'autre extrême, les grandes sociétés mondiales du secteur, qui veulent une interdiction de ces exigences relatives à l'emplacement car elles les voient comme une entrave qui « limite l'accès aux services mondiaux » en raison du coût supplémentaire que cela suppose pour les entreprises, et les milieux libre-échangistes mondiaux les voient comme « le principal instrument du protectionnisme de l'ère de l'information »[22].

21 Bowman, C (6 janvier 2017) *Data Localization Laws: an emerging global trend (Lois sur l'emplacement des données: une tendance mondiale émergente).* Consulté sur : http://jurist.org/hotline/2017/01/data-localization-laws-an-emerging-global-trend.php

22 Chander, A. (9 octobre 2018) *The coming north American digital trade zone (La future zone de commerce numérique nord-américaine).* Council on Foreign Relations. Consulté sur : https://www.cfr.org/blog/coming-north-american-digital-trade-zone

Bien que les obligations en matière d'emplacement aient connu une croissance progressive depuis les années 1990, comme illustré dans le graphique ci-dessous, le PTP, prédécesseur du PTPGB, a été le premier accord de libre-échange à contenir une telle disposition spécifique limitant sévèrement les situations dans lesquelles un emplacement des données est autorisé.



Source : ECIPE, Base de données des estimations du commerce numérique

S'il n'existe pas de disposition commune dans les quatre traités en examen, c'est parce que l'accord UE-Japon ne comporte pas de clause spécifique en la matière. Le PTPGB, l'ACEUM et la Communication de l'UE à l'OMC conviennent toutefois qu'il ne devrait jamais être permis qu'un pays exige que les données soient localisées sur son territoire en tant que condition préalable pour accéder au marché dudit pays. C'est là une clause très clairement libellée : « une Partie n'exige pas d'une personne visée qu'elle utilise ou situe des installations informatiques sur le territoire de cette Partie comme condition à l'exercice des activités commerciales sur ce territoire ».

Cependant, les trois textes diffèrent grandement quant à la description des circonstances dans lesquelles les pays peuvent appliquer des obligations en matière d'emplacement des données, c'est-à-dire, techniquement, des dérogations. Dans les faits, l'ACEUM interdit dans tous les cas des critères de localisation des données, même pour les données financières (en vertu d'un ensemble de règles différent qui figure dans le chapitre relatif aux services financiers) ou les données sanitaires, deux cas pour lesquels il aurait pu exister une forte justification à obliger au stockage local.

Le PTPGB contient bien une dérogation qui à première vue semble permettre aux parties une ample marge de manœuvre : ce que dit le texte sur les exigences relatives à l'emplacement des données qui poursuivent un « objectif légitime de politique publique », incluant la santé, l'environnement et la vie privé. Cependant, ce vaste ensemble d'objectifs est en fait précisé et limité par l'obligation que la restriction ne soit pas plus grande que nécessaire. De manière générale, ceci a donné lieu à des interprétations étroites dans la jurisprudence, et l'expérience concrète de tenter de recourir à la dérogation nous dit que celle-ci ne donne pas l'espace politique dont certains pays voudraient disposer dans cet important domaine.

Il est possible de faire valoir des arguments convaincants à la fois pour et contre l'imposition d'exigences relatives à l'emplacement des données. Outre les arguments avancés par les Big Tech, certains groupes de défense des droits numériques œuvrent aussi en vue de limiter les exigences relatives à l'emplacement des données. Les groupes de défense des droits numériques craignent que ces exigences soient utilisées pour « faciliter les restrictions à la liberté d'expression par les gouvernements nationaux »[23] lorsqu'ils essayent d'obliger les sociétés numériques à conserver les données au niveau local, là où il sera facile d'y accéder, contrairement aux données stockées dans un pays tiers. En outre, les entreprises ayant leur siège dans certains pays s'opposent à y conserver leurs données en raison de la piètre qualité de l'infrastructure numérique locale[24].

Néanmoins, les arguments en faveur de cette localisation des données sont eux aussi assez convaincants. Nombreux sont ceux qui énoncent des préoccupations concernant le volume de données détenues à notre sujet par les géants du secteur, et précisent que les exigences en matière de localisation pourraient contribuer au développement d'une infrastructure de données bien plus décentralisée. Ce qui gagne en importance d'ailleurs si l'on tient compte de la volonté croissante des pays de développer leurs propres capacités nationales d'IA, puisque les données sont la ressource fondamentale pour accroître les capacités de toute technologie en lien avec l'IA. Il existe en outre pléthore d'objectifs de politique publique qui pourraient exiger de manière tout à fait légitime que les données soient localisées, par exemple la surveillance des réglementations du secteur financier, ou d'autres secteurs, et les objectifs de sécurité nationale.

23 Ruiz, J. (23 novembre 2018) *Open Rights Group submission to UK consultation on a new free trade agreement with the United States of America (Communication du Open Rights Group dans le cadre de la consultation britannique sur un nouvel accord de libre-échange avec les États-Unis)*. Consulté sur : https://www.openrightsgroup.org/assets/files/pdfs/submissions/org_fta_consultation_usa.pdf

24 Chander, A. & Uyen, P. (13 mars 2015). *Data Nationalism (Nationalisme des données)*. Emory Law Journal, Vol. 64, No. 3, 2015. Disponible auprès du SSRN : https://ssrn.com/abstract=2577947

Nous ne cherchons pas ici à parvenir à trancher définitivement et dire si la localisation des données est une bonne ou une mauvaise chose, mais plutôt à souligner la complexité du débat en cours. Il est difficile de concilier des facteurs tels que les exigences de localisation (qui pourraient entraîner que des grandes sociétés du secteur se retirent d'un pays, ce qui aurait des répercussions pour les populations et entreprises locales qui ne seraient plus en mesure d'utiliser leurs services) et, d'autre part, le fait que l'absence de ces géants du secteur pourrait être la seule manière de garantir l'émergence d'options alternatives nationales, qu'il est presque impossible de développer dans un marché entièrement ouvert et libre. Ainsi, notre conclusion principale pour la présente partie est que ce domaine n'est pas approprié pour les négociations commerciales. L'Inde a assumé à cet égard un rôle de premier plan, et son souhait de conserver le droit d'appliquer des exigences relatives à la localisation des données est l'une des raisons de son rejet récent du chapitre sur le commerce électronique dans l'Accord de partenariat économique régional global (RCEP)[25].

25 Raghavan, TCA. (11 octobre 2019) *India rejects RCEP e-commerce chapter (L'Inde rejette le chapitre du RCEP sur le commerce électronique).* The Hindu. Consulté sur : https://www.thehindu.com/business/india-rejects-rcep-e-commerce-chapter/article29659912.ece

PROTECTION DES DONNÉES

PTPGB	EU-Japan	ACEUM	Communication de l'UE à l'OMC
Article 14.8 : Protection des renseignements personnels 1. Les Parties reconnaissent les avantages économiques et sociaux qu'apporte la protection des renseignements personnels des usagers du commerce électronique et la contribution que cette protection entraîne en renforçant la confiance des consommateurs à l'égard du commerce électronique. 2. À cette fin, chacune des Parties adopte ou maintient un cadre juridique assurant la protection des renseignements personnels des usagers du commerce électronique. Lors de l'élaboration de son cadre juridique visant la protection des renseignements personnels, chacune des Parties devrait prendre en compte les principes et les lignes directrices énoncés par les organismes internationaux concernés. 3. Chacune des Parties s'efforce d'adopter des pratiques non discriminatoires pour protéger les usagers du commerce électronique à l'encontre des atteintes à la protection des renseignements personnels qui se produisent dans le cadre de sa compétence. 4. Chacune des Parties devrait publier de l'information sur la protection des renseignements personnels qu'elle accorde aux usagers du commerce électronique, y compris sur la manière selon laquelle : (a) les individus peuvent exercer des recours ; et (b) les établissements d'affaires peuvent se conformer à toutes les exigences juridiques. 5. Reconnaissant que les Parties peuvent adopter différentes approches juridiques en matière de protection des renseignements personnels, chacune des Parties devrait encourager l'élaboration de mécanismes favorisant une compatibilité entre les différents régimes. De tels mécanismes peuvent comprendre la reconnaissance des résultats relatifs à la réglementation, qu'elle soit accordée de façon autonome ou par arrangement mutuel, ou des cadres internationaux plus larges. À cette fin, les Parties s'efforcent d'échanger de l'information sur de tels mécanismes appliqués dans leur pays et d'explorer des façons d'élargir ces mécanismes ou d'autres arrangements adéquats pour favoriser leur compatibilité.	Article 8.78 Protection des consommateurs 3. Les parties reconnaissent l'importance d'adopter et de maintenir des mesures, en conformité avec leurs dispositions légales et réglementaires respectives, afin de protéger les données à caractère personnel des utilisateurs du commerce électronique.	Article 19.8 : Protection des renseignements personnels 1. Les Parties reconnaissent les avantages économiques et sociaux qu'apporte la protection des renseignements personnels des usagers du commerce numérique et la contribution que cette protection entraîne en renforçant la confiance des consommateurs à l'égard du commerce numérique. 2. À cette fin, chacune des Parties adopte ou maintient un cadre juridique assurant la protection des renseignements personnels des usagers du commerce numérique. Lors de l'élaboration de ce cadre juridique, chacune des Parties devrait tenir compte des principes et lignes directrices des organismes internationaux compétents, tels que le cadre de la protection de la vie privée de l'APEC et la Recommandation du Conseil de l'OCDE concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (2013). 3. Les Parties reconnaissent, conformément au paragraphe 2, que ces grands principes incluent : la limitation en matière de collecte, le choix, la qualité des données, la finalité de la collecte des données, la limitation de l'utilisation, les garanties de sécurité, la transparence, la participation individuelle et la responsabilité. Les Parties reconnaissent également l'importance d'assurer le respect des mesures de protection des renseignements personnels et de faire en sorte que toute restriction des échanges transfrontières des renseignements personnels est nécessaire et demeure proportionnelle aux risques associés. 4. Chacune des Parties s'efforce d'adopter des pratiques non discriminatoires pour protéger les usagers du commerce numérique contre les atteintes à la protection des renseignements personnels survenant dans les limites de sa juridiction. 5. Chacune des Parties publie de l'information sur la protection des renseignements personnels qu'elle accorde aux usagers du commerce numérique, y compris sur les moyens permettant : (a) aux personnes physiques d'exercer des recours ; (b) aux entreprises de se conformer à toutes les exigences juridiques. 6. Reconnaissant que les Parties peuvent adopter différentes approches juridiques en matière de protection des renseignements personnels, chacune des Parties devrait encourager l'élaboration de mécanismes favorisant une compatibilité entre les différents régimes. Les Parties s'efforcent d'échanger de l'information sur les mécanismes appliqués dans leur pays et d'explorer des façons d'élargir ces mécanismes ou d'autres arrangements adéquats pour promouvoir leur compatibilité. Les Parties reconnaissent que le système de règles transfrontalières de protection de la vie privée de l'APEC est un mécanisme valable pour faciliter les transferts transfrontières de renseignements tout en protégeant les renseignements personnels.	2.8 Protection des données à caractère personnel et de la vie privée 1. Les Membres reconnaissent que la protection des données à caractère personnel et de la vie privée est un droit fondamental et que des normes élevées à cet égard contribuent au renforcement de la confiance dans l'économie numérique et au développement du commerce. 2. Les Membres pourront adopter et maintenir les mesures de sauvegarde qu'ils jugeront appropriées pour assurer la protection des données à caractère personnel et de la vie privée, y compris par l'adoption et l'application de règles relatives au transfert transfrontières de données à caractère personnel. Aucune des dispositions des disciplines et engagements convenus n'affectera la protection des données à caractère personnel et de la vie privée assurée par les mesures de sauvegarde des Membres. 3. On entend par données à caractère personnel tout renseignement concernant une personne physique identifiée ou identifiable.

Le volume de données que nous créons et partageons dans le cadre de nos vies quotidiennes connaît une croissance exponentielle. Quatre-vingt-dix pour cent des données du monde entier ont été créées au cours des deux dernières années, et plus de 2,5 milliards de gigabytes de données sont produits chaque jour, l'équivalent de l'espace de stockage de 19,5 millions d'iPads nouveaux[26]. Des entreprises entières sont fondées sur le principe de procéder sans relâche à la collecte du plus grand nombre possible de données sur les usagers d'internet, en vue de monétiser ces données. L'UE a pris les devants en matière législative, avec son Règlement général sur la protection des données qui exige que les entreprises obtiennent le consentement des usagers avant de procéder à la collecte de données et qui régit la manière dont elles pourront utiliser, partager ou vendre ces données à de tierces parties. Cette position s'oppose à celle du reste du monde, pratiquement, en particulier celle des États-Unis, où n'existent que des protections minimes des données.

Ce qui signifie que les dispositions sur la protection des données sont sans nul doute parmi les plus controversées et difficiles, puisque les positions fondamentales des principales parties à la négociation (États-Unis et UE[27]) sont à ce point diamétralement opposées.

Les textes concernant les protections des données dans les quatre traités commencent avec des ressemblances générales ; toutefois, les petites différences entre eux nous en disent beaucoup sur les positions de chacune des parties à la négociation. Dans le PTPGB, l'accord UE-Japon et l'ACEUM, on trouve un engagement des parties qui « reconnaissent les avantages économiques et sociaux qu'apporte la protection des renseignements personnels ». En revanche, la Communication de l'UE à l'OMC va plus loin, en reconnaissant que « la protection des données à caractère personnel et de la vie privée est un droit fondamental ». Cette différence dans le libellé est significative, puisque les premiers textes reconnaissent simplement la possibilité de tirer des avantages sociaux et économiques de la mise en œuvre de politiques de protection des données et laissent aux pays la faculté d'appliquer une législation, alors que la Communication de l'UE énonce les concepts de « protections des données » et de « droit fondamental » de façon à ce qu'il soit vraisemblablement impératif pour les États d'adopter des mesures. Ce qui dévoile l'approche fondamentalement différente de la protection des données personnelles entre l'UE et les États-Unis. Quant à l'accord UE-Japon, son libellé mélange les principaux textes américains de l'ACEUM et du PTPGB avec certains aspects de la Communication de l'UE à l'OMC, reconnaissant la validité de la législation sur la protection des données ainsi que les lois existantes sans pour autant aller aussi loin que l'évocation d'un « droit fondamental ».

Le PTPGB et l'ACEUM semblent tous deux exiger des États qu'ils prennent des mesures positives pour que chaque partie « adopte ou maintienne un cadre juridique assurant la protection des renseignements personnels ». Cependant, cette clause comporte une note de bas de page importante qui prévoit que « … une Partie peut se conformer à l'obligation prévue par le présent paragraphe en adoptant … des lois prévoyant l'application d'engagements volontaires en matière de vie privée pris par les entreprises ». Cette précision permet à une partie d'être en conformité rien qu'en établissant un mécanisme de surveillance des régimes volontaires existants de protection des données. Or, les régimes volontaires de conformité mis en place par les entreprises ne parviennent pas à atteindre les objectifs pour lesquels ils ont été mis en place[28, 29] ; sachant les défis rencontrés dans l'UE pour faire respecter le RGPD, l'on pourrait s'interroger sur le bien-fondé des régimes volontaires dans ce domaine. Alors que l'accord UE-Japon reste muet sur les mesures à prendre, la Communication de l'UE à l'OMC couvre très clairement la possibilité pour une partie de mettre en œuvre une législation sévère en matière de protection des données. Elle prévoit en effet que les pays « pourront adopter et maintenir [d]es mesures de sauvegarde », y compris par « l'adoption et l'application de règles relatives au transfert transfrontières de données à caractère personnel ». L'ACEUM met en garde spécifiquement contre l'application de restrictions aux flux transfrontières de données à moins que la restriction soit « nécessaire et demeure proportionnelle aux risques associés ».

Un aspect positif qu'il convient de souligner est l'inclusion de la protection des données en tant que disposition spécifique, en particulier parce qu'elle reconnaît le rôle que les régimes de protections des données peuvent jouer pour accroître la confiance dans le commerce numérique. Et même s'il est peu probable que les États-Unis utilisent cette disposition de la sorte, elle laisse malgré tout la possibilité, même en vertu de l'ACEUM et du PTPGB, à un État d'adopter des règles de protection de la vie privée et des données personnelles qui soient plus proches de celles de l'UE.

L'UE ne va pas sacrifier sa position sur la protection des données, puisque celle-ci fait partie intégrante de sa stratégie de différenciation d'avec l'approche libre-échangiste libérale des États-Unis et du capitalisme d'état de la Chine. Afin que l'UE soit en mesure de transférer les données personnelles, son partenaire commercial devrait se soumettre à un « test d'adéquation »[30] pour vérifier que le niveau de protection des données sera suffisant. Il en découle une argumentation intéressante : si l'UE permettait aux États-Unis d'insérer la note de bas de page décrite plus haut, qui accepte que des régimes volontaires soient suffisants

26 Dans l'hypothèse d'un stockage maximum normalisé de 128GB par iPad (https://www.apple.com/uk/ipad-10.2/)
27 Vraisemblablement, la Chine aussi, mais aucun des accords faisant l'objet de notre analyse n'inclut la Chine.
28 Laufer, W.S. (2013) *Social Accountability and Corporate Greenwashing (La responsabilité sociale et l'écoblanchiment des entreprises).* Journal of Business Ethics 43, 253–261 (2003) doi:10.1023/A:1022962719299
29 Koehler, D. (2007) *The Effectiveness of Voluntary Environmental Programs—A Policy at a Crossroads? (L'efficacité des programmes environnementaux volontaires : une politique à la croisée des chemins ?)* Policy Studies Journal Vol 35, Issue 4
30 Commission européenne. *Adequacy Decisions (Décisions sur l'adéquation).* Consulté sur : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (en anglais uniquement)

au niveau de la conformité avec les dispositions de l'accord de libre-échange, alors les États-Unis pourraient avancer qu'étant donné qu'ils respectent leurs obligations en vertu du traité, leurs protections doivent être jugées adéquates et suffisantes. Cela constituerait une victoire stratégique de grande ampleur pour les États-Unis, et sonnerait le glas du régime de protection des données de l'UE.

L'autre stratégie des États-Unis, qui consiste à faire en sorte que des règles minimales de protection des données n'empêchent pas la coopération avec les pays dans lesquels il existe des niveaux de protection élevés, est implicite dans le paragraphe 5 de la disposition. Cette section, fondamentalement, encourage les États à reconnaître mutuellement leurs règles respectives de protection de la vie privée et des données, même si elles sont loin d'être analogues quant à leur impact sur la protection des données. Comme observé par la Fondation pour la liberté électronique, cette clause signifie en réalité que des endroits comme l'UE, dotés de lois plus sévères en matière de protection des données à caractère personnel, sont encouragés à traiter les régimes de protection des données tels que ceux des États-Unis, qui sont des dispositifs volontaires, comme s'ils étaient équivalents, afin de permettre la collecte, le traitement et le transfert transfrontières de ces données[31].

Le principe qui veut que l'internet devrait être d'accès libre et non discriminatoire a été important dans le développement de l'internet et de l'économie numérique dans son ensemble. Le concept de la « neutralité du réseau » établit que les « fournisseurs de services internet (FSI) doivent traiter toutes les communications internet sur un pied d'égalité, sans aucune discrimination ni variation dans les prix pratiqués en fonction de l'usager, du contenu, du site web, de la plateforme, de l'application, du type d'équipement, de l'adresse source, de l'adresse de destination ou de la méthode de communication »[32]. Ce principe a des impacts réels ; en fait, on peut légitimement se demander si des services tels que Skype ou Netflix auraient pu croître et prospérer s'ils n'avaient pas été protégés contre une discrimination à l'égard de leur trafic grâce aux principes fondamentaux de neutralité du réseau.

Sans neutralité du réseau, les FSI pourraient limiter ce que vous pouvez ou ne pouvez pas voir. C'est déjà le cas dans nombre de régimes autoritaires de par le monde, qui tentent de contrôler activement et de gérer les informations qui sont accessibles et les services qui sont utilisables par leurs habitants. La crainte, si la neutralité du réseau devait disparaître, est que certains contenus et services puissent être complètement bloqués par l'un ou l'autre FSI, qui pourrait d'ailleurs obliger les sites web à les rétribuer faute de quoi ils subiraient des vitesses ralenties de transfert de données, ce qui risquerait de faire disparaître les services en ligne de plus petites dimensions.

ACCÈS À UN INTERNET OUVERT

PTPGB	UE-Japon	ACEUM	Communication de l'UE à l'OMC
Article 14.10 : Principes relatifs à l'accès à Internet et à l'utilisation d'Internet pour le commerce électronique Sous réserve des politiques, lois et règlements applicables, les Parties reconnaissent les avantages pour les consommateurs sur leurs territoires d'être en mesure : (a) d'avoir accès aux services et aux applications de leur choix disponibles sur Internet, et de les utiliser, sous réserve d'une gestion raisonnable du réseau ; (b) de se connecter à Internet avec les dispositifs d'utilisateurs clients de leur choix, à condition que ces dispositifs n'endommagent pas le réseau ; (c) d'avoir accès à de l'information sur les pratiques de gestion du réseau de leurs fournisseurs d'accès Internet.		Article 19.10 : Principes relatifs à l'accès à Internet et à l'utilisation d'Internet pour le commerce numérique Les Parties reconnaissent qu'il est avantageux pour les consommateurs sur leurs territoires d'être en mesure : (a) d'avoir accès aux services et aux applications de leur choix disponibles sur Internet, et de les utiliser, sous réserve d'une gestion raisonnable du réseau ; (b) de connecter les dispositifs d'utilisateur final de leur choix à Internet, à condition que ces dispositifs n'endommagent pas le réseau ; (c) d'avoir accès à de l'information sur les pratiques de gestion du réseau de leur fournisseur d'accès Internet.	2.9 Accès à un internet ouvert Sous réserve des politiques, lois et règlements applicables, les Membres devraient maintenir ou adopter des mesures appropriées pour faire en sorte que les utilisateurs finals sur leur territoire puissent : (a) accéder, distribuer et utiliser les services et applications de leur choix disponibles sur Internet, sous réserve d'une gestion raisonnable et non discriminatoire du réseau ; (b) connecter les dispositifs de leur choix à Internet, à condition que ces dispositifs ne nuisent pas au réseau ; (c) avoir accès aux informations relatives aux pratiques de gestion du réseau appliquées par leur fournisseur de services d'accès à Internet.

31 Malcom, J. & Maira, S. (5 novembre 2015) *Release of the full TPP text after five years of secrecy confirms threats to users' rights (La publication du texte complet du PTP après cinq années de secret confirme les menaces qui pèsent sur les droits des usagers).* Electronic Frontier Foundation. Consulté sur : https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights

32 Wikipedia - https://en.wikipedia.org/wiki/Net_neutrality (en anglais ; la version française est quelque peu différente)

Le texte des accords de commerce ne consacre pas le principe de la neutralité du réseau, mais le PTPGB et l'ACEUM le décrivent en tant que « Principes relatifs à l'accès à Internet et à l'utilisation d'Internet pour le commerce électronique », alors que l'UE a simplement adopté le titre « Accès à un internet ouvert ». Il est important de souligner que plutôt que de consacrer le concept de la neutralité du réseau, les dispositions visent à garder l'internet aussi ouvert que possible.

L'accord UE-Japon ne contient aucune mention d'un accès à un internet ouvert. Il ne faut probablement pas interpréter cette absence autrement que par le fait que la question n'avait pas une importance suffisante aux yeux des deux parties pour exiger de la faire figurer dans l'accord, ou qu'elles ne pensaient pas parvenir aisément à un libellé satisfaisant qui reflète de manière adéquate leurs positions respectives, puisque l'UE dispose non seulement de son propre texte en la matière mais elle a aussi conclu des accords de libre-échange incluant de telles dispositions.

Les autres accords de libre-échange utilisent le même libellé, si ce n'est que le PTPGB et la Communication de l'UE à l'OMC précisent au préalable que les dispositions s'appliquent « sous réserve des politiques, lois et règlements applicables ». Le texte commun n'établit aucune obligation contraignante pour les États mais fait plutôt en sorte que les parties « reconnaissent qu'il est avantageux » pour les personnes et les entreprises d'avoir la possibilité « d'avoir accès aux applications et services de leur choix » et d'être en mesure de « connecter les dispositifs de leur choix à Internet » et « d'avoir accès à de l'information sur les pratiques de gestion du réseau » des fournisseurs d'accès Internet. Il existe quelques petites réserves, telles que le fait de ne pouvoir connecter un dispositif à un réseau qu'à la condition que le dispositif n'endommage pas le réseau.

Il existe des différences intéressantes, subtiles mais importantes, entre le PTPGB et l'ACEUM d'une part et la Communication de l'UE à l'OMC d'autre part. Les textes disent tous que pour les consommateurs, « l'accès aux services et applications de leur choix » peut se faire sous réserve d'une « gestion raisonnable du réseau », expression très ample qui laisse la possibilité aux FSI de mettre en œuvre des politiques de gestion du trafic. Ainsi ce texte ouvre très clairement la voie pour que les FSI commencent à gérer activement le trafic de leur réseau, en infraction flagrante des principes de la neutralité du réseau. L'UE quant à elle ajoute un adjectif d'une importance essentielle à cette disposition, « non discriminatoire ». Cet adjectif ne figure pas dans les autres traités alors qu'il fournit une véritable garantie contre toute gestion de trafic discriminatoire de la part des FSI, qui s'apparente dès lors au principe de neutralité du réseau. Dans l'ensemble, la disposition sur la neutralité du réseau ne confère pas de protection parce qu'elle est trop ténue, en particulier dans les traités menés par les États-Unis. Et, ce qui est plus accablant encore, elle « risque d'empêcher dans les faits le développement de normes mondiales plus fortes et conséquentes »[33].

Même si nombreux sont ceux qui pensent, aux États-Unis, que la neutralité du réseau a disparu à cause de la réinstauration, par la Commission fédérale au commerce, de l'*Internet Freedom Order* en 2017 mis en œuvre en 2018, qui confère aux FSI entière liberté de « faire pratiquement à leur guise »[34], en Europe et dans une grande partie du reste du monde, cette bataille si importante fait encore rage.

33 Malcom, J. & Maira, S. (5 novembre 2015) *Release of the full TPP text after five years of secrecy confirms threats to users' rights (La publication du texte complet du PTP après cinq années de secret confirme les menaces qui pèsent sur les droits des usagers).* Electronic Frontier Foundation. Consulté sur : https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights

34 Kelly, M. (11 juin 2018) *Net Neutrality is dead – what now? (La neutralité du réseau n'est plus. Et maintenant, que fait-on ?*) Consulté sur : https://www.theverge.com/2018/6/11/17439456/net-neutrality-dead-ajit-pai-fcc-internet

INCIDENCES CONCRÈTES SUR LE TRAVAIL ET LES MARCHÉS DE L'EMPLOI

L'analyse présentée dans la partie précédente montre clairement les profondes préoccupations existantes au sujet de la possibilité que des domaines critiques de l'économie numérique voient leurs règles fixées au niveau mondial par les intérêts des pays industrialisés, et plus particulièrement par les géants du secteur qui se trouvent dans ces pays. Nous avons mis en exergue certaines des problématiques posées par chacune des dispositions. Le présent chapitre en revanche nous donnera l'occasion de nous pencher sur les incidences de l'ensemble du chapitre consacré au commerce électronique, dans le cadre des accords de libre-échange dans lesquels il s'inscrit, sur le monde du travail et les marchés de l'emploi.

Il est important d'observer que les incidences concrètes que nous allons recenser sont des possibilités, basées sur des hypothèses. Nous décrivons clairement ces hypothèses dans chacun des exemples lors de leur application. L'économie numérique étant encore en plein développement, sachant en outre que de nombreux pays doivent encore adhérer à des accords de libre-échange, nombre de répercussions restent encore à découvrir. De même, il se pourrait que les hypothèses formulées au sujet de nouveaux domaines de textes juridiques ne prévoient pas certaines incidences concrètes qui ne seront détectées qu'à l'épreuve des faits, avec une mise en œuvre et une application effectives.

Il apparaît clairement que les géants du secteur ont déjà un impact matériel sur le monde du travail, dont l'essentiel est d'ordre disruptif et affecte directement la vie des travailleurs, en particulier dans les secteurs les plus précaires et les moins bien rémunérés du marché de l'emploi.

Dans de nombreux cas, comme suggéré dans l'analyse ci-dessous, ce que font souvent les accords sur le commerce numérique, c'est ne pas créer de problèmes supplémentaires… ce qui arrive pourtant parfois. Un exemple : les restrictions accrues au partage des codes sources. En revanche, ces accords comportent essentiellement des dispositions qui avantagent surtout les géants du secteur, concernant par exemple les flux transfrontières de données ou l'interdiction des exigences en matière d'emplacement, ce qui permet aux géants du secteur de continuer à bénéficier de manière disproportionnée de l'économie numérique. Comme synthétisé par Deborah James, directrice de Our World is Not for Sale (Notre monde n'est pas à vendre), les grands groupes d'entreprises « utilisent depuis longtemps les accords sur le commerce pour verrouiller des règles qui avantagent leurs soi-disant droits à faire des bénéfices, tout en limitant la capacité des gouvernements à réglementer leurs activités en défense de l'intérêt public et ce, souvent à un point qui n'aurait jamais été atteint par la voie démocratique normale »[35].

INCIDENCE 1 – ACCROÎTRE LA PRÉCARITÉ DU TRAVAIL

La technologie a déjà un effet disruptif sur les marchés du travail partout dans le monde, et la future automation ainsi que la quatrième révolution industrielle vont multiplier la disruption dans les décennies à venir[36]. S'il est vrai que les géants du secteur ont contribué à la création de certains emplois hautement qualifiés dans l'ingénierie, la programmation informatique et la conception des produits, il n'en reste pas moins que la majorité des nouveaux emplois créés ou rendus plus porteurs en raison de la technologie sont des emplois précaires et faiblement qualifiés. Parmi les exemples de ce type d'emplois, citons les livreurs pour Hermes, les équipes faisant du ménage sur TaskRabbit ou la saisie des données sur le Turc mécanique d'Amazon. De manière générale, ces activités sont décrites comme étant réalisées par des travailleurs définis comme « indépendants » ou « intérimaires », ce qui les prive d'une grande partie des droits du travail[37]. Souvent, aucun horaire fixe ou prévisible n'est donné, ce qui peut être un facteur attractif pour certaines personnes, mais rend difficile de pourvoir aux besoins d'une famille ou d'obtenir un crédit hypothécaire. Les systèmes d'évaluation, une surveillance exagérée et des objectifs officiels imposés enlèvent du pouvoir aux travailleurs, en considération des employeurs et des acheteurs. En effet, une évaluation négative ou des objectifs non atteints, même si la première n'était pas méritée et les derniers impossibles à atteindre, peuvent avoir de graves conséquences, y compris des sanctions ou la perte de l'emploi.

35 James, D (22 novembre 2017) *Twelve reasons to oppose rules on digital commerce in the WTO (Douze raisons de s'opposer aux règles sur le commerce numérique à l'OMC)*. Consulté sur : https://www.huffpost.com/entry/twelve-reasons-to-oppose-rules-on-digital-commerce

36 Manyika, J et al (2017) *Jobs Lost, jobs gained: Workforce transitions in times of automation (Emplois perdus, emplois gagnés: transition de la main-d'œuvre à l'ère de l'automation)*. Mckinsey Global Institute. Consulté sur : https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

37 Eurofound (2018) *Platform work: Employment status, employment rights and social protection (Plateformes d'emploi: statut d'emploi, droits du travail et protection sociale)*. Consulté sur : https://www.eurofound.europa.eu/data/platform-economy/dossiers/employment-status

L'élément clé du succès de toutes ces plateformes est le volume colossal de données qu'elles collectent et traitent, auquel s'ajoute la volonté d'avoir un effet disruptif sur les marchés existants pour finir par les dominer, en faisant souvent fi des réglementations en vigueur et sans penser aux répercussions générales sur le plan social. Certes, ce ne sont pas les géants du secteur qui ont inventé le statut de faux indépendant ou le travail précaire, mais ils en ont étendu la portée et en ont changé la nature, parfois de manière importante. Un récent rapport a indiqué que 17 % de la population en Espagne prenait part au travail sur plateforme[38]. À mesure de la prolifération du travail sur plateforme, la négociation collective perd du terrain, puisque celle-ci est nettement plus compliquée pour les travailleurs à leur compte. Entre-temps, la surveillance des travailleurs s'est considérablement étendue, à la fois en envergure et en profondeur. Parmi les exemples, citons la capture des frappes sur le clavier des travailleurs, pratique à laquelle se livrent à l'heure actuelle 45 % des entreprises étatsuniennes[39], ou encore l'obligation de porter des dispositifs de traçage, dont 202 millions ont été distribués en 2016[40], ou le recours à des logiciels spécialisés pour surveiller les applications de réseaux sociaux et de messagerie privée du personnel[41].

Bon nombre des géants du secteur, par exemple Uber[42] ou Foxconn[43], ont comme objectif explicite d'automatiser au maximum leurs opérations, et investissent des milliards à cette fin. Ce sont les travailleurs qui fournissent les données requises pour élaborer les algorithmes essentiels… mais ces algorithmes vont les remplacer. La nature de ces marchés numériques pilotés par les données fait que l'entreprise qui est tombée sur une mine de données et qui a la capacité de les transformer en renseignements exploitables dispose d'un véritable avantage concurrentiel[44].

Nombre des dispositions relatives au commerce électronique analysées dans le présent rapport, notamment sur l'emplacement des données, la confidentialité du code source, la libre circulation des flux de données transfrontières et l'abolition de la neutralité du réseau, avantagent les plus grandes entreprises transnationales de la technologie parce qu'elles exploitent les économies d'échelle favorisées surtout par le secret du code source, et qui sont donc les mieux à même de tirer profit des flux de données et d'assumer les coûts d'un internet non neutre. Ces flux de données, ainsi que le code et les apprentissages à partir des données, vont connaître une importance croissante à l'avenir, à mesure que de plus en plus d'emplois seront automatisés et mis sur plateforme. Ceci rendra de plus en plus difficile la création ou la survie d'options locales non numériques, surtout si elles ont des approches sociales et environnementales différentes. Tant que le modèle d'emploi au sein des géants du secteur n'aura pas changé, cette évolution risque d'aboutir à une augmentation du nombre de personnes contraintes de travailler dans les conditions associées au travail sur plateforme.

INCIDENCE 2 – RENDRE PLUS DIFFICILE L'APPLICATION DE LA LÉGISLATION LOCALE DU TRAVAIL

Lorsqu'il y a infraction à la loi, il faut traduire une entité en justice pour qu'elle réponde de ses actes. Cette procédure est facilitée si une entreprise est enregistrée localement, parce que cette entité locale pourra être tenue juridiquement de s'astreindre à la procédure légale nationale et de respecter le jugement rendu. D'autre part, comme la CSI l'a déjà dit par le passé, « sans cette présence locale des entreprises, il n'existe aucune entité à poursuivre en justice et la capacité des tribunaux nationaux à faire respecter les normes du travail, ainsi que d'autres droits, est fondamentalement entravée ».

La plus récente Communication de l'UE à l'OMC, concernant les services de télécommunication, propose déjà que les fournisseurs de services ne soient pas contraints d'établir une entité légale locale. Le très influent Cato Institute dit que son accord idéal entre le Royaume-Uni et les États-Unis serait celui qui « interdirait toute exigence en matière de *présence locale*, à savoir une condition qui obligerait les fournisseurs de service d'une autre partie à être doté d'un bureau, d'un magasin ou de toute autre forme de présence »[45]. Un nombre croissant de services passent par l'intermédiaire de plateformes, et l'internet nous permet d'échanger des biens, des services et des informations avec n'importe qui, mais nous devons veiller à conserver notre faculté de faire appliquer la législation nationale en tant que de besoin, y compris le droit du travail.

L'affaiblissement progressif de notre capacité à faire respecter la législation nationale n'est pas une possibilité théorique éloignée, mais un phénomène qui a déjà

38 Canigueral, A. (30 juin 2019) *How can tech meet the needs of platform workers? (Comment la technologie peut-elle répondre aux besoins des travailleurs des plateformes ?*) Consulté sur : https://www.thersa.org/discover/publications-and-articles/rsa-blogs/2019/06/tech-platform-workers
39 McCann, D. & Warin, R. (2018) *Who Watches the Worker? (Qui surveille les travailleurs ?*) New Economics Foundation. Consulté sur : https://neweconomics.org/2018/06/who-watches-the-workers
40 Wild, J. (28 février 2017) *Wearables in the workplace and the dangers of staff surveillance (Dispositifs portables sur le lieu de travail et les dangers de la surveillance du personnel*). The Financial Times. Consulté sur : https://www.ft.com/content/089c0d00-d739-11e6-944b-e7eb37a6aa8e
41 Solon, O. (6 novembre 2017) *Big Brother isn't just watching: workplace surveillance can track your every move (Big Brother ne se contente pas de vous regarder : la surveillance sur le lieu de travail retrace votre moindre geste).* The Guardian. Consulté sur : https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology
42 Newton, C. (28 mai 2014) *Uber will eventually replace all its drivers with self-driving cars (Uber finira par remplacer tous ses conducteurs par des véhicules autonomes).* The Verge. Consulté sur : https://www.theverge.com/2014/5/28/5758734/uber-will-eventually-replace-all-its-drivers-with-self-driving-cars
43 Javelosa, J. (3 janvier 2017) *Apple manufacturer Foxconn to fully replace humans with robots (Le fabricant d'Apple, Foxconn, remplacera tous les humains par des robots).* Consulté sur : https://futurism.com/apple-manufacturer-foxconn-to-fully-replace-humans-with-robots
44 Mayer-Schonberger, V. & Ramge, T. (2018) Reinventing Capitalism. John Murray
45 Ikenson, D., Lester, S. & Hannan, D. (2019) The ideal US-UK Free Trade Agreement. Cato Institute. Consulté sur : www.ifreetrade.org/pdfs/US-UK-FTA.pdf

commencé, facilité par internet, par la technologie numérique et par le commerce mondial. On en voit déjà des exemples à petite échelle avec certains services, comme le tutorat en ligne. Dans ce secteur, il est très facile de recruter comme tuteur une personne qui vit dans votre pays mais qui travaille pour une plateforme, ou pour une agence ayant son siège dans un autre pays. Dans certains cas, l'entreprise par le biais de laquelle vous confiez un travail n'aura pas d'entité juridique dans votre pays. Ce qui veut dire qu'il sera difficile pour ceux qui achètent le service de se retourner contre l'entreprise si celle-ci n'a pas effectué le service correctement ou pour toute autre raison nécessitant un recours juridique.

Si ce phénomène était étendu aux principales sociétés de l'économie des petits boulots, comme Uber, et que celles-ci n'avaient pas l'obligation d'avoir une entité juridique locale, il deviendrait extrêmement difficile de faire appliquer le droit du travail national et les droits des travailleurs : à l'heure actuelle de nombreux pays essayent de faire respecter le droit du travail par des plateformes ayant une présence locale. S'il devient difficile à ce point de faire respecter le droit du travail, les autorités locales auraient pour seule option d'attaquer les conducteurs eux-mêmes, puisque ceux-ci existent du point de vue juridique dans le pays. Cependant, les autorités se rendraient vite compte qu'il est pratiquement impossible de faire appliquer quelque législation du travail que ce soit puisque ces dispositions juridiques, du salaire minimum au congé maladie, ne s'appliquent pas aux entrepreneurs indépendants. Il est par conséquent essentiel, si l'on veut garantir une possibilité de faire respecter le droit du travail localement, que toute entreprise recrutant du personnel dans un pays dispose d'une entité juridique dans ce pays. Ce n'est qu'ainsi que le droit du travail pourra protéger tout le monde et que les entreprises s'acquitteront de leurs responsabilités face à leurs travailleurs.

INCIDENCE 3 – LÉSINER PAR NÉCESSITÉ SUR LES DROITS DES TRAVAILLEURS

Le marché du travail consiste en un équilibre entre différentes forces, et de manière générale les travailleurs doivent lutter avec acharnement pour que leurs droits soient inscrits dans la loi (par rapport aux entreprises et aux propriétaires des entreprises). Ce n'est pas grâce à la générosité des entreprises que l'on a mis fin au travail des enfants ou que l'on a adopté la semaine de cinq jours, mais plutôt grâce aux efforts concertés des travailleurs, des syndicats et de la société civile, en dépit de l'adversité, qui ont fait qu'en dernière instance les gouvernements responsables démocratiquement mettent en œuvre les nouvelles législations. La transformation numérique de la société met à l'épreuve certains de ces acquis si chèrement gagnés, au sujet de ce qu'est un travailleur et des droits et protections dont il doit jouir.

La plupart des dispositions des accords de commerce comportent des dérogations qui permettent aux gouvernements de réglementer dans des domaines qui sans cela seraient interdits par les accords de libre-échange. Ces dérogations sont souvent complétées par des conditions supplémentaires, stipulant qu'elles doivent répondre à « un objectif légitime de politique publique » et ne doivent pas être « plus restrictives que nécessaires », ce que l'on appelle le test de nécessité.

Il est important de reconnaître l'évolution dans le temps de ce test, au fur et à mesure des décisions prises par l'Organe d'appel de l'OMC. L'un des premiers exemples porte sur l'interdiction en Californie d'un additif pour l'essence qui polluait l'approvisionnement en eau. Cependant, un fournisseur canadien de cet additif a argué que cette décision ne remplissait pas le critère du test de nécessité, puisqu'en théorie la Californie aurait pu résoudre le problème en exigeant que toutes les cuves de stockage soient déterrées pour être rendues étanches. L'OMC a statué en faveur de l'entreprise canadienne qui avait dans les faits proposé une solution entraînant moins de restrictions au commerce mondial. Cette jurisprudence des débuts a été critiquée parce qu'elle penchait trop en faveur du commerce[46]. Même si la jurisprudence a quelque peu évolué, il reste très difficile pour les parties de remplir les critères du test de nécessité légitime pour certaines dérogations.

Lorsqu'on le prend en considération dans l'abstrait, le test de nécessité peut sembler relativement raisonnable. Il peut néanmoins devenir problématique, comme expliqué dans l'excellent exemple présenté par Laura Bannister, conseillère principale auprès du Mouvement pour la justice sociale, lors du récent Forum public de l'OMC organisé sur la surveillance des travailleurs[47]. De nombreux travailleurs de l'économie des petits boulots font déjà l'objet d'une lourde surveillance au travail, qui est en train de s'élargir et commence à couvrir aussi les horaires non travaillés[48]. Les travailleurs et les syndicats sont déjà en train de réclamer de nouveaux droits numériques pour les travailleurs et d'exiger que cesse la surveillance numérique excessive. Si leurs revendications venaient à aboutir et que le gouvernement adoptait une politique qui interdise ou encadre strictement la capacité des entreprises à collecter des données sur la base de cette surveillance excessive, cette politique pourrait être vue comme étant « plus restrictive que nécessaire » par un tribunal du commerce. Et ce, parce que l'entreprise du secteur technologique sera en mesure de démontrer l'incidence de cette politique sur sa capacité commerciale, alors que les syndicats et les travailleurs auront le plus grand mal à démontrer

46 Howse, R. (2002) *Human Rights in the WTO: Whose Rights? What Humanity? Comments on Petersmann (Droits humains à l'OMC : Les droits de qui ? Quelle humanité ? Commentaires sur Petersmann*). 13 EJIL 651, p. 657.
47 Enregistrement audio de la séance 129 du Forum public de l'OMC. Consulté sur : https://www.wto.org/audio/pf19session129.mp3
48 McCann, D. & Warin, R. (2018) *Who Watches the Worker? (Qui surveille les travailleurs ?)* New Economics Foundation. Consulté sur : https://neweconomics.org/2018/06/who-watches-the-workers

scientifiquement et sans nul doute possible que la surveillance des travailleurs et la collecte de données les concernant portent atteinte au bien-être et à la vie privée des travailleurs. D'autres domaines cruciaux pour les travailleurs et les syndicats pourraient également rencontrer le même problème face au test de nécessité, par exemple la vie privée des travailleurs, la sécurité des données ou la propriété commune des données.

INCIDENCE 4 – DÉFIS POSÉS À LA TRANSPARENCE ALGORITHMIQUE

Les algorithmes ne sont pas une nouveauté, mais grâce à la révolution numérique ils sont en train de devenir une partie sans cesse croissante de notre vie. Ils sont indispensables dans le monde en ligne compte tenu de la nécessité de trier des volumes colossaux d'information afin de faire de l'internet le précieux service qu'il est aujourd'hui. Au fil de la croissance de l'économie numérique, la portée des algorithmes s'est étendue. Ils sont désormais chargés de près de 40 % des échanges en bourse au Royaume-Uni, ils sont chargés du vol des avions durant plus de 95 % du temps de vol, et ce sont bientôt eux qui pourraient se retrouver aux commandes de nos voitures. En outre les algorithmes commencent à se diffuser dans de nouveaux domaines pour aider à la prise de décisions humaines, par exemple pour déterminer le bien-fondé d'un entretien d'embauche avec tel candidat, ou statuer sur la probabilité de récidive chez un délinquant, ou décider des prestations sociales qui seront nécessaires pour tel bénéficiaire. Bien que ces algorithmes décisionnels se présentent tous sous un vernis d'objectivité technologique, rappelons qu'ils sont conçus par des personnes, tout comme la collecte de données qui les nourrit, et que par conséquent leurs paramètres et hypothèses de base sont façonnées par des décisions humaines, donc en fin de compte subjectives.

Alors que les algorithmes pénètrent des zones de plus en plus sensibles de notre vie, il est indispensable de se doter d'un systèmes responsabilisant de manière conséquente les créateurs et diffuseurs de ces systèmes de décision par algorithme, en particulier là où les décisions auront un impact significatif sur des individus.

Les dispositions sur les codes sources dans les futurs accords sur le commerce électronique rendraient très difficile pour les gouvernements d'exiger un accès au code source comme condition pour permettre à autrui d'accéder à son marché. La restriction à des domaines juridiques très précis tels que la propriété intellectuelle ou le droit de la concurrence impliquerait une grande difficulté à exiger l'accès pour garantir les exigences en matière de transparence, de responsabilité et d'audit des futurs systèmes de reddition de comptes algorithmique.

Les dispositions sur les codes sources rendraient difficile également pour les travailleurs de se pencher sur le fonctionnement interne des algorithmes qui vont pourtant se trouver au cœur du monde du travail. Les algorithmes sont déjà utilisés dans une vaste palette de domaines relatifs au travail, et les algorithmes de recrutement sont certainement ceux dont on parle le plus. Ces systèmes algorithmiques d'aide à l'embauche passent en revue les CV et les candidatures en ligne en vue de sélectionner les candidats les plus appropriés, ce qui permet d'automatiser certaines des procédures de recrutement, voire toutes. En 2018 Amazon a décidé d'abandonner son propre algorithme de recrutement, alors qu'il travaillait depuis quatre ans à son développement, parce que l'entreprise s'est aperçue « que son nouveau système ne respectait le principe de l'égalité entre les sexes dans ses notations »[49]. Si même Amazon, dotée de fonds presque illimités et d'une armée de codeurs de l'IA, ne parvient pas à rectifier les préjugés inscrits dans un algorithme, on ne peut que s'interroger sur la possibilité qu'auraient eu les vendeurs commerciaux d'un tel logiciel de recrutement.

Afin de compter sur une plus grande transparence concernant ces codes sources critiques, et de mieux comprendre leur fonctionnement, les défenseurs d'une déontologie de l'IA veulent que l'on donne aux algorithmes une plus grande visibilité pour que l'on puisse les inspecter et les comprendre, en particulier lorsqu'ils mènent à une prise de décisions susceptibles d'avoir des conséquences pernicieuses ou négatives, par exemple le refus d'une candidature pour un emploi ou un accident provoqué par un véhicule sans chauffeur. Or, cette transparence risque d'être rendue très difficile, voire impossible, avec les interdictions, dans les ALE existants, de communiquer les codes sources. En effet, comme le précise la journaliste primée Kate Kaye, « La pression exercée pour restreindre l'accès aux algorithmes se fait au détriment des personnes, au détriment des usagers et au détriment des consommateurs »[50].

INCIDENCE 5 – ÉTENDRE LE DROIT DES SOCIÉTÉS DU NUMÉRIQUE À ACCÉDER AU MARCHÉ

Une révolution silencieuse est en cours au sein des pouvoirs publics, appellée Tech.gouv, qui pourrait transformer la nature des services publics et de ceux qui en sont responsables, parce que les systèmes de décision automatisée sont de plus en plus utilisés pour déterminer qui doit bénéficier des services publics ; en outre

49 Dastin, J. (10 octobre 2018) *Amazon scraps secret Ai recruiting tool that showed bias against women (Amazon met au rebut son outil secret d'IA pour le recrutement qui comportait un préjugé sexiste).* Consulté sur : https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-id

50 Kaye, K. (8 novembre 2018) *How the tech industry coordinated to squelch algorithm transparency in the new NAFTA deal (Comment le secteur technologique s'est concerté pour étouffer la transparence des algorithmes dans le nouvel ALENA*). Consulté sur : https://redtailmedia.org/2018/11/08/how-the-tech-industry-prevented-algorithm-transparency-in-nafta-2-0/

des systèmes sont mis en place pour cibler « de manière plus efficiente » les maigres ressources publiques. Imitant d'autres technologies ayant un effet disruptif telles que fintech[51] ou proptech[52], un récent rapport de PriceWaterhouseCooper avançait que « Tech.gouv a le pouvoir de transformer la prestation de services publics, avec de meilleurs résultats pour moins d'argent et en améliorant l'expérience utilisateur »[53].

Nous observons déjà que des sociétés technologiques se retrouvent au cœur de décisions clés que nous associons habituellement à l'État. Par exemple, les algorithmes prédictifs qui formulent des suggestions aux services de la police concernant les domaines dans lesquels se concentrer compte tenu de leurs ressources de plus en plus limitées[54] ou des logiciels qui tentent de calculer les probabilités qu'un nouveau-né soit victime de maltraitance à l'avenir[55].

Le fait que les services publics reposent de plus en plus sur des algorithmes et des données numériques pourrait également signifier que le secteur privé se retrouve à jouer un rôle accru dans des domaines centraux des services publics. Les défis supplémentaires que pourraient introduire les règles du commerce électronique ont trait à la restriction du pouvoir gouvernemental de contrôler et réglementer les activités des entreprises qui seraient chargées de certains services publics fondamentaux. Les règles du commerce électronique pourraient signifier que les pouvoirs publics ne peuvent plus exiger par défaut une communications des codes sources, ni limiter les flux de données ou exiger qu'une partie de la collecte et de l'analyse des données soit effectuée localement. Or, il est essentiel de pouvoir exiger le code source si l'on veut veiller au bon fonctionnement du système conformément aux spécifications du système tel qu'il a été conçu, et garantir qu'aucune discrimination ne s'applique à l'encontre de certaines parties de la population. De même, il est essentiel de pouvoir limiter les flux de données puisque certaines données sont extrêmement sensibles, par exemples celles recueillies par les services de la santé ou de la police. Par conséquent il ne serait pas approprié que l'option par défaut pour ces données soit la possibilité d'un transfert international car celui-ci signifierait que l'on perd la compétence juridictionnelle nationale en la matière et, partant, que l'on perd l'accès aux données.

Un autre défi vient du fait que la numérisation des services publics est utilisée aussi comme un outil en vue d'accroître puis de verrouiller l'étendue des services publics susceptibles d'être délégués au secteur privé, dans des domaines tels que les soins de santé, l'éducation, les collectivités locales, la distribution de l'eau et de l'électricité, qui seraient confiés à des sociétés technologiques qui tentent d'élargir leurs droits à « l'accès aux marchés ». Par exemple, Uber, qui veut en fin de compte être à la tête d'une plateforme unique de mobilité fondée sur le plus possible d'automatisation, a reconnu avoir l'intention de présenter des propositions visant à élargir les droits relatifs à « l'accès aux marchés » pour les sociétés du numérique dans des secteurs qui dépendent de l'OMC. Uber veut également étendre la portée et la couverture de ces secteurs, ce qui pourrait amener à exposer un nombre accru de services publics à la menace de la privatisation, éventuellement en s'opposant à la volonté expresse de la population et du gouvernement.

Une privatisation accrue opérée par les sociétés du numérique mettrait d'importants services publics entre les mains des grandes sociétés numériques, qui n'ont pratiquement aucune responsabilité ni obligations envers les communautés locales en termes de garantie de qualité et d'accessibilité des services.

INCIDENCE 6 – POUVOIR ACCRU DES BIG TECH SUR LES TRAVAILLEURS

L'introduction de la technologie de collecte, d'analyse et de traitement des données a eu un effet de disruption sur le délicat équilibre entre travailleur et employeur, faisant retourner le pouvoir résolument entre les mains des employeurs. C'est particulièrement vrai dans le cadre des nouvelles plateformes de travail telles que Deliveroo ou le Turc mécanique d'Amazon, mais cette tendance s'est infiltrée dans tous les domaines du travail. Un récent rapport rédigé par la New Economics Foundation a conclu que les entreprises sont en train de multiplier les manières d'exercer davantage de pouvoir sur les travailleurs[56]. Tout d'abord, en étendant la surveillance de leurs salariés au-delà des principaux horaires de travail, et physiquement en incluant la surveillance du corps même des travailleurs. Cela peut sembler incroyable, mais 45 % des entreprises aux États-Unis tiennent un registre des frappes clavier effectuées par leur personnel[57]. En deuxième lieu, l'entreprise étant propriétaire des données qu'elle produit, celles-ci sont utilisées de manière prépondérante pour avantager la direction de l'entreprise, ce qui mène à une charge de travail accrue pour chaque travailleur et, lorsqu'il n'est plus possible de recourir à plus de travail pour produire plus, à la diminution du personnel. L'exemple type de cette inten-

51 Se référant à une entreprise qui applique la technologie pour proposer des services dans le secteur de la finance.
52 Se référant à une entreprise qui applique la technologie pour proposer des services dans le secteur immobilier, en particulier celui de la location.
53 PriceWaterhouseCooper. *Gov.Tech: the power to transform public services in the UK* (Tech.gouv : le pouvoir de transformer les services publics au Royaume-Uni). Consulté sur : https://www.pwc.co.uk/industries/government-public-sector/govtech.html
54 Couchman, H. (2019) *Policing by Machine (La police gérée par une machine*). Consulté sur : https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf
55 Pegg, D. & McIntyre, N. (16 septembre 2018) *Child abuse algorithms: from science fiction to cost-cutting (Algorithmes sur la maltraitance des enfants : de la science-fiction à l'optimisation des coûts).* Consulté sur : https://www.theguardian.com/society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality
56 McCann, D. & Warin, R. (2018) *Who Watches the Worker? (Qui surveille les travailleurs ?)* New Economics Foundation. Consulté sur : https://neweconomics.org/2018/06/who-watches-the-workers
57 Johnson, C. (2017) *Meeting the Ethical Challenges of Leadership: Casting Light or Shadow (Relever les défis éthiques du leadership : faire la lumière ou plonger dans l'ombre*). SAGE Publications Inc.

sification du travail est donné par Amazon : un contrôle compulsif et la fixations d'objectifs sévères font qu'il est possible dans cette entreprise de retracer, d'enregistrer et d'évaluer toutes les activités des travailleurs, afin de vérifier qu'ils atteignent à tout moment les cibles de l'entreprise, pour exigeantes qu'elles soient. Enfin, les employeurs se cachent derrière des systèmes décisionnels algorithmiques qui leur permettent concrètement de ne plus être tenus pour responsables et éventuellement d'intégrer dans les décisions des préjugés affectant les travailleurs.

Ces évolutions ont déjà conduit à une réduction du pouvoir des travailleurs en faveur des employeurs. Les accords sur le commerce numérique n'ont pas créé ces problématiques, mais ils limitent en revanche l'espace politique dont les pays disposent, ce qui rend plus compliqué d'atténuer ces résultats négatifs. Trois des dispositions figurant dans les chapitres sur le commerce numérique des accords de commerce permettent aux Big Tech de renforcer et de cimenter leur position de pouvoir sur les travailleurs. Tout d'abord, les transferts transfrontières de données, n'étant pas réglementés, permettront aux Big Tech d'acquérir toutes les données dont elles ont besoin pour surveiller leur main-d'œuvre tout en effectuant une analyse minutieuse des données, aidant les entreprises à tirer le meilleur parti de leurs travailleurs. Ensuite, la disposition qui veille à ce que le code source ne soit pas facilement accessible, en particulier pour des problématiques de préjugés ou de discriminations, permettra aux entreprises de se cacher derrière les « boîtes noires » d'algorithmes qu'elles exploitent. Enfin, le recours au test de nécessité pourrait dans les faits restreindre la possibilité pour les travailleurs de riposter contre les pratiques intrusives de collecte des données par leur entreprise.

Comme nous l'avons observé dans l'exemple consacré au test de nécessité, celui-ci pourrait entraver la capacité des travailleurs et de leur syndicat de résister à la surveillance et au contrôle intrusifs des entreprises. C'est d'autant plus préoccupant que l'on voit se multiplier les cas de personnes licenciées pour un comportement en dehors du lieu de travail et en dehors des horaires de travail. L'on prévoit que d'ici 2021 plus de 500 millions de salariés seront surveillés par le biais de technologies portables. Les entreprises utilisent les données pour mettre au point le renseignement numérique qui contrôlera et gèrera le reste de la main-d'œuvre encore plus étroitement, ouvrant un nouveau cycle d'intrusion et de surveillance.

Les dispositions portant sur le code source menacent de permettre aux employeurs de se cacher derrière des systèmes automatisés de prise de décisions, ce qui réduit leur responsabilité. Des décisions fondamentales, comme de recruter ou de licencier quelqu'un, sont de plus en plus souvent prises par des algorithmes. Si l'on n'a pas accès au code source, il pourrait être très difficile de déterminer si un système fonctionne correctement ou s'il comporte un biais discriminatoire contre certains groupes de population.

INCIDENCE 7 – MENACER L'AVENIR DES INDUSTRIES NATIONALES D'UN PAYS EN EXIGEANT LE LIBRE TRANSFERT DES DONNÉES

Il est assez incroyable, à plus d'un titre, que les grandes sociétés technologiques comptent parmi les entreprises à la valeur la plus élevée au monde, en particulier compte tenu que bon nombre d'entre elles, comme Google ou Facebook, proposent un produit dont l'utilisation est gratuite, alors que d'autres, comme Uber ou Spotify, n'ont pas encore atteint un seuil bénéficiaire. Ce qui sous-tend cette valorisation, ce sont les colossales mines de données collectées par ces entreprises au fil de leurs opérations, données qui sont au cœur de leur succès et de leur position dominante. Toutes les sociétés technologiques s'appuient sur la capacité de collecter et de tirer profit de gros volumes de données sur leurs utilisateurs et sur les travailleurs qui relèvent de leur écosystème, souvent complétés par des ensembles de données achetés à des tiers. Leurs ingénieurs construisent des algorithmes sophistiqués en vue d'analyser les données et de les transformer en renseignements exploitables, qu'ils pourront ensuite monétiser en vue d'engendrer des revenus et des bénéfices. L'une des meilleures illustrations du phénomène est probablement le cas d'Uber. Uber est une société de transport valorisée à l'heure actuelle autour de 50 milliards de dollars, et qui pourtant ne détient pas un seul véhicule et ne recrute pas un seul chauffeur, tout en continuant d'enregistrer des pertes immenses[58]. Uber a perdu la somme faramineuse de 5,24 milliards de dollars au second trimestre 2019[59]. Ce qui manque à Uber en termes de capital et d'infrastructure est compensé par la collecte et l'analyse d'un volume colossal de données sur les usagers, les conducteurs et leurs voitures et sur leurs déplacements dans la ville et leurs interactions les uns avec les autres. Ces données lui permettent non seulement d'ajuster et d'améliorer le service proposé à ses clients dès aujourd'hui, mais à l'avenir elles permettront à Uber d'atteindre son objectif ultime, à savoir se transformer en une société de transport qui se passerait complètement des conducteurs, puisque les données commencent à être utilisées pour construire des véhicules autonomes qui finiront par remplacer la totalité de son parc automobile. Bien que sans être directement en rapport avec les dispositions du chapitre numérique des accords de commerce, Uber a récemment signalé son intention de poursuivre la Colombie qui l'a interdit sur le marché national – réaction qui ne pourra que devenir plus courante à mesure que les accords sur le commerce comporteront des chapitres sur le numérique[60].

58 Palmer, A. (1er octobre 2019) *Uber and Lyft close to record lows as investor skepticism grows around recent IPO (Les cours d'Uber et Lyft historiquement bas ; le scepticisme des investisseurs face à leur introduction en bourse augmente*). Consulté sur : https://www.cnbc.com/2019/10/01/uber-closes-at-record-low-worth-less-than-50-billion.html
59 Clark, K. (8 août 2019) *Uber lost more than $5B last quarter (Uber a perdu plus de 5 milliards de dollars le trimester dernier*). Consulté sur : https://techcrunch.com/2019/08/08/uber-stock-plummets-following-second-quarter-earnings-report/
60 Griffin, O. (10 janvier 2020) *Uber to take exit ramp in Colombia after 'arbitrary' court ruling (Uber sur la bretelle de sortie en Colombie à l'issue d'un arrêt "arbitraire").*

À la lumière des circonstances décrites plus haut, il est difficile de comprendre pourquoi des pays devraient se retrouver dans l'impossibilité de mettre en œuvre des politiques et des législations leur permettant de développer leur propre industrie technologique nationale en posant des limites aux flux de données susceptibles de quitter le pays ou en exigeant une localisation des serveurs et des personnes. Comme l'a fait la Norvège avec la technologie d'extraction pétrolière[61] ou la Corée du Sud avec la technologie grand public[62], il est essentiel que les pays disposent d'outils pour imposer des conditions sur les entreprises qui veulent accéder au marché national, qui sont celles qui vont faire naître la nouvelle génération d'activités commerciales et les nouveaux emplois.

C'est le cas particulièrement parce qu'à l'avenir le succès des entreprises, dans bon nombre de secteurs, sera ancré sur leur capacité à collecter et analyser les données. Si une grande partie des données est recueillie par des plateformes transnationales qui sont en mesure d'agréger des ensembles de données au niveau mondial, grâce à la libre circulation transfrontières des données, alors il sera beaucoup plus difficile pour les concurrents nationaux d'émerger ; en effet, ceux-ci, même s'ils ont le capital nécessaire pour recruter des personnes et se doter des systèmes analytiques, n'auront jamais la possibilité d'obtenir la même quantité de données.

INCIDENCE 8 – AVANTAGER LES SOCIÉTÉS TRANSNATIONALES PLUTÔT QUE LES MICRO, PETITES ET MOYENNES ENTREPRISES (MPME)

L'un des principaux arguments avancés publiquement en faveur de l'inclusion dans les accords de libre-échange des dispositions sur le commerce électronique ou sur le commerce numérique est qu'elles rendent possible et favorisent la capacité des MPME de faire du commerce numérique et donc d'avoir des débouchés dans des marchés qui auparavant n'étaient accessibles qu'aux grandes multinationales. Des règles complètement reformulées, écrites par et pour les MPME, pourraient contribuer à ce noble objectif et donner à ces entreprises de réelles possibilités de croissance et de nouveaux débouchés commerciaux. Néanmoins, dans les faits, les accords déjà conclus et ceux qui sont proposés ne font que très peu, voire rien, pour aider les MPME, car ils sont complètement alignés sur les besoins des Big Tech, qui sont celles qui vont le plus profiter des accords. En outre, le fonctionnement même de l'économie numérique tend généralement à favoriser les géants du secteur plutôt que les MPME.

Les MPME sont le véritable moteur de l'économie, non seulement dans les pays en développement mais aussi dans les pays industrialisés. Ce sont elles qui représentent la majorité de l'emploi soit, concrètement, 45 % des postes de travail ; elles constituent aussi une grande partie de l'activité économique, à hauteur de 33 % des revenus nationaux[63]. Cependant les exigences des Big Tech, promues par une armée croissante de lobbyistes, sont souvent en conflit avec les besoins de MPME. Un exemple probant concerne le paiement des impôts. Les géants du secteur abusent de leur présence mondiale pour faire en sorte de réduire au minimum leur assujettissement à l'impôt, ce qui mène à des situations telles que celle de la filiale irlandaise d'Apple dont le taux d'imposition a été de 0,005 % en 2014[64]. De même, Uber au Royaume-Uni fait transiter les paiements de tous ses clients par le Luxembourg, évitant ainsi d'avoir à payer la TVA au Royaume-Uni, même si cette pratique a été dénoncée devant les tribunaux[65]. Ces pratiques font qu'il est très difficile pour les MPME d'être concurrentielles, car elles ne sont pas en mesure de se prévaloir de structures complexes d'optimisation fiscale et auront un handicap de coût de 20 %.

La combinaison de plusieurs des dispositions pourrait placer des obstacles supplémentaires, d'une part en empêchant l'apparition de MPME et en ne leur permettant pas d'être concurrentielles face aux géants du secteur bien établis, et d'autre part en favorisant ces géants de la technologie. Par exemple, la libre circulation transfrontières des données serait moins avantageuse pour les MPME qui n'ont pas besoin de cette disposition pour leurs activités, puisqu'elles sont pour l'essentiel basées dans un seul pays. Les MPME auraient également moins de probabilités de tirer profit de l'achat de grands ensembles de données collectées grâce à la circulation transnationale des données. En revanche, puisque l'analyse de grands ensembles de données permet d'améliorer les services numériques, la libre circulation transfrontières des données serait tout à l'avantage des Big Tech.

Les MPME ont fait valoir des inquiétudes très particulières au sujet de la concentration des marchés des Big Tech dans de nombreux secteurs qui sont fondamentaux pour le commerce électronique, par exemple les places de marchés, les solutions de paiement électronique, et la logistique. Les MPME se plaignent également du fait que les entreprises présentes dans ces marchés si concentrés sont à même d'exploiter leur position dominante pour faire payer aux autres des frais ou adhésions excessives. Ces marchés concentrés signifient que les MPME, ayant un pouvoir de négocia-

Consulté sur : https://www.reuters.com/article/us-uber-colombia/uber-to-take-exit-ramp-in-colombia-after-arbitrary-court-ruling-idUSKBN1Z921L

61 Heum, P. (2008) *Local Content Development: experience from oil and gas activities in Norway (Développement du contenu local: l'expérience des activités pétrolières et gazières en Norvège).* Institute for research in economics and business administration. Consulté sur : https://openaccess.nhh.no/nhh-xmlui/bitstream/handle/11250/166156/A02_08.pdf?sequence=1

62 Chen, C. & Sewell, G. (1996) *Strategies for technological development in South Korea and Taiwan: the case of semiconductors (Stratégies de développement technologique en Corée du Sud et à Taïwan : le cas des semiconducteurs).* Research Policy Volume 25, Issue 5, Pages 759-783. Consulté sur : https://www.sciencedirect.com/science/article/abs/pii/0048733395008616

63 OCDE (2017) *Renforcer les contributions des PME dans une économie mondialisée et numérique.* Consulté sur : https://search.oecd.org/fr/industrie/C-MIN-2017-8-FR.pdf

64 Taylor, H. (30 août 2016) *How Apple managed to pay a 0.005 percent tax rate in 2014 (Comment Apple a réussi à obtenir un taux d'imposition de 0,005 % en 2014*). Consulté sur : https://www.cnbc.com/2016/08/30/how-apples-irish-subsidiaries-paid-a-0005-percent-tax-rate-in-2014.html

65 Kaminski, I. (10 octobre 2019) *Uber's VAT liability confirmed (L'assujettissement d'Uber à la TVA confirmé*. Consulté sur : https://ftalphaville.ft.com/2019/10/09/1570629132000/Uber-s-UK-VAT-liability-confirmed/

tion réduit, sont à la merci des grandes entreprises du secteur, parce que si elles veulent mettre un pied sur le marché mondial du commerce électronique, elles sont obligées d'acheter leurs services, même à des conditions qui leur semblent injustes. L'essor de cette dynamique a mené à une résurgence de l'intérêt accordé au concept de monopsone, le cousin éloigné (et moins connu) du monopole. Alors que le monopole se définit comme « une structure de marché caractérisée par la présence d'un seul vendeur qui vend un produit unique sur le marché », le monopsone décrit « une situation de marché dans lequel n'existe qu'un seul acheteur ».

Comme observé par Richard Hill, grand militant de la société civile : « Alors que du point de vue conceptuel le commerce électronique est bon pour les PME, les règles qui sont proposées à l'OMC pour le régir permettraient aux plateformes, dont la position dominante pose déjà un problème aux PME, de les presser encore plus en leur faisant payer davantage ». Alors que de plus en plus d'achats se font en ligne et que l'on assiste à la fermeture accélérée des magasins physiques, les pays vont rencontrer un gros problème de recettes fiscales, notamment les collectivités locales dont les revenus dépendent souvent considérablement des impôts fonciers des entreprises locales.

INCIDENCE 9 – L'AGRICULTURE ET LE COMMERCE NUMÉRIQUE

L'agriculture mondiale et le secteur alimentaire dans son ensemble subissent une révolution qui pourrait être aussi dramatiques que toutes celles qui l'ont précédée. Il y a eu trois grandes révolutions, à commencer par la révolution agricole originale des 18e et 19e siècles en Europe, suivie de la révolution verte des années 1950 et 1960 puis de la révolution des OGM des années 2000. Aujourd'hui, la perspective d'exploitations agricoles sans ouvriers, où le travail serait effectué par des robots, ne semble pas si éloignée ; d'aucuns y réfléchissent[66], alors que d'autres y prennent déjà part (à grands frais)[67]. Ce n'est pas tout de suite en revanche que cette idée sera adoptée par le grand public. Pourtant, ce à quoi l'on assiste à l'heure actuelle, c'est la restructuration radicale de la manière dont se produisent et sont distribués les aliments, et par qui. Au niveau mondial, le système alimentaire de petite échelle dans lequel de petites exploitations agricoles, généralement familiales, cultivent de petites parcelles de terre, en recourant souvent aux méthodes traditionnelles, et vendent leur propre production dans les marchés locaux ou dans la rue, réussit encore à nourrir 70 % de la population mondiale[68]. Au cours des dernières années, tout comme les méthodes de culture traditionnelles avaient été mises en question, ce sont les marchés traditionnels qui ont dû faire face à une concurrence accrue des places de marché en ligne. Cette transition a le potentiel d'accabler des millions de personnes dont les moyens de subsistance sont en train de devenir un secteur porté par les métadonnées, la technologie et les entreprises d'envergure mondiale.

Les avancées des Big Tech dans le secteur agricole et de l'agroalimentaire en général présentent un certain nombre de défis à ceux qui dépendent de l'agriculture de petite échelle et qui en vivent. Une inquiétude croissante est que les nouvelles technologies numériques, qui permettent d'assembler des gènes en laboratoire, font apparaître de nouvelles formes de biopiraterie qui contournent les réglementations existantes au détriment des communautés locales et indigènes[69]. C'est ainsi qu'un actif précieux, qui est un bien commun utilisé par tous les paysans, serait transformé en quelque chose dont le secteur de l'agro-technologie serait propriétaire. Le comportement d'entreprises telles que Monsanto, qui s'est retrouvée sur le devant de la scène lors de la troisième révolution agricole, et développe des semences stériles dites Terminator de sorte que les paysans ne peuvent pas conserver de semences, tout en traînant devant les tribunaux ceux qui le font, alimente cette crainte. En outre, maintenant que l'agriculture même s'appuie sur des procédés qui dépendent chaque fois plus de la technologie, qu'il s'agisse de la culture, de la récolte, de la distribution, on se retrouve avec des entreprises technologiques qui n'avaient rien à voir avec le secteur agricole, comme Fujitsu et Amazon, qui se mettent à acheter de plus en plus d'entreprises du secteur et pourraient finir par dominer la technologie agricole[70]. Et comme dans tout domaine porté par les données, la crainte est aussi celle d'assister, au fil du temps, à la concentration de ces grandes entreprises pour se retrouver devant un nombre encore plus restreint de méga-entreprises, comme on le voit déjà dans de nombreux pans de l'agriculture aujourd'hui[71].

De plus en plus de denrées alimentaires sont désormais livrées en passant par des plateformes numériques plutôt que sur les marchés ou dans des commerces physiques. La plateformisation du système de livraison des denrées alimentaires est non seulement en train de remettre en question les moyens de subsistance des exploitants agricoles, mais pose aussi un problème plus général de réglementation et de responsabilité.

66 Paquette, D. (17 février 2019) *Farmworker vs Robot (Ouvrier agricole contre robot).* Consulté sur : https://www.washingtonpost.com/news/national/wp/2019/02/17/feature/inside-the-race-to-replace-farmworkers-with-robots/

67 Thu, M. & Hong, B. (24 mars 2016) *Smart farming a bright future for Vietnam (Un brillant avenir pour l'agriculture intelligente au Vietnam*). Consulté sur : https://www.nationthailand.com/business/30282386

68 ETC (2017) *Who will feed us? Industrial food chain vs the peasant food web (Qui va nous nourrir ? Agroalimentaire industriel contre réseaux paysans d'alimentation*). ETC Group. Consulté sur : https://www.etcgroup.org/content/who-will-feed-us-industrial-food-chain-vs-peasant-food-web

69 Servick, K. (17 novembre 2016) *Rise of digital DNA raises biopiracy fears (L'essor de l'ADN numérique réveille des craintes de biopiratage).* Consulté sur : https://www.sciencemag.org/news/2016/11/rise-digital-dna-raises-biopiracy-fears

70 Site Web de Fujitsu. *IoT in Agriculture (L'internet des objets dans l'agriculture).* Consulté sur : https://www.fujitsu.com/global/themes/internet-of-things/hyperconnected-business/agriculture/

71 ETC (2018) *Too big to feed: the short report (Trop grand pour nourrir: un bref rapport).* ETC Group. Consulté sur : https://www.etcgroup.org/content/too-big-feed-short-report

Par exemple, Alibaba, gigantesque plateforme chinoise de commerce électronique, vend du lait frais, souvent importé, directement aux consommateurs chinois (et d'autres pays aussi). Les pays à s'être dotés de réglementations qui traitent de manière adéquate de la distribution en ligne de denrées alimentaires sont relativement rares, notamment pour des livraisons transfrontières ; or ces réglementations incluent des normes d'une importance vitale en termes de sécurité des aliments, raison pour laquelle la multiplication des canaux de commercialisation électronique internationaux pose de graves défis[72]. Par exemple, qui doit être tenu pour responsable des questions relatives à la qualité du lait, à la manière dont il est produit ? ; en dernière instance, contre qui se retourner juridiquement si des problèmes devaient survenir ? Cette situation serait encore plus compliquée si les propositions contenues dans la nouvelle vague d'accords sur le commerce étaient mises en œuvre, ce qui rendrait légal pour un opérateur économique tel qu'Alibaba, ou d'autres plateformes de commerce électronique, de se lancer dans ces activités sans avoir de « présence locale » dans le pays, ou encore de contourner l'exigence d'acheter local[73].

Un troisième défi posé à l'agriculture de petite échelle par les Big Tech est le niveau d'intégration verticale et horizontale que nous observons dans le secteur de la technologie agricole. Un exemple probant : le rachat par Monsanto de la société d'agriculture numérique et compagnie d'assurances The Climate Corporation pour près d'un milliard de dollars[74]. Pour Monsanto, ce qu'il y avait de plus précieux dans ce rachat, c'était l'immense volume de données sur les fermiers, les cultures et le climat, ainsi que la capacité de faire de ces données du renseignement exploitable, afin de dire aux agriculteurs quoi semer, combien d'azote utiliser ou quel pesticide appliquer. Si pour de nombreux agriculteurs ce sont là des informations utiles, ils ne se rendent généralement pas compte que les données qu'ils fournissent sont encore plus précieuses pour la société technologique, qui va les utiliser pour ensuite les cribler de marketing ciblé. Surtout, ces entreprises viseront souvent à finir par automatiser les moyens de subsistance en utilisant ces données en conjonction avec « les progrès de la puissance de calcul, la dextérité, la planification du mouvement et l'optique informatisée, qui rendent possible une nouvelle génération de robots »[75]. Les dispositions qui consolident la libre circulation internationale des données rendront plus facile pour les entreprises multinationales du secteur technologique agricole de recueillir et compiler des données du monde entier. Ce qui leur permettra, ayant davantage de données, de générer de meilleurs produits que ceux qui auraient pu être mis au point localement par des agriculteurs à partir de leurs propres données, ou même au niveau national en tentant une agrégation des données. En outre, le fait d'interdire le partage obligatoire du code source de logiciels chaque fois plus indispensables dans les exploitations agricoles, même dans le cadre de programmes de transfert de technologies, protégera les intérêts des multinationales technologiques agricoles au détriment des petits agriculteurs locaux et du soutien à une industrie nationale.

Notre système de production alimentaire commence à être absorbé par la croissance de la nouvelle génération d'agro-industries, alimentées par les données et les rachats, qui cherchent à capter l'information (plutôt que la terre) par exemple sur les semences, l'ADN ou les données sur les sols et l'efficacité du recours aux pesticides, tout en commercialisant une « agriculture de précision » toujours plus sophistiquée[76]. Cette évolution fait en sorte que les agriculteurs dépendent chaque fois plus d'une poignée de grandes sociétés multinationales, lesquelles, par leur recours à la technologie de l'agriculture de précision, peuvent réduire au minimum l'utilisation d'intrants tels que l'eau ou les pesticides, tout en portant les rendements au maximum. À ceci s'ajoute le fait que bon nombre d'agriculteurs dépendent déjà d'entreprises telles que Monsanto pour leurs semences et leurs engrais. On pourrait voir cette évolution comme une contribution à la solution au changement climatique dans le secteur agricole[77], mais la technologie liée à l'agriculture de précision est extrêmement onéreuse, et seules les plus grandes entreprises agricoles peuvent se les permettre. Par conséquent, ces changements vont encore plus précariser les moyens de subsistance des petits agriculteurs, car on les accuse injustement de la crise du climat et ils ne seront pas en mesure de se procurer les dernières technologies de précision.

Historiquement, le lobby de l'agro-industrie a toujours critiqué que l'alimentation et l'agriculture soient exclues des accords de libre-échange (ALE) bilatéraux[78]. Maintenant, non seulement de nombreux ALE incluent-ils le secteur agricole, mais les ALE sont souvent utilisés aussi pour tenter de forcer l'ouverture des marchés ou de restreindre la faculté des gouvernements à imposer leur normes et réglementations. En même temps, la puissance de l'agro-industrie à grande échelle portée par la technologie progresse au sein de l'OMC par le biais des dispositions sur la propriété intellectuelle de l'ADPIC, qui protègent des formes spécifiques de propriété intellectuelle et facilitent les fusions.

72 GRAIN (31 mai 2018) *Top e-commerce companies move into retail (Les plus importantes entreprises du commerce électronique se lancent dans la vente au détail).* Consulté sur : https://www.grain.org/en/article/5957-top-e-commerce-companies-move-into-retail

73 Voir Incidence 2 – Rendre plus difficile l'application de la législation locale du travail

74 Tsotsis, A. (2 octobre 2013) *Monsanto buys weather big data company climate corporation for around $1.1B (Monsanto achète la société de big data météorologique Climate Corporation pour environ 1,1 milliard de dollars).* Consulté sur : https://techcrunch.com/2013/10/02/monsanto-acquires-weather-big-data-company-climate-corporation-for-930m/

75 Alexander, B. (3 octobre 2018) *If farms are to survive, we need to think about them as tech companies (Pour que les fermes survivent, nous devons les voir comme des sociétés technologiques*). Consulté sur : https://qz.com/1383635/if-farms-are-to-survive-we-need-to-think-about-them-as-tech-companies/

76 NESTA website. *Precision Agriculture.* Consulté sur : https://www.nesta.org.uk/feature/precision-agriculture/

77 Klein, A. (26 juillet 2019 July 26) *How tech is helping the agriculture sector curb carbon emissions (Comment la technologie aide le secteur agricole à réduire les émissions de carbo*ne). Consulté sur : https://www.weforum.org/agenda/2019/07/agtech-can-climate-proof-the-planets-harvests/

78 Bilaterals webpage. *Agriculture and Food (Agriculture et alimentation).* Consulté sur : https://www.bilaterals.org/?-agriculture-food-

Même si les dispositions sur le commerce numérique ne sont pas celles qui créent les problèmes sous-jacents, la libre circulation des données, liée à l'interdiction d'exiger le transfert du code source (ainsi que les questions entourant la présence locale) signifient que les grandes entreprises de l'agro-industrie seront toujours celles qui tireront le plus grand avantage du commerce numérique, au détriment des petits agriculteurs.